AOS-CX 10.06 Monitoring Guide

8320, 8325, 8630 Switch Series

a Hewlett Packard
Enterprise company

Part Number: 5200-7712
Published: November 2020
Edition: 1

Notices

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

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

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

Acknowledgments

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 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)

Latest version available online

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

Command syntax notation conventions

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

Table Continued

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

About the examples

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

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

Understanding the CLI prompts

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

```
switch>
```

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

`switch>`

Indicates the operator command context.

`switch#`

Indicates the manager command context.

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

Indicates the configuration context for a feature. For example:

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

Identifies the `interface` context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

member/slot/port

On the 8325 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Line module number. Always 1.
- *port*: Physical number of a port on a line module

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

Diagnosing with the LEDs

This section describes LED patterns on the switch that indicate problem conditions for general switch operation troubleshooting.

1. Check the table for the LED pattern you see on the switch.
2. Refer to the corresponding diagnostic tip.

Table 1: *LED error indicators for 8320*

Global status	Port LED	Diagnostic tip
Off with power cord plugged in	N/A	1
Solid amber	N/A	2
Slow flash amber	N/A	3
Slow flash amber	Slow flash amber[1]	4
Solid green	Off with cable connected	5
Solid green	On, but the port is not communicating	6

[1] The flashing behavior is an on/off cycle approximately once every 1.6 seconds.

Table 2: *LED error indicators for 8325*

PS1/PS2 LEDs	Global Status	Fan	Port LED	Diagnostic Tip
Off with power cords plugged in	-	-	-	1
On amber[1]	Flashing amber	-	-	2
On green	Flashing amber	On amber	-	3
On green	Flashing amber	-	Flashing amber	4
On green	On green	-	Off with cable connected	5
On green	On green	-	On, but the port is not communicating	6

[1] Either the PS1 or PS2 LED is on amber, but not both.

Table 3: *Diagnostic tips*

Tip	Problem	Solution
1	Both switch power supplies are not plugged into an active AC power source.	Verify the AC power source works by plugging another device into the outlet. Or try plugging the power supplies into different outlets or try different power cords. If the problem is still not resolved, both power supplies may be faulty.
2	One of the power supplies is not plugged into an active A power source, or the power supply may have failed.	Verify that the power cord is plugged into an active power source and to the power supply. Make sure that the connections are snug. Try power cycling the switch by unplugging and plugging the power cord back into the other working power supply. If the PS1/PS2 LED is still not on, verify the AC power source works by plugging another device into the outlet or try a different power cord. If the power source and power cord are OK and this condition persists, the switch power supply may have failed. Call your Hewlett Packard Enterprise-authorized network reseller, or use the electronic support services from Hewlett Packard Enterprise to get assistance.
3	One of the switch fan assemblies may have failed.	Try disconnecting power from the switch and wait a few moments. Then reconnect the power to the switch and check the LEDs again If the error indication reoccurs, one of the fan assemblies has failed. If the ambient temperature does not exceed normal room temperature, the switch may continue to operate under this condition; but for best operation, replace the fan assembly. Call your Hewlett Packard Enterprise-authorized network reseller, or use the electronic support services from Hewlett Packard Enterprise to get assistance.

Table Continued

Tip	Problem	Solution
4	The network port for which the LED is flashing has experienced a self-test or initialization failure.	Try power cycling the switch. If the fault indication reoccurs: • There may be a port configuration mismatch where a 10G transceiver is installed in a port configured for 25G, or the reverse. • A 10GBase-T transceiver may be installed in an incompatible port. Only ports 1, 2, 4, 5, 7, 8, 10, and 11 support 10GBase-T transceivers. • The transceiver may have failed. • The switch port may have failed. Check the switch Event Log and show interface command output for indication of the fault condition. If the port is an SFP+/SFP28 transceiver or QSFP+/QSFP28 transceiver, verify that it is one of the transceivers supported by the switch. Unsupported or unrecognized transceivers will be identified with this fault condition. For a list of supported transceivers, see the *ArubaOS-Switch and ArubaOS-CX Transceiver Guide* in the **Hewlett Packard Enterprise Information Library**. The transceivers are also tested when they are "hot-swapped" - installed or changed while the switch is powered on. To verify that the port has failed, remove and reinstall the transceiver without powering off the switch. If the port fault indication reoccurs, you will have to replace the transceiver. Check the event log to see why the transceiver failed. To get assistance, call your Hewlett Packard Enterprise-authorized network reseller, or use the electronic support services from Hewlett Packard Enterprise.

Table Continued

Tip	Problem	Solution
5	The network connection is not working properly.	Try the following procedures: • For the indicated port, verify that both ends of the cabling, at the switch and the connected device, are connected properly. • Verify that the connected device and switch are both powered on and operating correctly. • Verify that you have used the correct cable type for the connection: ◦ For fiber-optic connections, verify that the transmit port on the switch is connected to the receive port on the connected device and that the switch receive port is connected to the transmit port on the connected device. ◦ The cable verification process must include all patch cables from any end devices, including the switch, to any patch panels in the cabling path. • Verify that the port has not been disabled through a switch configuration change. Use the console interface or, if you have configured an IP address on the switch, use the web browser interface to determine the state of the port and re-enable the port if necessary. • Verify that the switch port configuration matches the configuration of the attached device. For example, if the switch port is configured as “Full-duplex”, the port on the attached device also MUST be configured as “Full-duplex”. If the configurations do not match, the results could be an unreliable connection, or no link at all. • If the other procedures do not resolve the problem, try using a different port or a different cable.
6	The port may be improperly configured, or the port may be in a “blocking” state by the normal operation of the Spanning Tree, LACP, or IGMP features.	Use the switch console to see if the port is part of a dynamic trunk (through the LACP feature), if Spanning Tree is enabled on the switch, and if the port may have been put into a “blocking” state by those features. The `show lacp interfaces` command displays the port status for the LACP feature; the show spanning tree command displays the port status for Spanning Tree. Also check the Port Status screen using the `show interfaces` command to see if the port has been configured as “disabled”. Other switch features that may affect the port operation include VLANs, IGMP, and port group settings. Use the switch console to see how the port is configured for these features. Ensure that the device at the other end of the connection is indicating a good link to the switch. If it is not, the problem may be with the cabling between the devices or the connectors on the cable.

Chassis LEDs

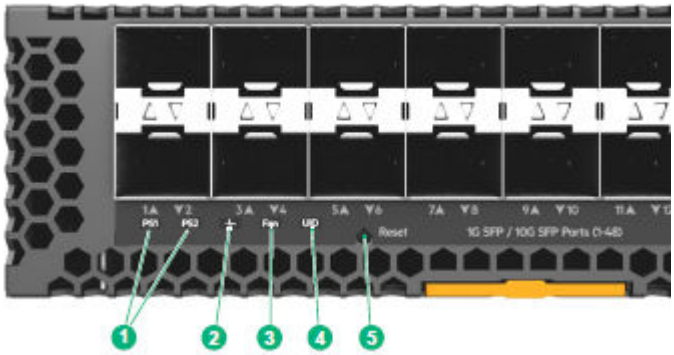

Table 4: *Chassis LED labels*

	LED
1	Power supply LEDs
2	Global status LEDs
3	Fan LED
4	Unit identification LED
5	Reset button

Table 5: *Chassis LED behavior*

Chassis LEDs	Function	State	Meaning
PS1/PS2	Power supply status	On green	Power supply is installed and operating normally.
		Slow flash amber	Fault detected for installed power supply.
		Off	Power supply is not installed or not receiving power.
Fan	Fan tray status	On green	System fans are operating normally.
		Slow flash amber	One or more system fans have a fault or the minimum number of fans are not installed.

Table Continued

Chassis LEDs	Function	State	Meaning
Global Status	Internal power status of the switch. Self-test status Switch/port fault status	On amber	The switch has passed self-test and is powered up normally.
		Slow flash green [1]	The switch self-test and initialization are in progress after the switch has been power cycled or reset. The switch is not operational until this LED stops blinking green.
		Slow flash amber [2]	A fault or initialization failure has occurred on the switch, one of the switch ports, OOBM port, USB port, console port, power supplies, or a fan. The Status LED for the component with the fault will flash simultaneously.
		Off	The unit is not receiving power.
UID (Unit Identification)	Used to identify a unit in a rack or collection of products.	On or slow flash [3]	The `LED locator on` command allows you to flash or turn on the LED. The default is 30 minutes.
		Off	LED will clear after the timeout period has expired.

[1] The slow flash behavior is an on/off cycle approximately every 1.6 seconds.

[2] The slow flash behavior is an on/off cycle approximately every 1.6 seconds.

[3] The slow flash behavior is an on/off cycle approximately every 1.6 seconds.

Port LEDs

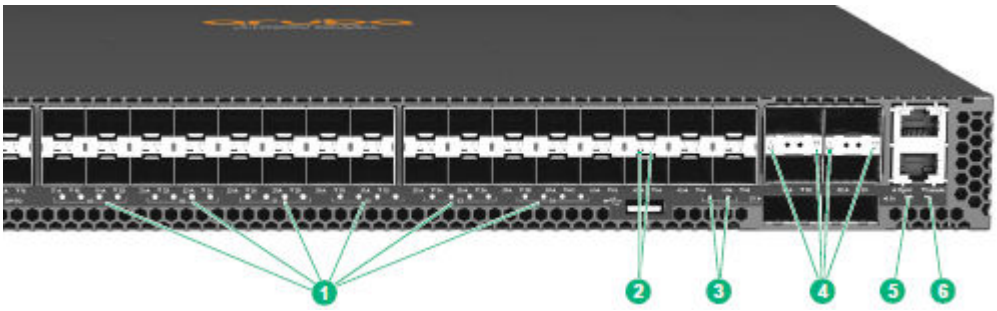

Table 6: *Port LED labels*

	LED
1	QSFP+ port lane LEDs — these LEDs are not used by the product and should remain off throughout the product's operation
2	SFP+ port LEDs
3	QSFP+ port 51, 54 LEDs
4	QSFP+ port 49, 50, 52, 53 LEDs
5	Out-of-band management port Link LED
6	Out-of-band management port Act (activity) LED

Table 7: *Port LED behavior*

Chassis LEDs	Function	State	Meaning
SFP+ port LEDs	To display link and activity information for the port.	On/flashing green	Shows a valid link at 1 Gbps or 10 Gbps. Flashing indicates port activity.
		Slow flash amber	When the Global Status LED is flashing amber, indicates an unsupported transceiver or a port failure.
QSFP+ port LEDs	To display link and activity information for the port.	On/flashing green	Shows a valid link at 40 Gbps. Flashing indicates port activity.
		Off	When the Global Status LED is flashing amber, indicates an unsupported transceiver or a port failure.
Management port Link LED	To display link information for the port.	On green	Shows a valid link.
Management port Act LED	To display activity information for the port.	Flashing green	Flashing indicates port activity.

