AOS-CX 10.13 Diagnostics and Supportability Guide

8100, 83xx, 9300, 10000 Switch Series

Hewlett Packard Enterprise

Published: October 2024
Version: 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.

Contents

Chapter 1
About this document

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

Applicable products

This document applies to the following products:

- Aruba 8100 Switch Series (R9W94A, R9W95A, R9W96A, R9W97A)
- Aruba 8320 Switch Series (JL479A, JL579A, JL581A)
- Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- Aruba 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL700C, JL701C, JL702C, JL703C, JL706C, JL707C, JL708C, JL709C, JL710C, JL711C, JL704C, JL705C, JL719C, JL718C, JL717C, JL720C, JL722C, JL721C)
- Aruba 9300 Switch Series (R9A29A, R9A30A, R8Z96A)
- Aruba 10000 Switch Series (R8P13A, R8P14A)

Latest version available online

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

Command syntax notation conventions

Convention	Usage
`example-text`	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (**[ ]**).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *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.

Convention	Usage
|	Vertical bar. A logical **OR** that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[ ]	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

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

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

Understanding the CLI prompts

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

```
switch>
```

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

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

switch(*CONTEXT-NAME*)#

Indicates the configuration context for a feature. For example:

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

Identifies the **interface** context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

On the 83xx, 9300, and 10000 Switch Series

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

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

If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split to 4 x 10G or 4 x 25G. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

Chapter 2
Debug logging

The debug logging framework provides an improved, customizable, and conditional logging framework with feature and entity based filtering options. Debug logging is a verbose, on-demand logging mechanism which customers and support can enable in order to obtain more information that will assist with troubleshooting.

Each debug logging event has both a Severity and a Module. Customers/support are required to enable a given Module in order to have those events logged. The log operation is not run when a Module is not enabled. All debug log events classified with a Severity of Error and above will always be logged. This ensures that both support and customers will be able to see these important events even when their respective debug log Module isn't enabled.

Debug logging is disabled by default.

Debug logging commands

clear debug buffer

```
clear debug buffer
```

Description

Clears all debug logs. Using the **show debug buffer** command will only display the logs generated after the **clear debug buffer** command.

Examples

Clearing all generated debug logs:

```
switch# show debug buffer
------------------------------------------------------------------------------
----------------------------
show debug buffer
------------------------------------------------------------------------------
----------------------------
2018-10-14:09:10:58.558710|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_CONFIG|No Port cfg
changes
2018-10-14:09:10:58.558737|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_EVENT|lldpd_stats_run
entered at time 8257199
2018-10-14:09:10:58.569317|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_CONFIG|No Port cfg
changes
2018-10-14:09:11:21.881907|hpe-sysmond|LOG_INFO|MSTR||SYSMON|SYSMON_CONFIG|Sysmon
poll interval changed to 32


switch# clear debug buffer
switch# show debug buffer
------------------------------------------------------------------------------
----------------------------
```

```
show debug buffer
------------------------------------------------------------------------------
----------------------------
2018-10-14:09:13:24.481407|hpe-sysmond|LOG_INFO|MSTR||SYSMON|SYSMON_CONFIG|Sysmon
poll interval changed to 51
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

debug {all | <MODULE-NAME>}