Chassis LEDs

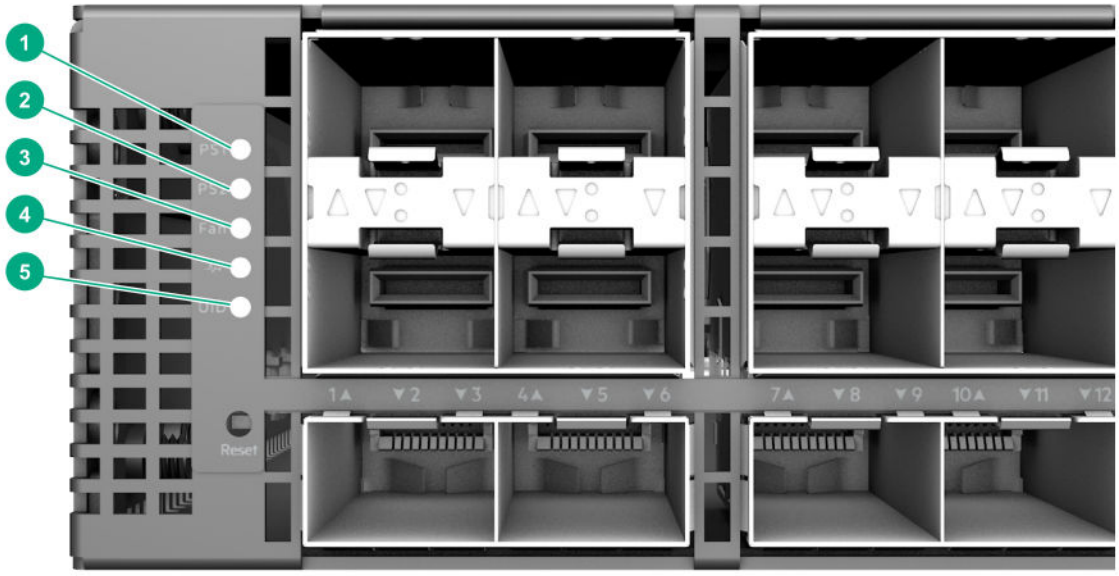

Table 8: *Chassis LEDs for the Aruba 8325-48Y8C (JL624A and JL625A)*

	LED
1	Power supply 1 (PS1) LEDs
2	Power supply 2 (PS2) LEDs
3	Fan LED
4	Global status LED
5	Unit identification LED

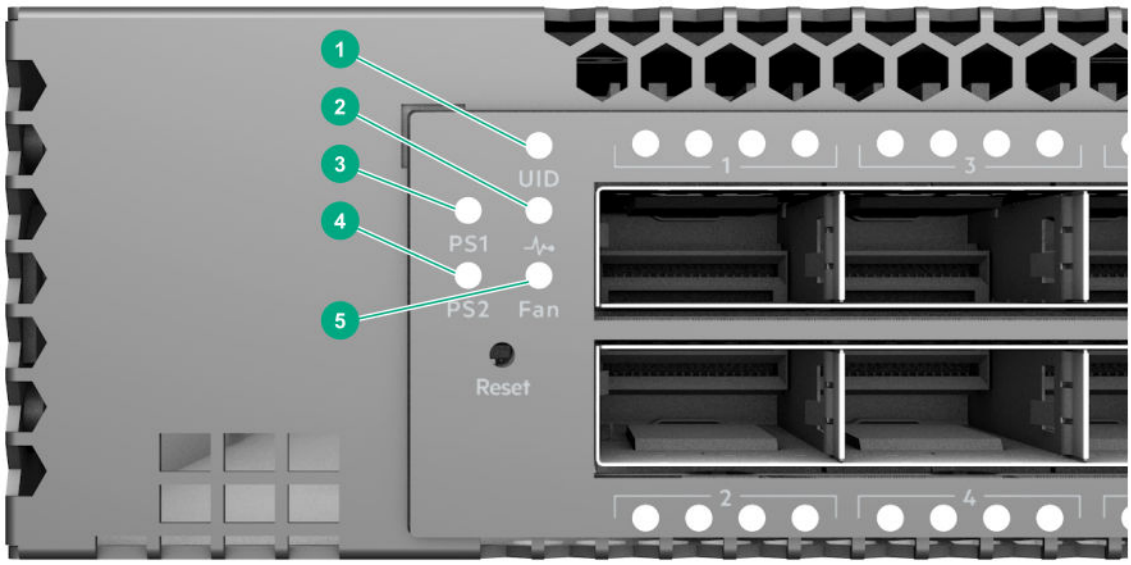

Table 9: *Chassis LEDs for the Aruba 8325-32C (JL 626A and JL627A)*

	LED
1	Unit identification LED
2	Global status LED
3	Power supply 1 (PS1) LEDs
4	Power supply 2 (PS2) LEDs
5	Fan LED

Table 10: *Chassis LED behavior*

Chassis LEDs	Function	State	Meaning
PS1/PS2	Power supply status	On green	Power supply is installed and operating normally.
		On amber	Fault detected for installed power supply, or power supply is not receiving power.
		Off	Power supply is not installed.
Fan	Fan tray status	On green	System fans are operating normally.
		On amber	One or more system fans have a fault or the minimum number of fans are not installed.
Global Status	Internal power status of the switch.	On green	The switch has passed self-test and is powered up normally.

Table Continued

Chassis LEDs	Function	State	Meaning
	Self-test status Switch/port fault status	Flashing amber	• The switch initialization is in progress during boot up. • A fault or initialization failure has occurred on the switch, one of the switch ports, power supplies, or a fan. • The port LEDs with the fault will flash simultaneously. LEDs for power supplies and fans with a fault will be on amber. • Port-speed mismatch. A transceiver is installed in a port configured for a different speed.
		Off	The unit is not receiving power.
UID (Unit Identification)	Used to identify a unit in a rack or collection of products.	On blue or flashing blue	The `LED locator on` command allows you turn on the LED. The default is 30 minutes. The `LED locator flashing` command will flash the LED.
		Off	The `LED locator off` command turns off the LED.

Port LEDs

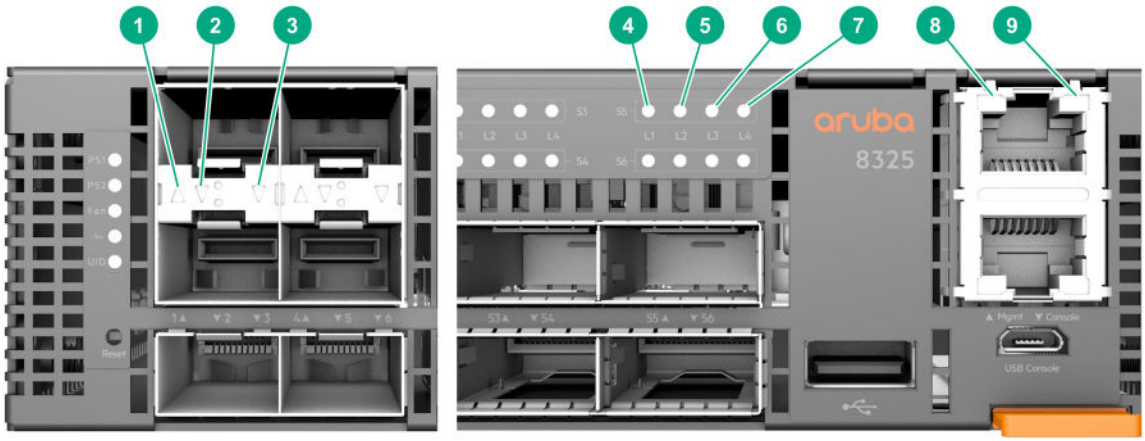

Table 11: *Port LEDs for the Aruba 8325-48Y8C (JL624A and JL625A)*

	LED
1	Upper SFP28 port LED
2	Middle SFP28 port LED
3	Lower SFP28 port LED
4	QSFP28 port LED and lane 1 indicator
5	QSFP28 lane 2 LED
6	QSFP28 lane 3 LED
7	QSFP28 lane 4 LED
8	Out-of-band management port Link LED
9	Out-of-band management port Act (activity) LED

Table 12: *Port LED behavior for the Aruba 8325-48Y8C (JL624A and JL625A)*

Chassis LEDs	Function	State	Meaning
SFP28 port LEDs	To display link and activity information for the port.	On/flashing green	Shows a valid link at 25/10 Gbps. • Fast flashing[1] indicates port activity at 25 Gbps. • Slow flashing[2] indicates port activity at 10 Gbps.
		Flashing amber	When the Global Status LED is simultaneously flashing amber, indicates port-speed mismatch, an incompatible, unsupported, faulty transceiver, or a port failure.
		Off	Port is disabled, not connected, or not receiving a link beat signal.

Table Continued

Chassis LEDs	Function	State	Meaning
QSFP28 port LEDs	To display link and activity information for the port.	On/flashing green	Shows a valid link at 100/40 Gbps. • Fast flashing[3] indicates port activity at 100 Gbps. • Slow flashing[4] indicates port activity at 40 Gbps.
		Flashing amber	When the Global Status LED is simultaneously flashing amber with the Lane 1 LED, indicates an unsupported or faulty transceiver, or a port failure.
		Off	Port is disabled, not connected, or not receiving a link beat signal. Lanes 2-4 are always off and are currently unused by HPE-Aruba software.
Management port Link LED	To display link information for the port.	On green	Shows a valid link.
		Off	Port is disabled, not connected, or not receiving a link beat signal.
Management port Act LED	To display activity information for the port.	Flashing yellow	Flashing indicates port activity.

1 The fast flashing behavior is an on/off cycle once every 0.8 seconds, approximately.

2 The slow flashing behavior is an on/off cycle once every 1.6 seconds, approximately.

3 The fast flashing behavior is an on/off cycle once every 0.8 seconds, approximately.

4 The slow flashing behavior is an on/off cycle once every 1.6 seconds, approximately.

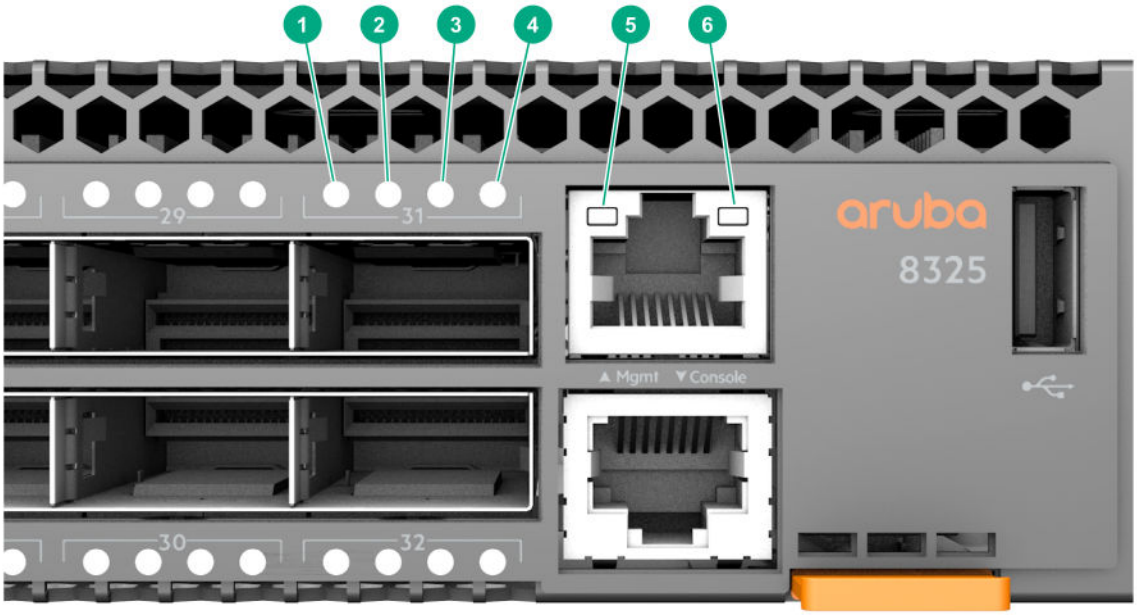

Table 13: *Port LEDs for the Aruba 8325-32C (JL626A and JL627A)*

	LED
1	QSFP28 port LED and lane 1 indicator
2	QSFP28 lane 2 LED (Not supported with currently released software.)
3	QSFP28 lane 3 LED (Not supported with currently released software.)
4	QSFP28 lane 4 LED (Not supported with currently released software.)
5	Unused
6	Out-of-band management port Link and Activity LED

Table 14: *Port LED behavior for the Aruba 8325-32C (JL626A and JL627A)*

Chassis LEDs	Function	State	Meaning
QSFP28 port LEDs	To display link and activity information for the port.	On/flashing green	Shows a valid link at 100/40 Gbps. • Fast flashing[1] indicates port activity at 100 Gbps. • Slow flashing[2] indicates port activity at 40 Gbps.
		Flashing amber	When the Global Status LED is simultaneously flashing amber with the Lane 1 LED, indicates an unsupported or faulty transceiver, or a port failure.
		Off	Port is disabled, not connected, or not receiving a link beat signal. Lanes 2-4 are always off and are currently unused by HPE-Aruba software.
Management port Link LED	To display link information for the port.	On green	Shows a valid link.
		Off	Port is disabled, not connected, or not receiving a link beat signal.
Management port Act LED	To display activity information for the port.	Flashing yellow	Flashing indicates port activity.

1 The fast flashing behavior is an on/off cycle once every 0.8 seconds, approximately.

2 The slow flashing behavior is an on/off cycle once every 1.6 seconds, approximately.

boot set-default

Syntax

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

Description

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

Command context

Manager (#)

Parameters

primary

Selects the primary network operating system image.

secondary

Selects the secondary network operating system image.

Authority

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

Example

Selecting the primary image as the default boot image:

```
switch# boot set-default primary
Default boot image set to primary.
```

boot system

Syntax

```
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.

Command context

Manager (#)

Parameters

`primary`

Selects the primary operating system image for this reboot and sets the configured default operating system image to `primary` for future reboots.

`secondary`

Selects the secondary operating system image for this reboot and sets the configured default operating system image to `secondary` for future reboots.

`serviceos`

Selects the service operating system for this reboot. Does not change the configured default operating system image. The service operating system acts as a standalone bootloader and recovery OS for switches running the ArubaOS-CX operating system and is used in rare cases when troubleshooting a switch.

Authority

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

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#
```

show boot-history

Syntax

```
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.

Command context

Manager (#)

Parameters

`all`

Shows boot information for the active management module and all available line modules.

Authority

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

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
...
```

bluetooth disable

Syntax

```
bluetooth disable

no bluetooth disable
```

Description

Disables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE). Bluetooth is enabled by default.

The `no` form of this command enables the Bluetooth feature on the switch.

Command context

```
config
```

Authority

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

Example

Disabling Bluetooth on the switch. *<XXXX>* is the switch platform and *<NNNNNNNNNN>* is the device identifier.

```
switch(config)# bluetooth disable
switch# show bluetooth
Enabled              : No
Device name          : <XXXX>-<NNNNNNNNNN>

switch(config)# show running-config
...
bluetooth disabled
...
```

bluetooth enable

Syntax

```
bluetooth enable

no bluetooth enable
```

Description

This command enables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

Default: Bluetooth is enabled by default.

The `no` form of this command disables the Bluetooth feature on the switch.

Command context

`config`

Authority

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

Usage

The default configuration of the Bluetooth feature is `enabled`. The output of the `show running-config` command includes Bluetooth information only if the Bluetooth feature is disabled.

The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

The Bluetooth feature requires the USB feature to be enabled. If the USB feature has been disabled, you must enable the USB feature before you can enable the Bluetooth feature.

Examples

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

clear events

Syntax

`clear events`

Description

Clears up event logs. Using the `show events` command will only display the logs generated after the `clear events` command.

Command context

Manager (`#`)

Authority

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

Examples

Clearing all generated event logs:

```
switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2018-10-14:06:57:53.534384|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 27
2018-10-14:06:58:30.805504|lldpd|103|LOG_INFO|MSTR|1|Configured LLDP tx-timer to 36
2018-10-14:07:01:01.577564|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 49

switch# clear events

switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2018-10-14:07:03:05.637544|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 34
```

clear ip errors

Syntax

```
clear ip errors
```

Description

Clears all IP error statistics.

Command context

Manager (#)

Authority

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

Example

Clearing and showing ip errors:

```
switch# clear ip errors
switch# show ip errors
---------------------------------
Drop reason                Packets
---------------------------------
Malformed packets                0
IP address errors                0
...
```

domain-name

Syntax

```
domain-name <NAME>

no domain-name [<NAME>]
```

Description

Specifies the domain name of the switch.

The no form of this command sets the domain name to the default, which is no domain name.

Command context

```
config
```

Parameters

<NAME>

Specifies the domain name to be assigned to the switch. The first character of the name must be a letter or a number. Length: 1 to 32 characters.

Authority

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

Examples

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Setting the domain name to the default value:

```
switch(config)# no domain-name
switch(config)# show domain-name

switch(config)#
```

hostname

Syntax

`hostname <HOSTNAME>`

`no hostname [<HOSTNAME>]`

Description

Sets the host name of the switch.

The `no` form of this command sets the host name to the default value, which is `switch`.

Command context

`config`

Parameters

<HOSTNAME>

Specifies the host name. The first character of the host name must be a letter or a number. Length: 1 to 32 characters. Default: `switch`

Authority

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

Examples

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
myswitch
```

Setting the host name to the default value:

```
myswitch(config)# no hostname
switch(config)#
```

led locator

Syntax

```
led locator {on | off | slow_blink | flashing | fast_blink | half_bright}
```

Description

Sets the state of the locator LED.

Command context

Manager (#)

Parameters

on

Turns on the LED.

off

Turns off the LED, which is the default value.

slow_blink

Sets the LED to slow blink on and off.

flashing

Sets the LED to blink on and off repeatedly.

fast_blink

Sets the LED to fast blink on and off.

half_bright

Sets the LED intensity to half bright.

Authority

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

Example

Setting the state of the locator LED:

```
switch# led locator flashing
```

mtrace

Syntax

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

Description

Traces the specified IPv4 source and group addresses.

Command context

Manager (#)

Parameters

IPV4-SRC-ADDR

Specifies the source IPv4 address to trace.

IPV4-GROUP-ADDR

Specifies the group IPv4 address to trace.

lhr *<IPV4-LHR-ADDR>*

Specifies the last hop router address from which to start the trace.

ttl *<HOPS>*

Specifies the Time-To-Live duration in hops. Range: 1 to 255 hops. Default: 8 hops.

vrf *<VRF-NAME>*

Specifies the name of the VRF. If a name is not specified the default VRF will be used.

Authority

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

Examples

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

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

Type escape sequence to abort.
Mtrace from 10.0.0.1 for Source 20.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  20.0.0.1 PIM  123 ms
```

Tracing with source and group addresses:

```
(switch)# mtrace 200.0.0.1 239.1.1.1

Type escape sequence to abort.
Mtrace from self for Source 200.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  200.0.0.1 PIM  123 ms
```

show bluetooth

Syntax

```
show bluetooth
```

Description

Shows general status information about the Bluetooth wireless management feature on the switch.

Command context

Operator (>) or Manager (#)

Authority

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

Usage

This command shows status information about the following:

- The USB Bluetooth adapter
- Clients connected using Bluetooth
- The switch Bluetooth feature.

The output of the `show running-config` command includes Bluetooth information only if the Bluetooth feature is disabled.

The device name given to the switch includes the switch serial number to uniquely identify the switch while pairing with a mobile device.

The management IP address is a private network address created for managing the switch through a Bluetooth connection.

Examples

Example output when Bluetooth is enabled but no Bluetooth adapter is connected. *<XXXX>* is the switch platform and *<NNNNNNNNNN>* is the device identifier.

```
switch# show bluetooth
Enabled              : Yes
Device name          : <XXXX>-<NNNNNNNNNN>
Adapter State        : Absent
```

Example output when Bluetooth is enabled and there is a Bluetooth adapter connected:

```
switch# show bluetooth
Enabled              : Yes
Device name          : <XXXX>-<NNNNNNNNNN>
Adapter State        : Ready
Adapter IP address   : 192.168.99.1
Adapter MAC address  : 480fcf-af153a

Connected Clients
-----------------
Name             MAC Address      IP Address     Connected Since
--------------   --------------   ------------   ------------------------
Mark's iPhone    089734-b12000    192.168.99.10   2018-07-09 08:47:22 PDT
```

Example output when Bluetooth is disabled:

```
switch# show bluetooth
Enabled             : No
Device name         : <XXXX>-<NNNNNNNNNN>
```

show capacities

Syntax

```
show capacities <FEATURE> [vsx-peer]
```

Description

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

Command context

Manager (#)

Parameters

<FEATURE>

Specifies a feature. For example, `aaa` or `vrrp`.

[vsx-peer]

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

Authority

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

Usage

Capacities are expressed in user-understandable terms. Thus they may not map to a specific hardware or software resource or component. They are not intended to define a feature exhaustively.

Examples

Showing all available capacities for BGP:

```
switch# show capacities bgp

System Capacities: Filter BGP
Capacities Name                                                                  Value
--------------------------------------------------------------------------------------
Maximum number of AS numbers in as-path attribute                                   32
...
```

Showing all available capacities for mirroring:

```
switch# show capacities mirroring

System Capacities: Filter Mirroring
Capacities Name                                                                Value
-------------------------------------------------------------------------------------
Maximum number of Mirror Sessions configurable in a system                         4
Maximum number of enabled Mirror Sessions in a system                              4
```

Showing all available capacities for MSTP:

```
switch# show capacities mstp

System Capacities: Filter MSTP
Capacities Name                                                                    Value
-----------------------------------------------------------------------------------------
Maximum number of mstp instances configurable in a system                             64
```

Showing all available capacities for VLAN count:

```
switch# show capacities vlan-count

System Capacities: Filter VLAN Count
Capacities Name                                                                    Value
-----------------------------------------------------------------------------------------
Maximum number of VLANs supported in the system                                    4094
```

show capacities-status

Syntax

```
show capacities-status <FEATURE>
     [vsx-peer]
```

Description

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

Command context

Manager (#)

Parameters

<FEATURE>

Specifies the feature, for example `aaa` or `vrrp` for which to display capacities, values, and status. Required.

[vsx-peer]

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

Authority

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

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name                                                          Value Maximum
-----------------------------------------------------------------------------------------------
Number of active gateway mac addresses in a system                                  0      16
Number of aspath-lists configured                                                   0      64
Number of community-lists configured                                                0      64
...
```

show core-dump

Syntax

`show core-dump [all | <SLOT-ID>]`

Description

Shows core dump information about the specified module. When no parameters are specified, shows only the core dumps generated in the current boot of the management module. When the `all` parameter is specified, shows all available core dumps.

Command context

Manager (`#`)

Parameters

`all`

Shows all available core dumps.

`<SLOT-ID>`

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

You must specify the slot ID for either the active management module, or the line module.

Authority

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

Usage

When no parameters are specified, the `show core-dump` command shows only the core dumps generated in the current boot of the management module. You can use this command to determine when any crashes are occurring in the current boot.

If no core dumps have occurred, the following message is displayed: `No core dumps are present`

To show core dump information for the standby management module, you must use the `standby` command to switch to the standby management module and then execute the `show core-dump` command.

In the output, the meaning of the information is the following:

`Daemon Name`

Identifies name of the daemon for which there is dump information.

`Instance ID`

Identifies the specific instance of the daemon shown in the `Daemon Name` column.

`Present`

Indicates the status of the core dump:

`Yes`

The core dump has completed and available for copying.

In Progress

Core dump generation is in progress. Do not attempt to copy this core dump.

Timestamp

Indicates the time the daemon crash occurred. The time is the local time using the time zone configured on the switch.

Build ID

Identifies additional information about the software image associated with the daemon.

Examples

Showing core dump information for the current boot of the active management module only:

```
switch# show core-dump
================================================================================
Daemon Name     | Instance ID | Present    | Timestamp             | Build ID
================================================================================
hpe-fand          1399          Yes          2017-08-04 19:05:34      1246d2a
hpe-sysmond       957           Yes          2017-08-04 19:05:29      1246d2a
================================================================================
Total number of core dumps : 2
================================================================================
```

Showing all core dumps:

```
switch# show core-dump all
================================================================================
Management Module core-dumps
================================================================================
Daemon Name     | Instance ID | Present    | Timestamp           | Build ID
================================================================================
hpe-sysmond       513           Yes          2017-07-31 13:58:05    e70f101
hpe-tempd         1048          Yes          2017-08-13 13:31:53    e70f101
hpe-tempd         1052          Yes          2017-08-13 13:41:44    e70f101

Line Module core-dumps
================================================================================
Line Module : 1/1
================================================================================
dune_agent_0      18958         Yes          2017-08-12 11:50:17    e70f101
dune_agent_0      18842         Yes          2017-08-12 11:50:09    e70f101
================================================================================
Total number of core dumps : 5
================================================================================
```

show domain-name

Syntax

```
show domain-name
```

Description

Shows the current domain name.

Command context

Manager (#)

Authority

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

Usage

If there is no domain name configured, the CLI displays a blank line.

Example

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

show environment fan

Syntax

```
show environment fan [vsf | vsx-peer]
```

Description

Shows the status information for all fans and fan trays (if present) in the system.

Command context

Manager (#)

Parameters

vsf

Shows output from the VSF member-id on switches that support VSF.

[vsx-peer]

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

Authority

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

Usage

For fan trays, `Status` is one of the following values:

ready

The fan tray is operating normally.

fault

The fan tray is in a fault event. The status of the fan tray does not indicate the status of fans.

empty

The fan tray is not installed in the system.

For fans:

Speed

Indicates the relative speed of the fan based on the nominal speed range of the fan. Values are:

Slow

The fan is running at less than 25% of its maximum speed.

Normal

The fan is running at 25-49% of its maximum speed.

Medium

The fan is running at 50-74% of its maximum speed.

Fast

The fan is running at 75-99% of its maximum speed.

Max

The fan is running at 100% of its maximum speed.

N/A

The fan is not installed.

Direction

The direction of airflow through the fan. Values are:

front-to-back

Air flows from the front of the system to the back of the system.

N/A

The fan is not installed.

Status

Fan status. Values are:

uninitialized

The fan has not completed initialization.

ok

The fan is operating normally.

fault

The fan is in a fault state.

empty

The fan is not installed.

Examples

Showing output for a system without a fan tray:

```
switch# show environment fan

Fan information
```

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

show environment led

Syntax

```
show environment led [vsf <MEMBER-ID>| vsx-peer]
```

Description

Shows state and status information for all the configurable LEDs in the system.

Command context

Operator (>) or Manager (#)

Parameters

vsf *<MEMBER-ID>*

Shows output from the specified VSF member-id on switches that support VSF.

[vsx-peer]

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

Authority

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

Example

show environment power-supply

Syntax