```
debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] [severity
   (emer|crit|alert|err|notice|warning|info|debug)] {port <PORT-NAME> |
    vlan <VLAN-ID> | ip <IP-ADDRESS> | mac <MAC-ADDRESS> |
    vrf <VRF-NAME> | instance <INSTANCE-ID>}
no debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] {port | vlan | ip | mac |
    vrf | instance}
```

Description

Enables debug logging for modules or submodules by name, with optional filtering by specific criteria. The **no** form of this command disables debug logging.

Parameter	Description
`all`	Enables debug logging for all modules.
<MODULE-NAME>	Enables debug logging for a specific module. For a list of supported modules, enter the **debug** command followed by a space and a question mark (?).
<SUBMODULE-NAME>	Enables debug logging for a specific submodule. For a list of supported submodules, enter the **debug** ***<MODULE-NAME>*** command followed by a space and a question mark (?).
`severity (emer|crit|alert|err| notice|warning|info|debug)`	Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is **debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and

Parameter	Description
	above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.
`debug`	Specifies storage of debug logs with severity level of **debug** (default).
`port`	Displays debug logs for the specified port, for example **1/1/1**.
`vlan <VLAN-ID>`	Displays debug logs for the specified VLAN. Provide a VLAN from 1 to 4094.
`ip <IP-ADDRESS>`	Displays debug logs for the specified IP Address.
`mac <MAC-ADDRESS>`	Displays debug logs for the specified MAC Address, for example **A:B:C:D:E:F**.
`vrf <VRF-NAME>`	Displays debug logs for the specified VRF.
`instance <INSTANCE-ID>`	Displays debug logs for the specified instance. Provide an instance ID from 1 to 255.

Examples

```
switch# debug all
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

debug db

```
debug db {all | sub-module} [level <MINIMUM-SEVERITY>] [filter]

no debug db {all | sub-module} [level <MINIMUM-SEVERITY>] [filter]
```

Description

Enables or disables debug logging for a db module or submodules, with an option to filter by specific criteria.

The **no** form of this command disables debug logging for the db module or submodule.

Parameter	Description
`all`	Enables all submodules for the db log.
`sub-module`	Enables debug logging for supported submodules. Specify **rx** or **tx** debug logs.
`filter`	Specifies supported filters for the db log. Specify **table**, **column**, or **client**. Optional
`severity (emer|crit|alert|err| notice|warning|info|debug)`	Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is **debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.
`debug`	Specifies storage of debug logs with severity level of **debug** (default).

Usage

DBlog is a high performance, configuration, and state database server logging infrastructure where a user can log the transactions which are sent or received by clients to the configuration and state database server. It can be enabled through the CLI and REST, and also supports filters where a user can filter out logs on the basis of table, column, or client. It is helpful for debugging when the user wants to debug an issue with a particular client, table, or column combination. It is not enabled by default. A combination of filters can also be applied to filter out messages based on table, column, and client.

There are three submodules for the "db" module:

1. **all**: When All is enabled, no filters are applied to any of the debug logs, even if other submodules are configured with filters.
2. **tx**: If enabled, only the replies and notifications sent out for the initial and incremental updates are logged.

3. **rx**: If enabled, only the transactions sent to the configuration and state database server are logged.

The keyword **all** may be used to enable or disable debug logging for all sub-modules. Also a combination of filters can be used to filter the message types.

If the table or client filter is applied, then the messages belonging to this specific table or client will be logged. The column filter can also be applied to further filter messages on a table, providing a mechanism to filter messages on a column. The table and client filter can be used in combination or separately, but column can only be used in conjunction with table.

Examples

Configuring all submodules with severity **debug**:

```
switch# debug db all severity debug
```

Configuring the **tx** submodule with **table Interface** filter and severity **debug**:

```
switch# debug db tx table Interface severity debug
```

Configuring the **rx** submodule with **table Interface column statistics** filter and severity **debug**:

```
switch# debug db rx table Interface column statistics severity debug
```

Disabling the **rx** submodule:

```
switch# no debug db rx
```

Disabling the **tx** submodule **table Interface**:

```
switch# no debug db tx table Interface
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

debug destination

```
debug destination {syslog | file | console | buffer} [severity
(emer|crit|alert|err|notice|warning|info|debug)]
no debug destination {syslog | file | console}
```

Description

Sets the destination for debug logs and the minimum severity level for each destination

The **no** form of this command unsets the destination for debug logs.

Parameter	Description
`{syslog | file | console | buffer}`	Selects the destination to store debug logs. Required.
`syslog`	Specifies that the debug logs are stored in the **syslog**.
`file`	Specifies that debug logs are stored in **file**.
`console`	Specifies that debug logs are stored in **console**.
`buffer`	Specifies that debug logs are stored in **buffer** (default).
`severity (emer|crit|alert|err| notice|warning|info|debug)`	Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is**debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.
`debug`	Specifies storage of debug logs with severity level of **debug** (default).

Usage

Events that have a severity equal to or higher than the configured severity level are stored in the designated destination. The product defaults to **buffer** for destination and **debug** as a severity level.

Examples

```
switch# debug destination syslog severity alert

switch# debug destination console severity info

switch# debug destination file severity warning
```

```
switch# debug destination buffer severity err
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show debug

```
show debug [vsx-peer]
```

Description

Displays the enabled debug types.