```
show environment power-supply [vsf | vsx-peer]
```

Description

Shows status information about all power supplies in the switch.

Command context

Operator (>) or Manager (#)

Parameters

`vsf`

Shows output from the VSF member-id on switches that support VSF.

`[vsx-peer]`

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

Authority

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

Usage

The following information is provided for each power supply:

Mbr/PSU

Shows the member and slot number of the power supply.

Product Number

Shows the product number of the power supply.

Serial Number

Shows the serial number of the power supply, which uniquely identifies the power supply.

PSU Status

The status of the power supply. Values are:

`OK`

Power supply is operating normally.

`OK*`

Power supply is operating normally, but it is the only power supply in the chassis. One power supply is not sufficient to supply full power to the switch. When this value is shown, the output of the command also shows a message at the end of the displayed data.

`Absent`

No power supply is installed in the specified slot.

`Input fault`

The power supply has a fault condition on its input.

`Output fault`

The power supply has a fault condition on its output.

`Warning`

The power supply is not operating normally.

Wattage Maximum

Shows the maximum amount of wattage that the power supply can provide.

Example

show environment temperature

Syntax

```
show environment temperature [detail] [vsf | vsx-peer]
```

Description

Shows the temperature information from sensors in the switch that affect fan control.

Command context

Operator (>) or Manager (#)

Parameters

detail

Shows detailed information from each temperature sensor.

vsf

Shows output from the VSF member-id on switches that support VSF.

[vsx-peer]

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

Authority

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

Usage

Temperatures are shown in Celsius.

Valid values for status are the following:

normal

Sensor is within nominal temperature range.

min

Lowest temperature from this sensor.

max

Highest temperature from this sensor.

low_critical

Lowest threshold temperature for this sensor.

critical

Highest threshold temperature for this sensor.

fault

Fault event for this sensor.

emergency

Over temperature event for this sensor.

Examples

show events

Syntax

Description

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

Command context

Manager (#)

Parameters

-e *<EVENT-ID>*

Shows the event logs for the specified event ID. Event ID range: 101 through 99999.

-s {alert | crit | debug | emer | err | info | notice | warn}

Shows the event logs for the specified severity. Select the severity from the following list:

- `alert`: Displays event logs with severity alert and above.
- `crit`: Displays event logs with severity critical and above.
- `debug`: Displays event logs with all severities.
- `emer`: Displays event logs with severity emergency only.
- `err`: Displays event logs with severity error and above.
- `info`: Displays event logs with severity info and above.
- `notice`: Displays event logs with severity notice and above.
- `warn`: Displays event logs with severity warning and above.

-r

Shows the most recent event logs first.

-a

Shows all event logs, including those events from previous boots.

-n *<count>*

Displays the specified number of event logs.

-c {lldp | ospf | ... | }

Shows the event logs for the specified event category. Enter `show event -c` for a full listing of supported categories with descriptions.

-d {lldpd | hpe-fand | ... |}

Shows the event logs for the specified process. Enter `show event -d` for a full listing of supported daemons with descriptions.

Authority

Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

Examples

Showing event logs:

```
switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
```

Showing the most recent event logs first:

```
switch# show events -r
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Showing all event logs:

```
switch# show events -a
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
```

Showing event logs related to the DHCP relay agent:

```
switch# show events -c dhcp-relay
2016-05-31:06:26:27.363923|hpe-relay|110001|LOG_INFO|DHCP Relay Enabled
2016-05-31:07:08:51.351755|hpe-relay|110002|LOG_INFO|DHCP Relay Disabled
```

Showing event logs related to the DHCPv6 relay agent:

```
switch# show events -c dhcpv6-relay
2016-05-31:06:26:27.363923|hpe-relay|109001|LOG_INFO|DHCPv6 Relay Enabled
2016-05-31:07:08:51.351755|hpe-relay|109002|LOG_INFO|DHCPv6 Relay Disabled
```

Showing event logs related to IRDP:

```
switch# switch# show events -c irdp
2016-05-31:06:26:27.363923|hpe-rdiscd|111001|LOG_INFO|IRDP enabled on interface %s
2016-05-31:07:08:51.351755|hpe-rdiscd|111002|LOG_INFO|IRDP disabled on interface %s
```

Showing event logs related to LACP:

```
switch# show events -c lacp
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Showing event logs as per the specified process:

```
switch# show events -d lacpd
-------------------------------------------------
show event logs
-------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

Displaying the specified number of event logs:

```
switch# show events -n 5
-------------------------------------------------
show event logs
-------------------------------------------------
2018-03-21:06:12:15.500603|arpmgrd|6101|LOG_INFO|AMM|-|ARPMGRD daemon has started
2018-03-21:06:12:17.734405|lldpd|109|LOG_INFO|AMM|-|Configured LLDP tx-delay to 2
2018-03-21:06:12:17.740517|lacpd|1307|LOG_INFO|AMM|-|LACP system ID set to 70:72:cf:d4:34:42
2018-03-21:06:12:17.743491|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity 42cc3df7-1113-412f-b5cb-e8227b8c22f2
2018-03-21:06:12:17.904008|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity 4409133e-2071-4ab8-adfe-f9662c06b889
```

show hostname

Syntax

```
show hostname [vsx-peer]
```

Description

Shows the current host name.

Command context

Manager (#)

Parameters

[vsx-peer]

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

Authority

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

Example

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
myswitch
```

show images

Syntax

```
show images [vsx-peer]
```

Description

Shows information about the software in the primary and secondary images.

Command context

Operator (>) or Manager (#)

Parameters

[vsx-peer]

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

Authority

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

Example

Showing the primary and secondary images on a 8320 switch:

```
switch# show images
--------------------------------------------------------------------------------
ArubaOS-CX Primary Image
--------------------------------------------------------------------------------
Version : TL.10.05.0001I
Size    : 405 MB
Date    : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

--------------------------------------------------------------------------------
ArubaOS-CX Secondary Image
--------------------------------------------------------------------------------
Version : TL.10.05.0001I
Size    : 405 MB
Date    : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

Default Image : primary

------------------------------------------------------
Management Module 1/1 (Active)
------------------------------------------------------
Active Image       : primary
Service OS Version : TL.01.05.0002-internal
BIOS Version       : TL-01-0013
```

show ip errors

Syntax

```
show ip errors [vsx-peer]
```

Description

Shows IP error statistics for packets received by the switch since the switch was last booted.

Command context

Operator (>) or Manager (#)

Parameters

[vsx-peer]

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

Authority

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

Usage

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

Drop reasons are the following:

Malformed packet

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

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

IP address error

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

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

Invalid TTLs

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

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

Example

Showing ip error statistics for packets received by the switch:

```
switch# show ip errors
---------------------------------
Drop reason                Packets
---------------------------------
Malformed packets                1
IP address errors               10
...
```

show module

Syntax

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

Description

Shows information about installed line modules and management modules.

Command context

Operator (>) or Manager (#)

Parameters

<SLOT-ID>

Specifies the member and slot numbers in format `member/slot`. For example, to show the module in member 1, slot 3, enter `1/3`.

`[vsx-peer]`

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

Authority

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

Usage

Identifies and shows status information about the line modules and management modules that are installed in the switch.

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

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

To show the configuration information—if any—associated with that line module slot, use the `show running-configuration` command.

Status is one of the following values:

`Active`

This module is the active management module.

`Standby`

This module is the standby management module.

`Deinitializing`

The module is being deinitialized.

`Diagnostic`

The module is in a state used for troubleshooting.

`Down`

The module is physically present but is powered down.

Empty

The module hardware is not installed in the chassis.

Failed

The module has experienced an error and failed.

Failover

This module is a fabric module or a line module, and it is in the process of connecting to the new active management module during a management module failover event.

Initializing

The module is being initialized.

Present

The module hardware is installed in the chassis.

Ready

The module is available for use.

Updating

A firmware update is being applied to the module.

Examples

Showing all installed modules:

Showing a slot that does not contain a line module:

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

show running-config

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<FEATURE>

Specifies the name of a feature. For a list of feature names, enter the `show running-config` command, followed by a space, followed by a question mark (?). When the `json` parameter is used, the `vsx-peer` parameter is not applicable.

all

Shows all default values for the current running configuration.

[vsx-peer]

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

Authority

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

Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version ArubaOS-CX 10.0X.XXXX
!
lldp enable
linecard-module LC1 part-number JL363A
vrf green
!
!
!
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
router ospf 1 vrf green
    area 0.0.0.0
router pim vrf green
    enable
    rp-address 30.0.0.4
vlan 1
    no shutdown
vlan 20
    no shutdown
vlan 30
    no shutdown
interface 1/1/1
    no shutdown
    no routing
    vlan access 30
interface 1/1/32
    no shutdown
    no routing
    vlan access 20
interface bridge_normal-1
    no shutdown
interface bridge_normal-2
    no shutdown
interface vlan20
    no shutdown
    vrf attach green
    ip address 20.0.0.44/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
```

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

    ip pim-sparse hello-interval 100
```

Showing the current running configuration in json format:

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

Show the current running configuration without default values:

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

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

Show the current running configuration with default values:

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

show running-config current-context

Syntax

```
show running-config current-context
```

Description

Shows the current non-default configuration running on the switch in the current command context.

Command context

`config` or a child of `config`. See Usage.

Authority

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

Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (`config`) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance.

  Support for this command is provided for one level below the `config` context. For example, entering this command for a child of a child of the `config` context not supported.

  If you enter the command on a child of the `config` context, the current configuration of that context and the children of that context are displayed.

- The global configuration (`config`) context.

  If you enter this command in the global configuration (`config`) context, it shows the running configuration of the entire switch. Use the `show running-configuration` command instead.

Examples

Showing the running configuration for the current interface:

```
switch(config-if)# show running-config current-context
interface 1/1/1
    vsx-sync qos vlans
    no shutdown
    description Example interface
    no routing
vlan access 1
    exit
```

Showing the current running configuration for the management interface:

```
switch(config-if-mgmt)# show running-config current-context
interface mgmt
    no shutdown
    ip static 10.0.0.1/24
    default-gateway 10.0.0.8
    nameserver 10.0.0.1
```

Showing the running configuration for the external storage share named `nasfiles`:

```
switch(config-external-storage-nasfiles)# show running-config current-context
external-storage nasfiles
   address 192.168.0.1
   vrf default
   username nasuser
   password ciphertext AQBapalKj+XMsZumHEwIc9OR6YcOw5Z6Bh9rV+9ZtKDKzvbaBAAAAB1CTrM=
   type scp
   directory /home/nas
   enable
switch(config-external-storage-nasfiles)#
```

Showing the running configuration for a context that does not have instances:

```
switch(config-vsx)# show run current-context
vsx
    inter-switch-link 1/1/1
```

```
    role secondary
    vsx-sync sflow time
```

show startup-config

Syntax

```
show startup-config [json]
```

Description

Shows the contents of the startup configuration.

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

Command context

Manager (#)

Parameters

`json`

Display output in JSON format.

Authority

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

Examples

Showing the startup-configuration in non-JSON format for an 8320 switch:

Showing the startup-configuration in JSON format:

```
switch# show startup-config json
Startup configuration:
{
    "AAA_Server_Group": {
        "local": {
            "group_name": "local"
        },
        "none": {
            "group_name": "none"
        }
    },
...
```

show system

Syntax

```
show system [vsx-peer]
```

Description

Shows general status information about the system.

Command context

Operator (>) or Manager (#)

[vsx-peer]

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

Authority

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

Usage

CPU utilization represents the average utilization across all the CPU cores.

System Contact, System Location, and System Description can be set with the `snmp-server` command.

Examples

Showing system information for the VSX primary and secondary (peer) switch on an 8320:

show system resource-utilization

Syntax

```
show system resource-utilization [daemon <DAEMON-NAME> | module <SLOT-ID>] [vsx-peer]
```

Description

Shows information about the usage of system resources such as CPU, memory, and open file descriptors.

Command context

Manager (#)

Parameters

daemon *<DAEMON-NAME>*

Shows the filtered resource utilization data for the process specified by *<DAEMON-NAME>* only.

NOTE: For a list of daemons that log events, enter `show events -d ?` from a switch prompt in the manager (#) context.

module *<SLOT-ID>*

Shows the filtered resource utilization data for the line module specified by *<SLOT-ID>* only.

[vsx-peer]

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

Authority

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

Examples

Showing all system resource utilization data:

```
switch# show system resource-utilization
System Resources:
Processes: 70
CPU usage(%): 20
Memory usage(%): 25
Open FD's: 1024

Process              CPU Usage(%)          Memory Usage(%)     Open FD's
-------------------------------------------------------------------------
pmd                     2                       1                  14
hpe-sysmond             1                       2                  11
hpe-mgmdd               0                       1                  5
...
```

Showing the resource utilization data for the pmd process:

```
switch# show system resource-utilization daemon pmd
Process              CPU Usage          Memory Usage    Open FD's
-------------------------------------------------------------------------
pmd                      2                 1              14
```

Showing resource utilization data when system resource utilization polling is disabled:

```
switch# show system resource-utilization
System resource utilization data poll is currently disabled
```

Showing resource utilization data for a line module:

```
switch# show system resource-utilization module 1/1
System Resource utilization for line card module: 1/1
CPU usage(%): 0
Memory usage(%): 35
Open FD's: 512
```

show tech

Syntax

`show tech [basic | <FEATURE>] [local-file]`

Description

Shows detailed information about switch features by automatically running the `show` commands associated with the feature. If no parameters are specified, the `show tech` command shows information about all switch features. Technical support personnel use the output from this command for troubleshooting.

Command context

Manager (`#`)

Parameters

`basic`

Specifies showing a basic set of information.

<FEATURE>

Specifies the name of a feature. For a list of feature names, enter the `show tech` command, followed by a space, followed by a question mark (?).

`local-file`

Shows the output of the `show tech` command to a local text file.

Authority

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

Usage

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

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

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

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

Example

Showing the basic set of system information:

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

******************************
Command : show core-dump all
******************************
no core dumps are present

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

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

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

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

show usb

Syntax
```
show usb
```

Description

Shows the USB port configuration and mount settings.

Command context

Operator (>) or Manager (#)

Parameters

[vsx-peer]

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

Authority

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

Examples

If USB has not been enabled:

```
switch> show usb
Enabled: No
Mounted: No
```

If USB has been enabled, but no device has been mounted:

```
switch> show usb
Enabled: Yes
Mounted: No
```

If USB has been enabled and a device mounted:

```
switch> show usb
Enabled: Yes
Mounted: Yes
```

show usb file-system

Syntax
```
show usb file-system [<PATH>]
```

Description

Shows directory listings for a mounted USB device. When entered without the <PATH> parameter the top level directory tree is shown.

Command context

Operator (>) or Manager (#)

Parameters

<PATH>

Specifies the file path to show. A leading "/" in the path is optional.

Authority

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

Usage

Adding a leading "/" as the first character of the *<PATH>* parameter is optional.

Attempting to enter '..' as any part of the *<PATH>* will generate an invalid path argument error. Only fully-qualified path names are supported.

Examples

Showing the top level directory tree:

```
switch# show usb file-system
/mnt/usb:
'System Volume Information'  dir1'

/mnt/usb/System Volume Information':
IndexerVolumeGuid  WPSettings.dat

/mnt/usb/dir1:
dir2  test1

/mnt/usb/dir1/dir2:
test2
```

Showing available path options from the top level:

```
switch# show usb file-system /
total 64
drwxrwxrwx 2 32768 Jan 22 16:27 'System Volume Information'
drwxrwxrwx 3 32768 Mar  5 15:26 dir1
```

Showing the contents of a specific folder:

```
switch# show usb file-system /dir1
total 32
drwxrwxrwx 2 32768 Mar  5 15:26 dir2
-rwxrwxrwx 1     0 Feb  5 18:08 test1

switch# show usb file-system dir1/dir2
total 0
-rwxrwxrwx 1 0 Feb  6 05:35 test2
```

Attempting to enter an invalid character in the path:

```
switch# show usb file-system dir1/../..
Invalid path argument
```

show version

Syntax

```
show version [vsx-peer]
```

Description

Shows version information about the network operating system software, service operating system software, and BIOS.

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Example

system resource-utilization poll-interval

Syntax

```
system resource-utilization poll-interval <SECONDS>
```

Description

Configures the polling interval for system resource information collection and recording such as CPU and memory usage.

Command context

```
config
```

Parameters

<SECONDS>

Specifies the poll interval in seconds. Range: 10-3600. Default: 10.

Authority

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

Example

Configuring the system resource utilization poll interval:

```
switch(config)# system resource-utilization poll-interval 20
```

top cpu

Syntax

```
top cpu
```

Description

Shows CPU utilization information.

Command context

Manager (#)

Authority

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

Example

Showing top CPU information:

```
switch# top cpu
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks:  76 total, 2 running, 74 sleeping,  0 stopped,  0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total,  2487508 free,  897040 used,   661948 buff/cache
KiB Swap:       0 total,        0 free,       0 used,  2859196 avail Mem

  PID USER     PRI  NI   VIRT    RES   SHR S  %CPU %MEM      TIME+ COMMAND
...
```

top memory

Syntax

```
top memory
```

Description

Shows memory utilization information.

Command context

Manager (#)

Authority

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

Example

Showing top memory:

```
switch> top memory
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks:  76 total, 2 running, 74 sleeping,  0 stopped,  0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total,  2487508 free,  897040 used,   661948 buff/cache
KiB Swap:       0 total,        0 free,       0 used,  2859196 avail Mem

  PID USER     PRI  NI   VIRT    RES   SHR S  %CPU %MEM      TIME+ COMMAND
...
```

usb

Syntax

```
usb
no usb
```

Description

Enables the USB ports on the switch. This setting is persistent across switch reboots and management module failovers. Both active and standby management modules are affected by this setting.

The `no` form of this command disables the USB ports.

Command context

```
config
```

Authority

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

Example

Enabling USB ports:

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

Disabling USB ports when a USB drive is mounted:

```
switch(config)# no usb
```

usb mount | unmount

Syntax

```
usb {mount | unmount}
```

Description

Enables or disables the inserted USB drive.

Command context

Manager (#)

Parameters

`mount`

Enables the inserted USB drive.

`unmount`

Disables the inserted USB drive in preparation for removal.

Authority

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

Usage

A USB drive must be unmounted before removal.

The supported USB file systems are FAT16 and FAT32.

Examples

Mounting a USB drive in the USB port:

```
switch# usb mount
```

Unmounting a USB drive:

```
switch# usb unmount
```

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

Syntax

```
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.

Command context

```
config-external-storage-<VOLUME-NAME>
```

Parameters

<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.

Authority

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

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
```

directory

Syntax

```
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.

Command context

```
config-external-storage-<VOLUME-NAME>
```

Parameters

<DIRECTORY-NAME>

Specifies the external storage directory for mapping the volume.

Authority

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

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
```

disable

Syntax

`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.

Command context

`config-external-storage-<VOLUME-NAME>`

Authority

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

Examples

Disabling a volume named logfiles:

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

enable

Syntax

`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.

Command context

`config-external-storage-<VOLUME-NAME>`

Authority

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

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
```

external-storage

Syntax

```
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.

Command context

```
config
```

Authority

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

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
```

password

Syntax

```
password {plaintext | ciphertext} <PASSWORD>

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

Description

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

The `no` form of this command clears the password for logging in to a network attached storage server.

Command context

```
config-external-storage-<VOLUME-NAME>
```

Parameters

`plaintext`

Specifies the password be in plain text format.

ciphertext

Specifies the password be in ciphertext format.

<PASSWORD>

Specifies the password.

Authority

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

Examples

Creating a volume named logfiles with the password xxxx:

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

Clearing the plaintext password xxxx:

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

show external-storage

Syntax

```
show external-storage [<VOLUME-NAME>]
```

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<VOLUME-NAME>

Specifies the external storage volume name that the show command will use.

Authority

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

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
```

show running-config external-storage

Syntax

```
show running-config external-storage
```

Description

Shows the running configuration of the external storage.

Command context

Operator (>) or Manager (#)

Authority

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

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
```

type

Syntax

```
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.

Command context

`config-external-storage-<VOLUME-NAME>`

Parameters

`nfsv3`

Specifies the NFSv3 network access protocol.

nfsv4

Specifies the NFSv4 network access protocol.

scp

Specifies the SCP network access protocol.

Authority

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

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
```

username

Syntax

```
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.

Command context

```
config-external-storage-<VOLUME-NAME>
```

Parameters

<USER-NAME>

Specifies the username.

Authority

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

Examples

Creating a volume named logfiles with the user name nassuser:

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

Clearing the user name nasuser from accessing the logfiles volume:

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

vrf

Syntax

```
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.

Command context

```
config-external-storage-<VOLUME-NAME>
```

Parameters

<VRF-NAME>

Specifies the VRF name.

Authority

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

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
```

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

- ArubaOS-CX supports only SLA configuration through CLI and thresholds can be configured using NAE agents using WebUI/REST.
- ArubaOS-CX supports only forever tests. On-demand tests are not supported.
- Maximum sessions: IP-SLA source 500, IP-SLA responder 100.
- 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 ArubaOS-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

http

Syntax

```
http {get | raw} URL [source {<SOURCE-IPV4-ADDR> | <IFNAME>} source-port <PORT-NUM>]
     [proxy proxy-url] [cache disable] [name-server <IPV4-ADDR-DNS-SERVER>]
     [probe-interval <30-604800>] [version<VERSION-NUMBER>] [http-raw-request <RAW-PAYLOAD>]
```

Description

Configures HTTP as the IP-SLA test mechanism. Requires destination URL and type of HTTP request (raw/get).

Command context

```
config-ip-sla-<IP-SLA-NAME>
```

Parameters

{get | raw}

Selects HTTP request type as GET or RAW where the system will generate or provide HTTP payload.

URL

Specifies HTTP URL address of syntax. http://<HOST NAME/IP-ADDRESS>:<PORT>/<PATH>.

source {*<SOURCE-IPV4-ADDR>* | *<IFNAME>*}

Selects the source IPv4 address for SLA probes or the source interface to use for sending IP-SLA probes.

source-port *<PORT-NUM>*

Specifies the value of the source port for the IP-SLA probes.

cache disable

Selects cache option for the HTTP server. By default the option is enabled.

name-server *<IPV4-ADDR-DNS-SERVER>*

Specifies the IPv4 address of DNS server.

probe-interval *<PROBE-INTERVAL>*

Specifies the probe interval in seconds. Range: 30 to 604800.

version *<VERSION-NUMBER>*

Specifies the source interface to use for sending IP-SLA probes.

http-raw-request *<RAW-PAYLOAD>*

HTTP raw request. String.

Authority

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

Examples

```
switch(config-ipsla-1)# http get http://device.arubanetworks.com/root/home.html
    switch(config-ipsla-1)# http raw http://device.arubanetworks.com/root/home.html
    switch(config-ipsla-1)# http 2.2.2.2 source 1/1/1
    switch(config-ipsla-1)# http http://device.arubanetworks.com  source 2.2.2.1
    switch(config-ipsla-1)# http http://device.arubanetworks.com/root/home.html source-interface 1/1/1
    switch(config-ipsla-1)# http http://device.arubanetworks.com  name-server 10.10.10.2
    switch(config-ipsla-1)# http raw raw-request "GET /en/US/hmpgs/index.html HTTP/1.0\r\n\r\n"
```

icmp-echo

Syntax

```
icmp-echo {<DEST-IPV4-ADDR>|<HOSTNAME>} [source {<SOURCE-IPV4-ADDR> | <IFNAME>}]
     [name-server <IPV4-ADDR-DNS-SERVER>] [payload-size <PAYLOAD-SIZE>]
     [tos <TYPE-OF-SERVICE>] [probe-interval <PROBE-INTERVAL>]
```

Description

Configures ICMP echo as the IP-SLA test mechanism. Requires destination address for the IP-SLA test.

Command context

```
config-ip-sla-<IP-SLA-NAME>
```

Parameters

{*<DEST-IPV4-ADDR>* | *<HOSTNAME>*}

Selects the destination IPv4 address for the IP-SLA or the hostname of the destination.

[source {*<SOURCE-IPV4-ADDR>* | *<IFNAME>*}]

Selects the source IPv4 address for SLA probes or the source interface to use for sending IP-SLA probes.

name-server *<IPV4-ADDR-DNS-SERVER>*

Specifies the DNS server for destination hostname resolution.

payload-size *<PAYLOAD-SIZE>*

Specifies the payload size of an SLA probe. Range: 0 to 1440.

tos *<TYPE-OF-SERVICE>*

Specifies the type of serve to be used in the probe packets. Range: 0 to 255.

probe-interval *<PROBE-INTERVAL>*

Specifies the probe interval in seconds. Range: 5 to 604800.