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

Examples

```
switch# show debug
-------------------------------------------------------------------------------
-
module sub_module severity vlan port    ip        mac               instance  vrf

-------------------------------------------------------------------------------
-
all     all          err    1   1/1/1   10.0.0.1  1a:2b:3c:4d:5e:6f  2
abcd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show debug buffer

```
show debug buffer [module <MODULE-NAME> | severity
(emer|crit|alert|err|notice|warning|info|debug)]
```

Description

Displays debug logs stored in the specified debug buffer with optional filtering by module or severity.

Parameter	Description
<MODULE-NAME>	Filters debug logs displayed by the specified module name.
`severity (emer|crit|alert|err| notice|warning|info|debug)`	Displays debug logs with a specified severity level. Defaults to**debug**. Optional.
`emer`	Displays debug logs with a severity level of **emergency** only.
`crit`	Displays debug logs with a severity level of **critical** and above.
`alert`	Displays debug logs with a severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Displays debug logs with a severity level of **warning** and above.
`info`	Displays debug logs with a severity level of **info** and above.
`debug`	Displays debug logs with a severity level of **debug** (default).

Examples

```
switch# show debug buffer

------------------------------------------------------------------------------
show debug buffer
------------------------------------------------------------------------------
2017-03-06:06:51:15.089967|hpe-sysmond|SYSMON|SYSMON_CONFIG|LOG_INFO|Sysmon poll
interval changed to 20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show debug destination

```
show debug destination [vsx-peer]
```

Description

Displays the configured debug destination and severity.

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

Examples

```
switch# show debug destination
------------------------------------------------------------------------
show debug destination
------------------------------------------------------------------------
 CONSOLE:info
 FILE:warning
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Chapter 3
Log Rotation

Log rotation provides you with the ability to systematically rotate and archive any log files produced by the system. Log rotation reduces log space required on the switch. Log rotation rotates and compresses the log files based on size and/or period. Rotated log files are stored locally or transferred to a remote host using TFTP.

Optionally, notifications can be triggered if a log buffer percent full threshold is exceeded, giving you the opportunity to save the logs elsewhere before the buffers are rotated with the oldest data being overwritten.

Log file paths

Logs stored in the following files are rotated:

- Audit logs are stored in file `/var/log/audit/audit.log`.
- Authentication logs are stored in file `/var/log/auth.log`.
- Event logs are stored in file `/var/log/event.log`.
- HTTPS server logs are stored in file `/var/log/nginx.log`.
- NTP logs are stored in file `/var/log/ntp.log`.
- Logs of bad login attempts are stored in `/var/log/btmp`.
- Logs of the last login sessions are stored in `/var/log/wtmp`.

About rotated log files

Rotated log files are compressed and stored locally in `/var/log/`, regardless of the remote host configuration. Rotated log files are stored with respective time extension to the granularity of hour in the format `file1-YYYYMMDDHH.gz` (for example, `messages-2015080715.gz`). Rotated log files are replaced when the number of old rotated log files exceeds three. The newly rotated log file replaces the oldest rotated log file.

TFTP, SFTP, or SCP are used to transfer rotated log files to a remote host. Only newly rotated log files are transferred to the remote host during the log rotation. Previously rotated log files are not re-transferred. After a log file is successfully transferred, it is removed from the switch.

Changing the size of the log rotation file

By default, the product rotates the log files when the maximum file size exceeds 100 MB. When the size of the log file exceeds the configured value, the rotation is triggered for that particular log file. Log rotation does not occur immediately after the maximum file size for the log file is reached since the cron job runs with an hourly periodicity.

`logrotate maxsize <10-200 MB>`

If you are planning to transfer the log rotation file by TFTP, set the log rotation file to no more than 32 MB.

Prerequisites

You must be in the configuration context:
`switch(config)#`

Changing the time frequency for log rotation

By default, the product rotates the log files daily. Enter the command at the configuration context in the CLI.

Prerequisites

You must be in the configuration context:
`switch(config)#`

Procedure

At the configuration context, enter:
`logrotate period {daily | hourly | weekly | monthly }`

daily: Rotates the log files daily. It is the default option.

hourly: Rotates the log files hourly.

weekly: Rotates the log files every week.

monthly: Rotates the log files every month.

Example command