Authority

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

Examples

```
switch(config)# ip-sla test
    switch(config-ip-sla-test)# icmp-echo 2.2.2.2
    switch(config-ip-sla-test)# icmp-echo 2.2.2.2 source 3.3.3.3
    switch(config-ip-sla-test)# icmp-echo 2.2.2.2 source 3.3.3.3 payload-size 400
    switch(config-ip-sla-test)# icmp-echo 2.2.2.2 source 3.3.3.3 payload-size 400 name-server 4.4.4.4
    switch(config-ip-sla-test)# icmp-echo 2.2.2.2 source 3.3.3.3 payload-size 400 name-server 4.4.4.4  probe-interval 80
```

ip-sla

Syntax

```
ip-sla <IP-SLA-NAME>
no ip-sla <IP-SLA-NAME>
```

Description

Creates an IP Service Level Agreement (SLA) profile and switches to the `config-ip-sla` context.

The `no` form of this command deletes an IP-SLA profile. By default, all profile use the default VRF (default).

Command context

`config`

Parameters

<IP-SLA-NAME>

Specifies an IP-SLA profile name. Length: 1 to 63 characters.

Authority

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

Examples

Creating an IP-SLA:

```
switch(config)# ip-sla 1
switch(config-ip-sla-1)#
```

Deleting an IP-SLA:

```
switch(config)# no ip-sla 1
switch(config)#
```

ip-sla responder

Syntax

```
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>
```

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.

Command context

`config`

Parameters

`<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.

Authority

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

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 <SLA-NAME>
```

show ip-sla responder

Syntax

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

Description

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

Command context

```
config
```

Parameters

<SLA-NAME>

Specifies the SLA name.

Authority

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

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
```

show ip-sla responder results

Syntax

```
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.

Command context

```
config
```

Parameters

<SLA-NAME>

Specifies the SLA name.

<SOURCE-IPV4-ADDR>

Specifies the source IPV4 address.

<PORT-NUM>

Specifies the port number. Range: 1 to 65535.

Authority

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

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
```

show ip-sla <SLA-NAME>

Syntax

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

Description

Shows the given IP-SLA source configuration and status.

Command context

Operator (>) or Manager (#)

Parameters

<SLA-NAME>

Specifies the SLA name.

results

Shows the statistics calculated for an SLA type.

Authority

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

Examples

```
switch# show ip-sla xyz results

   IP-SLA session status
      IP-SLA Name                    : xyz
      IP-SLA Type                    : tcp-connect
      Destination Host Name/IP Address: 2.2.2.1
      Destination Port               : 8888
      Source IP Address/IFName       : 2.2.2.2
      Source Port                    : 5555
      Status                         : Running

   IP-SLA session cumulative counters
      Total Probes Transmitted       : 1
      Probes Timed-out               : 0
      Bind Error                     : 0
      Destination Address Unreachable : 0
      DNS Resolution Failures        : 0
      Reception Error                : 0
      Transmission Error             : 0

   IP-SLA Latest Probe Results
```

```
       Last Probe Time                 : 2018 Jul 13 02:00:35
       Packets Sent                    : 1
       Packets Received                : 1
       Packet Loss in Test             : 0.0000%

    Minimum RTT(ms)                    : 0.7900
    Maximum RTT(ms)                    : 0.7900
    Average RTT(ms)                    : 0.7900
    DNS RTT(ms)                        : 0.0000
    TCP RTT(ms)                        : 0.9710

switch(config)# show ip-sla xyz
    IP-SLA Name             : xyz
    Status                  : scheduled
    IP-SLA Type             : tcp-connect
    VRF                     : ipslasrc
    Source Port             : 5555
    Source IP               : 2.2.2.2
    Source Interface        :
    Domain Name Server      :
    Probe interval(seconds) : 90


switch(config)# show ip-sla jitter-sla results
    IP-SLA session status
       IP-SLA Name                     : jitter-sla
       IP-SLA Type                     : udp-jitter-voip
       Destination Host Name/IP Address: 2.2.2.1
       Destination Port                : 8888
       Source IP Address/IFName        :
       Source Port                     : 5555
       Status                          : Running

    IP-SLA Session Cumulative Counters
       Total Probes Transmitted        : 1
       Probes Timed-out                : 0
       Bind Error                      : 0
       Destination Address Unreachable : 0
       DNS Resolution Failures         : 0
       Reception Error                 : 0
       Transmission Error              : 0

    IP-SLA Latest Probe Results
       Last Probe Time                 : 2018 Jul 13 02:02:48
       Packets Sent                    : 1
       Packets Received                : 1
       Packet Loss in Test             : 0.0000%

       Minimum RTT(ms)                 : 0.7900
       Maximum RTT(ms)                 : 0.7900
       Average RTT(ms)                 : 0.7900
       DNS RTT(ms)                     : 0.0000

       Min Positive SD                 : 1      Min Positive DS        : 2
       Max Positive SD                 : 1      Max Positive DS        : 2
       Positive SD Number              : 2      Positive DS Number     : 2
       Positive SD Sum                 : 2      Positive DS Sum        : 4
       Positive SD Average             : 5      Positive DS Average    : 5
       Min Negative SD                 : 1      Min Negative DS        : 1
       Max Negative SD                 : 1      Max Negative DS        : 1
       Negative SD Number              : 2      Negative DS Number     : 4
       Negative SD Sum                 : 2      Negative DS Sum        : 4
       Negative SD Average             : 5      Negative DS Average    : 5

       Max SD Delay                    : 0      Max DS Delay           : 0
       Min SD Delay                    : 0      Min DS Delay           : 0
       Average SD Delay                : 0      Average DS Delay       : 0

    Voice Scores:
       MOS  Score                      : 4.38   ICPIF                  : 0


switch(config)# show ip-sla m3op
    IP-SLA Name             : jitter-sla
    Status                  : Running
    IP-SLA Type             : udp-jitter-voip
    VRF                     : ipslasrc
    Source IP               : 2.2.2.2
    Source Interface        :
    Domain Name Server      :
    TOS                     : 10
    Probe Interval(seconds) : 90
    Advantage Factor        : 0
    Codec Type              : g711a
```

```
switch(config)# show ip-sla http-sla
    IP-SLA Name             : http-sla
    Status                  : Running
    IP-SLA Type             : http
    VRF                     : ipslasrc
    Source IP               : 2.2.2.2
    Source Interface        :
    Domain Name Server      : 10.10.10.2
    Probe Interval(seconds) : 90
    HTTP Request Type       : GET
    HTTP/HTTPS URL          : abcd.com/ws/home
    Cache                   : Enabled
    HTTP Proxy URL          :
    HTTP Version Number     : 1.1
    ```

IP-SLA status description
    ```
    | Status                  | Description                                    |
    |-------------------------|------------------------------------------------|
    | Running                 | SLA is fully operational                       |
    | Bind Error              | Another service is using the same source port  |
    | Interface Down          | Interface status is not up
    | Dns Resolution Error    | Failed to resolve destination hostname         |
    | No Route                | No available route to the responder            |
    | Internal Error          | Unexpected error prevents SLA session          |
    | Disabled                | SLA is disabled                                |
    |Configuration Incomplete | Configuration is not complete to enable the SLA|
    ```
IP SLA session cumulative counters description
    ```
    | Status                          | Description                                                                  |
    |---------------------------------|------------------------------------------------------------------------------|
    |Probes Timed-out                 | Total numbers of probes failed to receive response.                          |
    |Bind Error                       | Total numbers of probes transmission failed as source port not available.|
    |Destination Address Unreachable | Total numbers of probes transmission failed due to route unavailable.    |
    |DNS Resolution Failures          | Total numbers of probes failed due to DNS resolution failure.            |
    |Reception Error                  | Total numbers of probes failed due to internal error in reception.       |
    |Transmission Error               | Total numbers of probes failed due to internal errr in transmission.     |
```

start-test

Syntax

`start-test`

Description

Starts the IP-SLA probes.

Command context

`config-ip-sla-<IP-SLA-NAME>`

Authority

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

Examples

```
switch(config)# ip-sla test
switch(config-ip-sla-test)# start-test
```

stop-test

Syntax

`stop-test`

Description

Stops the IP-SLA probes.

Command context

`config-ip-sla-<IP-SLA-NAME>`

Authority

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

Examples

```
switch(config)# ip-sla test
switch(config-ip-sla-test)# stop-test
```

tcp-connect

Syntax

```
tcp-connect {<DEST-IPV4-ADDR> | <HOSTNAME>} <PORT-NUM> [source {<SOURCE-IPV4-ADDR> |
     <IFNAME>} [source-port <PORT-NUM>]] [name-server <IPV4-ADDR-DNS-SERVER>]
     [probe-interval <PROBE-INTERVAL>]
```

Description

Configures TCP connect as the IP-SLA test mechanism. Requires destination address/hostname and destination port for the IP-SLA of tcp-connect IP-SLA type.

Command context

`config-ip-sla-<IP-SLA-NAME>`

Parameters

{*<DEST-IPV4-ADDR>* | *<HOSTNAME>*}

Selects the destination IPv4 address for the IP-SLA or the hostname of the destination.

<PORT-NUM>

Destination port for the IP-SLA. 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.

[source-port *<PORT-NUM>*]

Specifies the port for the IP-SLA test.

[name-server *<IPV4-ADDR-DNS-SERVER>*]

Specifies the DNS server for destination hostname resolution.

[probe-interval *<PROBE-INTERVAL>*]

Probe interval in seconds. Range: 30 to 604800.

Authority

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

Examples

```
switch(config-ipsla-1)# tcp-connect 2.2.2.2 8080
       switch(config-ipsla-1)# tcp-connect 2.2.2.2 8080 source 2.2.2.1 source-port 6000
       switch(config-ipsla-1)# tcp-connect 2.2.2.2 8080 source 1/1/1 source-port 6000

       switch(config-ipsla-1)# tcp-connect https://device.arubanetworks.com 8080
       switch(config-ipsla-1)# tcp-connect https://device.arubanetworks.com 8080 source 2.2.2.1 source-port 6000
```

```
switch(config-ipsla-1)# tcp-connect https://device.arubanetworks.com 8080 source 1/1/1 source-port 6000
switch(config-ipsla-1)# tcp-connect https://device.arubanetworks.com 8080 name-server 10.10.10.2
```

udp-echo

Syntax

```
udp-echo {<DEST-IPV4-ADDR>|<HOSTNAME>} <PORT-NUM> [source {<SOURCE-IPV4-ADDR> |
    <IFNAME>} [source-port <PORT-NUM>]] [name-server <IPV4-ADDR-DNS-SERVER>] [payload-size
    <PAYLOAD-SIZE>] [tos <TYPE-OF-SERVICE>] [probe-interval <PROBE-INTERVAL>]
```

Description

Configures UDP echo as the IP-SLA test mechanism. Requires destination address/hostname and destination port number for the IP-SLA of udp-echo SLA type.

Command context

```
config-ip-sla-<IP-SLA-NAME>
```

Parameters

{*<DEST-IPV4-ADDR>* | *<HOSTNAME>*}

Selects the destination IPv4 address for the IP-SLA or the hostname of the destination.

<PORT-NUM>

Specifies the destination port for the IP-SLA. 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.

[source-port *<PORT-NUM>*]

Specifies source port for the IP-SLA test. Range: 1 to 65535.

[name-server *<IPV4-ADDR-DNS-SERVER>*]

Specifies the DNS server for destination hostname resolution.

[payload-size *<PAYLOAD-SIZE>*]

Specifies the payload size of an SLA probe. Range: 28 to 1440.

[*<TYPE-OF-SERVICE>*]

Type of service. Range: 0 to 255.

probe-interval *<PROBE-INTERVAL>*

Probe interval in seconds. Range: 5 to 604800.

Authority

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

Examples

```
switch(config-ipsla-1)# udp-echo 2.2.2.2 8080
    switch(config-ipsla-1)# udp-echo 2.2.2.2 8080 source 2.2.2.1
    switch(config-ipsla-1)# udp-echo https://device.arubanetworks.com 8080
    switch(config-ipsla-1)# udp-echo 2.2.2.2 8080 source 1/1/1
    switch(config-ipsla-1)# udp-echo 2.2.2.2 8080 source 2.2.2.1 payload-size 50
    switch(config-ipsla-1)# udp-echo 2.2.2.2 8080 source 1/1/1 payload-size 50
    switch(config-ipsla-1)# udp-echo 2.2.2.2 8080 payload-size 50
    switch(config-ipsla-1)# udp-echo https://device.arubanetworks.com 8080 source 2.2.2.1
```

```
    payload-size 50
switch(config-ipsla-1)# udp-echo https://device.arubanetworks.com 8080 source 1/1/1
    payload-size 50
switch(config-ipsla-1)# udp-echo https://device.arubanetworks.com 8080
    name-server 10.10.10.2
```

udp-jitter-voip

Syntax

```
udp-jitter-voip {<DEST-IPV4-ADDR> | <HOSTNAME>} <PORT-NUM> [codec-type <CODEC-TYPE>]
     [advantage-factor <VALUE>] [source {<SOURCE-IPV4-ADDR> | <IFNAME>} [source-port <PORT-NUM>]]
     [name-server <IPV4-ADDR-DNS-SERVER>][probe-interval <PROBE-INTERVAL>] [tos <TYPE-OF-SERVICE>]
```

Description

Configure UDP jitter voip as the IP-SLA test mechanism. Requires destination address/hostname and source address/interface for the IP-SLA of udp-jitter-voip IP-SLA type.

Command context

`config-ip-sla-<IP-SLA-NAME>`

Parameters

{*<DEST-IPV4-ADDR>*|*<HOSTNAME>*}

Selects the destination IPv4 address for the IP-SLA or the hostname of the destination.

<PORT-NUM>

Selects the port number for the IP-SLA. Range: 1 to 65535.

[codec-type *<CODEC-TYPE>*]

Selects the codec-type for the Voip IP-SLA test.

[advantage-factor *<ADVANTAGE-FACTOR>*]

Selects the value for the advantage factor. Default value is 0.

[source {*<SOURCE-IPV4-ADDR>* | *<IFNAME>*}]

Selects the source IPv4 address for SLA probes or the source interface to use for sending IP-SLA probes.

[source-port *<PORT-NUM>*]

Specifies the value of source port for the IP-SLA probes.

[name-server *<IPV4-ADDR-DNS-SERVER>*]

Specifies the DNS server for destination hostname resolution.

tos*<TYPE-OF-SERVICE>*

Specifies the type of service. Range: 0 to 255.

probe-interval *<PROBE-INTERVAL>*

Specifies the probe interval in seconds. Range: 120 to 604800.

Authority

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

Examples

```
switch(config-ipsla-1)# udp-jitter-voip  2.2.2.2 8080 advantage-factor 10 codec-
type g711a
    switch(config-ipsla-1)# udp-jitter-voip  2.2.2.2 8080 advantage-factor 10
codec-type g711a source 2.2.2.1
    switch(config-ipsla-1)# udp-jitter-voip  https://device.arubanetworks.com 8080
advantage-factor 10 codec-type g711a
    switch(config-ipsla-1)# udp-jitter-voip  2.2.2.2 8080 advantage-factor 10
codec-type g711a source 1/1/1
    switch(config-ipsla-1)# udp-jitter-voip  https://device.arubanetworks.com 8080
advantage-factor 10 codec-type g711a source 2.2.2.1
    switch(config-ipsla-1)# udp-jitter-voip  https://device.arubanetworks.com 8080
advantage-factor 10 codec-type g711a source 1/1/1
    switch(config-ipsla-1)# udp-jitter-voip  https://device.arubanetworks.com 8080
advantage-factor 10 codec-type g711a name-server 10.10.10.2 probe-interval 120
source 10.1.1.1 source-port 8888 tos 10
```

vrf

Syntax

`vrf <VRF-NAME>`

`no vrf [<VRF-NAME>]`

Description

Configures the VRF on which the SLA will send or receive packets. By default, the default VRF is used.

The `no` form of the command removes VRF from SLA.

Command context

`config-ip-sla-<IP-SLA-NAME>`

Parameters

<VRF-NAME>

Specifies a VRF name. Length: Default: default.

Authority

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

Examples

```
switch(config-ip-sla-test)# vrf ipslasrc
```

```
switch(config-ip-sla-test)# no vrf
```

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.

CAUTION: 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.

Mirroring statistics and sFlow

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.

Mirroring and sFlow configuration on the same port is supported.

Limitations

The following limitations apply when configuring multiple mirroring sessions on a switch:

- CPU generated packets egressing on a routed L3 interface will not be mirrored to the destination port.
- Untagged egress packets that get mirrored will have the native VLAN tag in the mirrored packet. These extra bytes can cause traffic loss at the mirror destination when running line rate traffic.
- True egress mirroring is not supported on 832x platforms. Egress mirroring takes place at the ingress. The packets that may get dropped at the egress might also have been mirrored at ingress. Traffic will be mirrored even before the policy actions are processed at the egress.
- Packets mirrored to CPU from a Layer-3 Route Only Port (ROP) will have a VLAN tag with the VLAN ID set to the internal VLAN ID assigned to that port.
- 832x platforms have 4 mirror ASIC resources that can be used among the different mirror sessions. Each direction in a mirror session will consume 1 mirror ASIC resource. Hence, a user can have up to 4 unidirectional mirror sessions or 2 bi-directional mirror sessions active at any given time. If there are no mirror ASIC resources available when attempting to enable a mirror session, the 'Operation Status' field of `show mirror` command for session ID will have the status set to 'platform_session_limit_reached.'
- The mirror destination port among the active mirror sessions must be unique i.e. 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.
- The interface/LAG used to transmit ERSPAN packets cannot be a source in *any* mirror session.
- The interface/LAG used to transmit ERSPAN packets must be unique per ERSPAN mirror session. If a change in the L3 topology causes multiple ERSPAN mirror sessions to use the same egress interface/LAG

to transmit the ERSPAN packets, then only one session will work. The other session(s) will go into an error state.

Mirroring commands

clear mirror

Syntax

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

Description

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

Command context

Manager (#)

Parameters

all

Specifies all configured sessions.

<SESSION-ID>

Specifies a numeric identifier for the session. Range: 1 to 4

Authority

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

Examples

Clearing mirror statistics for all configured mirror sessions:

```
switch# clear mirror all
```

Clearing mirror statistics for mirror session 1:

```
switch# clear mirror 1
```

comment

Syntax

```
comment <COMMENT>

no comment
```

Description

Specifies a descriptive comment for the mirroring session.

The no form of this command removes the comment.

Command context

config-mirror-<SESSION-ID>

Parameters

<COMMENT>

A comment string of up to 64 characters composed of letters, numbers, underscores, dashes, spaces, and periods.

Authority

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

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:

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

Removing the comment for mirroring session 3:

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

copy tshark-pcap

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<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.

Authority

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

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.
```

destination cpu

Syntax

```
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.

Command context

`config-mirror-<SESSION-ID>`

Authority

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

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
```

destination interface

Syntax

```
destination interface {<INTERFACE-ID>|<LAG-NAME>}

no destination interface
```

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.

Command context

`config-mirror-<SESSION-ID>`

Parameters

<INTERFACE-ID>

Specifies a interface. Format: `member/slot/port`.

<LAG-NAME>

Specifies a LAG (link aggregation group) identifier.

Authority

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

Usage

Only one destination is allowed per session.

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
```

destination tunnel

Syntax

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.

NOTE: 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.

Command context

`config-mirror-<SESSION-ID>`

Authority

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

Parameters

<TUNNEL-IPV4-ADDR>

Specifies the tunnel address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<SOURCE-IPv4-ADDR>

Specifies the source address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<DSCP-VALUE>

Specifies the DSCP value to be carried within the DS field of ERSPAN packet header. Range: 0 to 63. Default: 0.

<VRF-NAME>

Specifies a VRF name. Default: default.

Examples

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

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

Replacing the existing tunnel destination:

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

Replacing the existing destination with a different DSCP value:

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

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
```

diagnostic

Syntax

```
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.

NOTE: 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.

Command context

Manager (`#`)

Parameters

`file`

Saves captured packets to a temporary file.

`delete-file`

Deletes the most recent captured file.

Authority

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

Example

Performing diagnostic:

```
switch# diagnostic

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

disable

Syntax

```
disable
```

Description

Disables the mirroring session specified by the current command context.

Command context

`config-mirror-<SESSION-ID>`

Authority

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

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
```

enable

Syntax

`enable`

Description

Enables the mirroring session for the current command context.

Command context

`config-mirror-<SESSION-ID>`

Authority

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

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.

NOTE: 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
```

mirror session

Syntax

```
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.

Command context

```
config
```

Parameters

<SESSION-ID>

Specifies the session identifier. Range: 1 to 4

Authority

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

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)#
```

show mirror

Syntax

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

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.

Command context

Operator (>) or Manager (#)

Parameters

<SESSION-ID>

Specifies the session identifier. Range: 1 to 4

[vsx-peer]

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

Authority

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

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#
```

source interface

Syntax

```
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.

Command context

`config-mirror-<SESSION-ID>`

Parameters

<PORT-NUM>

Specifies a physical port on the switch. Use the format `member/slot/port` (for example, `1/3/1`).

<LAG-NAME>

Specifies the identifier for the LAG (link aggregation group).

<DIRECTION>

Selects the direction of traffic to be mirrored from this source interface. There is no default for this parameter. Valid values are the following:

both

Mirror both transmitted and received packets.

rx

Mirror only received packets.

tx

Mirror only transmitted packets.

Authority

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

Usage

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

NOTE: 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
```

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

Ports default to an unsplit state. When a port is 'split', the split interfaces become active and can be configured independently. For example, when a 40G QSFP+ port is split four ways, each split interface behaves like a separate 10G SFP+ port. The split interfaces have the same name as the base port with an added suffix to represent their lane of the breakout cable. Splitting an interface removes most of the port's configuration settings and makes it inactive. The port will no longer appear in many show interface commands and most configuration commands are not allowed.

The same thing happens in reverse when an interface is unsplit. However, note that the 'split' and 'no split' commands are always performed in the unsplit port's context. After splitting a port, a reboot is required to complete the process. On a chassis system, just the line modules of all newly split ports can be rebooted Otherwise, the entire system must be rebooted. Until the reboot, split interfaces can continue to be configured, but will remain in a 'down' state.

Limitations with split hydra cable support

- The 8400 switch does not support DAC breakout cables, only optical breakout cables.
- The JL365A module does not support Priority-Based Flow Control (PFC) on split ports.
- The JL366A module does not support 100G breakout cables.
- The JL720A module does not support split ports.

Split hydra cable support commands

split

Syntax

```
split [confirm]

no split [confirm]
```

Description

Splits a port into multiple interfaces. Only ports capable of supporting breakout cables, also known as splitter or Hydra cables, can be split.

Command context

```
config-if
```

Parameters

confirm

Specifies the confirmation of port splitting.

Authority

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

Usage

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

Model	Switch	Ports
JL479A	Aruba 8320 48 10/6 40 X472 5 2 Bdl	49-54 (40G)
JL579A	Aruba 8320 32 40G X472 5 2 Bdl	5-28 (40G - center 24 ports)
JL581A	Aruba 8320 48 T/6 40 X472 5 2 Bdl	49-54 (40G)
JL635A	Aruba 8325 48Y8C models (displayed by the CLI `show system`)	49-56 (40G or 100G)
JL624A	Aruba 8325-48Y8C FB 6 F 2 PS Bdl	49-56 (40G or 100G)
JL625A	Aruba 8325-48Y8C BF 6 F 2 PS Bdl	49-56 (40G or 100G)
JL626A	Aruba 8325-32C FB 6 F 2 PS Bdl	1-32 (40G or 100G)
JL627A	Aruba 8325-32C BF 6 F 2 PS Bdl	1-32 (40G or 100G)
JL636A	Aruba 8325 32C models (displayed by the CLI `show system`)	1-32 (40G or 100G)
JL717A	Aruba 8360-32Y4C (displayed by the CLI `show system`)	33-36
JL700A	Aruba 8360-32Y4C Prt2Pwr3F2PS Bdl	33-36
JL701A	Aruba 8360-32Y4C Pwr2Prt3F2PS Bdl	33-36
JL721A	Aruba 8360-12C (displayed by the CLI `show system`)	1-12
JL718A	Aruba 8360 16Y2C (displayed by the CLI `show system`)	17-18
JL702A	Aruba 8360-16Y2C Pwr2Prt3F2PS Bdl	17-18
JL703A	Aruba 8360-16Y2C Prt2Pwr3F2PS Bdl	17-18
JL721A	Aruba 8360-12C (displayed by the CLI `show system`)	1-12
JL708A	Aruba 8360-12C Pwr2Prt3F2PS Bdl	1-12
JL709A	Aruba 8360-12C Pwr2Prt3F2PS Bdl	1-12
JL722A	Aruba 8360 24XF2C (displayed by the CLI `show system`)	25-26
JL710A	Aruba 8360-24XF2C Prt2Pwr3F2PS Bdl	25-26
JL711A	Aruba 8360-24XF2C Prt2Pwr3F2PS Bdl	25-26
JL365A	Aruba 8400X 8p 40G QSFP+ Adv Mod	1-8 (40G)
JL366A	Aruba 8400X 6p 40G/100G QSFP28 Adv Mod	1-6 (100G split mode only) 40G split not supported

Examples

Splitting an interface:

```
switch(config-if)# interface 1/1/52
switch(config-if)# split

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

Continue (y/n)? y

switch(config-if)# show interface brief
-------------------------------------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason               Speed   Description
          VLAN                                                              (Mb/s)
```

```
--------------------------------------------------------------------------------------------------------------
1/1/52:1  --      routed QSFP+DA3x4     yes     down    Split reboot pending   --      --
1/1/52:2  --      routed QSFP+DA3x4     yes     down    Split reboot pending   --      --
1/1/52:3  --      routed QSFP+DA3x4     yes     down    Split reboot pending   --      --
1/1/52:4  --      routed QSFP+DA3x4     yes     down    Split reboot pending   --      --
```

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 *ArubaOS-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 ArubaOS-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 ArubaOS-CX switch by entering the **`snmp-server vrf`** 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.

logging

Syntax

```
logging {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}
     [udp [<PORT-NUM>] | tcp [<PORT-NUM>]] [include-auditable-events]
     [severity <LEVEL>] [vrf <VRF-NAME>]

no logging {<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}
     [udp [<PORT-NUM>] | tcp [<PORT-NUM>]] [severity <LEVEL>]
     [vrf <VRF-NAME>]

no logging
```

Description

Enables syslog forwarding to a remote syslog server.