```
switch(config)# logrotate period weekly
```

Resetting the time frequency to daily

Prerequisites

You must be in the configuration context:
`switch(config)#`

Procedure

At configuration context, enter the `no` form of the `logrotate period` command:

```
switch(config)# no logrotate period
```

Identifying a remote host for receiving rotated log files

You can send the rotated log files to a specified remote host Universal Resource Identifier (URI) by using the TFTP protocol. If no URI is specified, the rotated and compressed log files are stored locally in `/var/log/`. Only the TFTP protocol is supported for remote transfer, and the log rotation file cannot be more than 32 MB. Use the Linux TFTP command to transfer the file. Rotated log files are removed from the local path `/var/log/` when it is moved to TFTP server.

Prerequisites

You must be in the configuration context:
`switch(config)#`

Procedure

Provide the target IP address (IPv4 or IPv6) at the configuration context in the CLI:
`switch(config)# logrotate target {tftp://A.B.C.D | tftp://X:X::X:X}`

IPv4 Example

```
switch(config)# logrotate target tftp://192.168.1.132
```

IPv6 Example

```
switch(config)# logrotate target tftp://2001:db8:0:1::128
```

Remote transfer of rotated log files

Only the TFTP protocol is supported for remote transfer, and both IPv4 and IPv6 addresses are supported.

Only newly rotated log files are transferred to the remote host during the log rotation. Previously rotated log files are not transferred. After a file is successfully transferred, it is removed from the switch local path.

Packet level failures with TFTP are handled in the protocol itself. With each TFTP session failure, TFTP retries the file transfer three times. Retries have a timeout of five seconds.

Resetting the remote host for receiving rotated log files

Prerequisites

You must be in the configuration context:
`switch(config)#`

Procedure

At configuration context, enter the `no` form of the `logrotate target` command:

```
switch(config)# no logrotate target
```

Example:

```
switch(config)# logrotate target tftp://1.1.1.1
switch(config)# do show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
Target            : tftp://1.1.1.1
switch(config)# no logrotate target
switch(config)# do show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
switch(config)#
```

Resetting the size of the log rotation file

Prerequisites

You must be in the configuration context:
`switch(config)#`

Procedure

At configuration context, enter the `no` form of the `logrotate maxsize` command:

```
switch(config)# no logrotate maxsize
```

Verifying the log rotation parameters

At the command prompt, enter:
`switch# show logrotate`

Example output

```
switch# show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 10MB
switch#
```

Log rotation troubleshooting

Some common log file rotation troubleshooting items are as follows.

Log files not transferred remotely

Symptom

Rotated log files are not transferred to a remote host.

Cause

- The remote host might not be reachable.
- The TFTP server on the remote host might not have sufficient privileges for file creation.

Action

1. Verify that the remote host is reachable.
2. Ensure that the TFTP server is configured with the required file creation permissions.
3. For example, on the TFTPD-HPA server, change the configuration file in `/etc/default/tftpd-hpa` to include `-c` in `TFTP_OPTIONS`. (for example, `TFTP_OPTIONS="--secure -c`.).

Log rotation not occurring immediately after max file size

Symptom

Log rotation does not occur immediately after the maximum file size for the log file is reached.

Cause

The log rotation checks the size of the file on the first minute of every hour. If the maximum file size is reached in the meantime, the log rotation does not occur until the next hourly check of the file size.

Action

Log rotation is working as designed. The log rotation feature is designed to check the file size on an hourly basis.

Log rotation not occurring regardless of period

Symptom

Log rotation is not happening regardless of the `period` value.

Cause

Log files are not rotated when they are empty files (the log file size is zero).

Action

Log rotation occurs when the log file size is greater than zero.

Log rotation commands

logging threshold

```
logging threshold {audit-log | auth-log | commands-log |event-log |   | https-server-log}
<THRESHOLD%>
no logging threshold {audit-log | auth-log | commands-log | event-log |   | https-server-
log} [<THRESHOLD%>]
```

Description

Selects the logging buffer notification threshold for the specified logging buffer. Whenever the logging buffer space consumption exceeds the selected threshold (percent of buffer capacity), a LOG_BUFFER_ALMOST_FULL event and SNMP RMON trap is triggered. This gives you the opportunity to save the logs elsewhere before the buffers are rotated with the oldest data being overwritten.

Also, a LOG_BUFFER_WRAPPED event and SNMP RMON trap is triggered if the logging buffer capacity is fully consumed and the log buffer is rotated with the oldest data being overwritten.

The **no** form of this command resets the logging buffer warning threshold to its default. All logs except **audit-log** have a default of 90 (percent) and **audit-log** has a default of 50 (percent).

The largest REST payload that can be sent to RADIUS/TACACS servers is 1024 characters, and the maximum REST payload that can be sent to syslog servers is 3500 characters. Once this limit is exceeded, the log will display three dots (...) to indicate the the message has exceeded the character limit and is incomplete. .

Parameter	Description
`audit-log`	Selects the audit log.
`auth-log`	Selects the authentication log.
`commands-log`	Configure the logging threshold for commands log buffer
`event-log`	Selects the event log.
`https-server-log`	Selects the HTTPS server log.
`<THRESHOLD%>`	Selects the notification threshold as a percent that the selected logging buffer is full. Available percent values for all logs except `audit-log`: **`15 30 50 70 90 100`** Available percent values for `audit-log`: **`50 100`**

Examples

Setting the audit log threshold:

```
switch(config)# logging threshold audit-log 100
```

Setting the authentication log threshold:

```
switch(config)# logging threshold auth-log 50
```

Setting the event log threshold:

```
switch(config)# logging threshold event-log 70
```

Setting the HTTPS server log threshold:

```
switch(config)# logging threshold https-server-log 50
```

Resetting the audit log threshold to its default of 50:

```
switch(config)# no logging threshold audit-log
```

Resetting the authentication log threshold to its default of 90:

```
switch(config)# no logging threshold auth-log
```

Resetting the event log threshold to its default of 90:

```
switch(config)# no logging threshold event-log
```

Resetting the HTTPS server log threshold to its default of 90:

```
switch(config)# no logging threshold https-server-log
```

Command History

Release	Modification
10.11	Introduced the **commands-log** parameter.
10.09	Command introduced.

Command Information

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

logrotate maxsize

```
logrotate maxsize <MAX-SIZE>
no logrotate maxsize
```

Description

Specifies the maximum allowed log file size.

A log file that exceeds either the **logrotate maxsize** or the **logrotate period** (whichever happens first), triggers rotation of the log file.

The **no** form of this command resets the size of the log file to the default (100 MB).

Parameter	Description
<MAX-SIZE>	Specifies the allowed size the log file can reach before it is compressed and stored locally or transferred to a remote host. Range: 10 to 200 MB. Default: 100 MB.

Examples

Setting the maximum log file size:

```
switch(config)# logrotate maxsize 24
```

Resetting the maximum log file size to its default of 100 MB:

```
switch(config)# no logrotate maxsize
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

logrotate period

```
logrotate period {daily | hourly | monthly | weekly}
no logrotate period
```

Description

Sets the log file rotation time period. Defaults to daily.