The `no` form of this command disables syslog forwarding to a remote syslog server.

Command context

`config`

Parameters

{<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>}

Selects the IPv4 address, IPv6 address, or host name of the remote syslog server. Required.

[udp [<PORT-NUM>] | tcp [<PORT-NUM>]]

Specifies the UDP port or TCP port of the remote syslog server to receive the forwarded syslog messages.

udp [*<PORT-NUM>*]

Range: 1 to 65535. Default: 514

tcp [*<PORT-NUM>*]

Range: 1 to 65535. Default: 1470

include-auditable-events

Specifies that auditable messages are also logged to the remote syslog server.

severity *<LEVEL>*

Specifies the severity of the syslog messages:

- `alert`: Forwards syslog messages with the severity of `alert (6)` and `emergency (7)`.
- `crit`: Forwards syslog messages with the severity of `critical (5)` and above.
- `debug`: Forwards syslog messages with the severity of `debug (0)` and above.
- `emerg`: Forwards syslog messages with the severity of `emergency (7)` only.
- `err`: Forwards syslog messages with the severity of `err (4)` and above
- `info`: Forwards syslog messages with the severity of `info (1)` and above. Default.
- `notice`: Forwards syslog messages with the severity of `notice (2)` and above.
- `warning`: Forwards syslog messages with the severity of `warning (3)` and above.

vrf *<VRF-NAME>*

Specifies the VRF used to connect to the syslog server. Optional. Default: `default`

Authority

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

Examples

Enabling the syslog forwarding to remote syslog server 10.0.10.2:

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

Enabling the syslog forwarding of messages with a severity of `err (4)` and above to TCP port 4242 on remote syslog server 10.0.10.9 with VRF `lab_vrf`:

```
switch(config)# logging 10.0.10.9 tcp 4242 severity err vrf lab_vrf
```

Disabling syslog forwarding to a remote syslog server:

```
switch(config)# no logging
```

snmp-server community

Syntax

```
snmp-server community <STRING>

no snmp-server community <STRING>
```

Description

Adds an SNMPv1/SNMPv2c community string. A community string is a password that controls read access to the SNMP agent. A network management program must supply this name when attempting to get SNMP information from the switch. A maximum of 10 community strings are supported. Once you create your own community string, the default community string (`public`) is deleted.

The `no` form of this command removes the specified SNMPv1/SNMPv2c community string. When no community string exists, a default community string with the value `public` is automatically defined.

Command context

`config`

Parameters

<STRING>

Specifies the SNMPv1/SNMPv2c community string. Range: 1 to 32 printable ASCII characters, excluding space and question mark.

Authority

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

Examples

Setting the SNMPv1/SNMPv2c community string to **`private`**:

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

Removing SNMPv1/SNMPv2c community string **`private`**:

```
switch(config)# no snmp-server community private
```

snmp-server host

Syntax

```
snmp-server host <IPv4-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [vrf <VRF-NAME>]

no snmp-server host <IPv4-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [vrf <VRF-NAME>]

snmp-server host <IPv4-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [vrf <VRF-NAME>]

no snmp-server host <IPv4-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [vrf <VRF-NAME>]

snmp-server host <IPv4-ADDR> [trap version v3 | inform version v3] user <NAME>
[port <UDP-PORT>] [vrf <VRF-NAME>]

no snmp-server host <IPv4-ADDR> [trap version v3 | inform version v3] user <NAME>
[port <UDP-PORT>] [vrf <VRF-NAME>]
```

Description

Configures a trap/informs receiver to which the SNMP agent can send SNMP v1/v2c/v3 traps or v2c informs. A maximum of 30 SNMP traps/informs receivers can be configured.

The `no` form of this command removes the specified trap/inform receiver.

NOTE: Configuring `snmpv3 informs` is not supported.

Command context

`config`

Parameters

<IPv4-ADDR>

Specifies the IP address of a trap receiver in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255. You can remove leading zeros. For example, the address `192.169.005.100` becomes `192.168.5.100`.

`trap version` ***<VERSION>***

Specifies the trap notification type for SNMPv1 or v2c. Available options are: `v1` or `v2c`.

`inform version v2c`

Specifies the inform notification type for SNMPv2c.

`trap version v3`

Specifies the trap notification type for SNMPv3.

`user` ***<NAME>***

Specifies the SNMPv3 user name to be used in the SNMP trap notifications.

`community` ***<STRING>***

Specifies the name of the community string to use when sending trap notifications. Range: 1 - 32 printable ASCII characters, excluding space and question mark. Default: `public`.

<UDP-PORT>

Specifies the UDP port on which notifications are sent. Range: 1 - 65535. Default: 162.

`vrf` ***<VRF-NAME>***

Specifies the name of the VRF on which to send the notifications.

Authority

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

Examples

```
switch(config)# snmp-server host 10.10.10.10 trap version v1
switch(config)# no snmp-server host 10.10.10.10 trap version v1

switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public

switch(config)# snmp-server host 10.10.10.10 trap version v2c community public port 5000
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public port 5000

switch(config)# snmp-server host 10.10.10.10 trap version v2c community public port 5000 vrf default
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public port 5000 vrf default

switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public

switch(config)# snmp-server host 10.10.10.10 inform version v2c community public port 5000
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public port 5000

switch(config)# snmp-server host 10.10.10.10 inform version v2c community public port 5000 vrf default
```

```
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public port 5000 vrf default

switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin

switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin port 2000
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin port 2000
```

snmp-server vrf

Syntax

`snmp-server vrf <VRF-NAME>`

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

Description

Configures the VRF on which the SNMP agent listens for incoming requests. By default, the SNMP agent does not listen on any VRF.

The `no` form of this command stops the SNMP agent from listening for incoming requests on the specified VRF.

Command context

`config`

Parameters

<VRF-NAME>

Specifies the VRF on which the SNMP agent listens for incoming requests. The SNMP agent can listen on either the `mgmt` or `default` VRF. If configured for both, the SNMP agent listens on `default`, which has a higher priority.

Authority

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

Example

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

```
switch(config)# no snmp-server vrf default
```

snmpv3 context

Syntax

`snmpv3 context <NAME> vrf <VRF-NAME> [community <STRING>]`

`no snmpv3 context <NAME> [vrf <VRF-NAME>]`

Description

Creates an SNMPv3 context on the specified VRF.

The `no` form of this command removes the specified SNMP context.

Command context

`config`

Parameters

<NAME>

Specifies the name of the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark (?).

vrf *<VRF-NAME>*

Specifies the VRF associated with the context. Default: default.

community *<STRING>*

Specifies the SNMP community string associated with the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark. Default: public.

Authority

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

Examples

Creating an SNMPv3 context named **newContext**:

```
switch(config)# snmpv3 context newContext
```

Creating an SNMPv3 context named **newContext** on VRF **myVrf** and with community string **private**.

```
switch(config)# snmpv3 context newContext vrf myVrf community private
```

Removing the SNMPv3 context named **newContext** on VRF **myVrf**:

```
switch(config)# no snmpv3 context newContext vrf myVrf
```

snmpv3 user

Syntax

```
snmpv3 user <NAME> [auth <AUTH-PROTOCOL> auth-pass {plaintext | ciphertext}
<AUTH-PWORD> [priv <PRIV-PROTOCOL> priv-pass {plaintext | ciphertext} <PRIV-PWORD>] ]

no snmpv3 user <NAME> [auth <AUTH-PROTOCOL> auth-pass
<AUTH-PWORD> [priv <PRIV-PROTOCOL> priv-pass <PRIV-PWORD>] ]
```

Description

Creates an SNMPv3 user and adds it to an SNMPv3 context.

The `no` form of this command removes the specified SNMPv3 user.

Command context

`config`

Parameters

<NAME>

Specifies the SNMPv3 username. Range 1 - 32 printable ASCII characters, excluding space and question mark.

auth *<AUTH-PROTOCOL>*

Specifies the authentication protocol used to validate user logins. Available options are: `md5` or `sha`.

auth-pass {plaintext | ciphertext} *<AUTH-PWORD>*

Specifies the SNMPv3 user password. Range for `plaintext` is 8 - 32 printable ASCII characters, excluding space and question mark.

Range for `ciphertext` is 1 - 120 printable ASCII characters. This option is only used when copying user configuration settings between switches. It enables you to duplicate a user's configuration on another switch without having to know their password.

priv *<PRIV-PROTOCOL>*

Specifies the SNMPv3 security protocol (encryption method). Available options are: `aes` or `des`.

priv-pass {plaintext | ciphertext} *<PRIV-PWORD>*

Specifies the SNMPv3 user privacy passphrase. Range for `plaintext` is 8 - 32 printable ASCII characters, excluding space and question mark.

Range for `ciphertext` is 1 - 120 printable ASCII characters. This option is only used when copying user configuration settings between switches. It enables you to duplicate a user's configuration on another switch without having to know their password.

Authority

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

Examples

Defining an SNMPv3 user named **Admin** using **sha** authentication with the plaintext password **mypassword** and using **des** security with the plaintext password **myprivpass**:

```
switch(config)# snmpv3 user Admin auth sha auth-pass plaintext mypassword priv des priv-pass plaintext myprivpass
```

Removing an SNMPv3 user named `Admin`:

```
switch(config)# no snmpv3 user Admin
```

Defining an SNMPv3 user named **Admin** using **sha** authentication with the plaintext password **mypassword** and using **des** security with the plaintext password **myprivpass**:

```
switch(config)# snmpv3 user Admin auth sha auth-pass plaintext mypassword priv des priv-pass plaintext myprivpass
```

Copying an SNMP user from switch 1 to switch 2.

On switch 1, configure a user called **Admin**, then issue the `show running-config` command to display switch configuration settings. The snmpv3 user command uses the `ciphertext` option to protect the users's passwords.

```
switch1(config)# snmpv3 user Admin auth sha auth-pass plaintext mypassword
priv des priv-pass plaintext myprivpass
switch1(config)# exit
switch1# show running-config
Current configuration:
!
!Version ArubaOS-CX TL.10.00.0003-8017-gdeb0606~dirty
!
!
!
snmpv3 user Admin auth sha auth-pass ciphertext
AQBapZHf2d20GYr/xcGUzYzm0zjNf/4VKHtSqbNImqtfYbJYCgAAALkGFJVcSp3nZ3o=
priv des priv-pass ciphertext AQBapb0H2poBQKXPoVsC9L9qzZyfJQnzR7hmTr7LGsOsI7K3CgAAAKP98Rq2jfTrFwQ=
ssh server vrf mgmt
!
!
!
!
interface mgmt
    no shutdown
```

```
    ip dhcp
vlan 1
```

On switch 2, execute the snmpv3 user command that was displayed by `show running-config` on switch 1. This creates the user on switch 2 with the same configuration settings.

```
switch1(config)# snmpv3 user Admin auth sha auth-pass ciphertext
AQBapZHf2d20GYr/xcGUzYzm0zjNf/4VKHtSqbNImqtfYbJYCgAAALkGFJVcSp3nZ3o=
priv des priv-pass ciphertext AQBapb0H2poBQKXPoVsC9L9qzZyfJQnzR7hmTr7LGsOsI7K3CgAAAKP98Rq2jfTrFwQ=
```

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/**
Software licensing	**https://lms.arubanetworks.com/**
End-of-Life information	**https://www.arubanetworks.com/support-services/end-of-life/**
Aruba software and documentation	**https://asp.arubanetworks.com/downloads**

Accessing updates

To download product updates:

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/

IMPORTANT: 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.