A log file that exceeds either the **logrotate maxsize** or the **logrotate period** (whichever happens first), triggers rotation of the log file.

The **no** form of this command resets the log rotation period to the default of daily.

Parameter	Description
`daily`	Rotates log files on a daily basis (default) at 0:01.
`hourly`	Rotates log files every hour at the first second of the hour.
`monthly`	Rotates log files monthly on the first day of the month at 00:01.
`weekly`	Rotates log files once a week on Sunday at 00:01.

Examples

Setting a weekly period:

```
switch(config)# logrotate period weekly
```

Resetting the period to its default of daily:

```
switch(config)# no logrotate period
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

logrotate target

```
logrotate target <URI> [vrf <VRF_NAME>]
no logrotate target [<URI>] [vrf <VRF_NAME>]
```

Description

Using TFTP, sends the rotated log files to a specified remote host identified by Universal Resource Identifier (URI).

The **no** form of this command resets the target to the default, which stores the rotated and compressed log files locally in **/var/log/**.

Command context

Parameter	Description
`<URI>`	Specifies the URI of the remote host. The default directory is `local`.

Parameter	Description
	`tftp://{{<IPV4_ADDR>|IPV6_ADDR>}|HOST}[/<DIRECTORY>]`
`<VRF_NAME>`	Specifies the VRF name (Default: `default`).

Usage

- Rotated log files are compressed and stored locally in the path /var/log/ regardless of the remote host configuration.

Examples

Setting an IPv4 target:

```
switch(config)# logrotate target tftp://192.168.1.132
```

Setting an IPv4 target with a directory:

```
switch(config)# logrotate target tftp://192.168.1.132/logrotate/
```

Setting an IPv4 target with the default VRF:

```
switch(config)# logrotate target tftp://192.168.1.132 vrf mgmt
```

Setting an IPv6 target with the default VRF:

```
switch(config)# logrotate target tftp://2001:db8:0:1::128 vrf default
```

Resetting the target to local:

```
switch(config)# no logrotate target
```

Command History

Release	Modification
10.09	Updated the syntax and examples.
10.07 or earlier	--

Command Information

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

show logrotate

```
show logrotate [vsx-peer]
```

Description

Shows the log rotate configuration.

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

Examples

```
switch# show logrotate
Logrotate configurations :
Period            : weekly
Maxsize           : 20MB
Target            : tftp://2001:db8:0:1::128 vrf mgmt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Chapter 4
Reboot reasons

The **show boot-history** command displays the following reboot reasons for the management module:

Reboot reasons for management module

Figure 1 *Reboots handled through database*

Parameter	Description
Reboot requested by user	A user requested a switch reboot through the CLI or web UI.
Reset button pressed	The switch detected a short-press of the reset button.
Backplane fault	A backplane fault occured.
Configuration change	A configuration change resulted in a reboot.
Console error	Console failed to start.
Fabric fault	A fabric fault occurred.
All line modules faulted	A zero line card condition occurred.
Redundacy switchover requested	A user requested a redundancy switchover.
Redundant Management communication timeout	The standby management module has taken over from an unresponsive active management module.
Redundant Management election timeout	A failure to elect a standby management module in the alloted time.
Critical service fault (error)	A daemon critical to switch operation has stopped functioning. An extra error string may be present to describe the error in detail.
VSX software update	Reset triggered by a VSX software update.
Chassis critical temperature	Chassis operating temperature exceeded.
Chassis insufficient fans	Insufficient fans to cool the chassis.
Chassis unsupported PSUs/fans	Unsupported or misconfigured PSUs or system fans.
Management module critical temperature	Management module operating temperature exceeded.

Uncontrolled reboots

- ops-switchd crashed
- ovsdb-server crashed
- Reset
  - Software thermal reset
  - Power on reset
  - Watchdog reset
  - CPU request reset
  - cold reset
  - Long press reset
  - Jumper reset

  

  The resets are not applicable for 8320, 8325, and 9300 Switch series.
- switchd_agent crashed

Chapter 5
Event Logs

Event logging logs events generated by daemons, processes, and plug-ins running within the switch software. The event logging framework captures the event logs in a system journal by updating the journal fields and meta data.

Showing and clearing events

The `clear events` command is used to clear the event log of all events. The `show events` command is used to show all event logs generated by the switch since the last reboot. See the *Switch system and hardware commands chapter* chapter of the Fundamentals Guide for information on these commands.

The time stamp for event log messages generated from the Service OS indicates when the event log messages were transferred to the event log after a switch boot and not when the issue occurred.

See the *Security Guide* for information about accounting logs.

Chapter 6
Client Filter

Event log client filter provides the ability to filter event logs for specific IP or MAC addresses. This enables the REST client to query event logs from the switch's journal while filtering for IP or MAC address values.

New keys for IP and MAC addresses are added to the switch's journal of pre-existing keys (for example ID and Category).

Log messages

Log messages are generated to record various events occurring within the system. Each message contains a unique ID to represent an event and its attributes such as category, module ID or module role. The unique ID can then be used to filter for specific event types from a switch's journal.

- REST API can filter for ***all*** events occurring on a specific IP or MAC address.
- REST API can filter for a ***specific*** event occurring on a specific IP or MAC address.
- REST API can filter for events based on a list of IPs and MACs.

Event log client filter does not support Go language daemons. Only C daemons are supported.

Chapter 7
Network Configuration Validator

Network configuration validator (NCV) is a configuration troubleshooting tool that helps to detect switch configuration anomalies using a set of feature configuration templates. NCV helps to detect misconfigurations, identity incomplete or inter-dependent configurations, and mutually exclusive configurations.

NCV only displays possible warnings and does not recommend any configuration changes. NCV does not detect configuration issues based on network topologies.

Showing and clearing events

The `clear events` command is used to clear the event log of all events. The `show events` command is used to show all event logs generated by the switch since the last reboot. See the *Switch system and hardware commands chapter* chapter of the Fundamentals Guide for information on these commands.

The time stamp for event log messages generated from the Service OS indicates when the event log messages were transferred to the event log after a switch boot and not when the issue occurred.

See the *Security Guide* for information about accounting logs.

Network configuration validation commands

switch config-validator

```
switch config-validator [config <CONFIG-NAME>] [feature <feature>] [mode {consistency | vsx-sync}] [format {cli | json}]
```

Description

Runs configuration validation to detect configuration anomalies.

Parameter	Description
config	Specifies configuration to be validated. The default configuration is **running-config**.
feature <feature>	Specifies the name of the feature to be validated.
mode	Specifies configuration validation mode. The default is **consistency**.
consistency	Validates feature configuration for consistency check.
vsx-sync	Validates VSX configuration synchronization between VSX peers for VSX enabled features.
format	Specifies the results display format. The default is **cli**.

Examples

Running configuration validation with switches for the vsx feature.

```
switch (config)# switch config-validator config running-config feature vsx
Line number 36: Configuration `system-mac <VSX_SYSTEM_MAC>` is recommended
Line number 36: Multi chassis configuration is recommended for VSX redundancy
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8325 8360 9300 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

Chapter 8
Cable Diagnostics

The Time-Domain Reflectometer (TDR) feature helps characterize and locate cable faults in an Ethernet cable. TDR involves showing a reflection at any impedance change within the cable when a low voltage pulse is sent into the cable. TDR measures the time between release and return of the low voltage pulse from any reflections. The distance to the reflection can be calculated by measuring the time and the transmission velocity of the pulse.

TDR or Cable Diagnostics is a port feature supported on some switches running AOS-CX software. TDR is used to detect cable faults on the following ports:

Table 1: *Cable fault detection on supported ports types*

Platforms	1GbT	5G-SmartRate	10G-SmartRate
8360 (Supported only on JL720A and JL720C)	-	-	Yes

From AOS-CX 10.11, TDR or Cable Diagnostics can also be run from CX API.

How TDR works on AOS-CX platforms

The implementation of TDR in AOS-CX platforms is dependent on the physical layer chips (PHYs) that are part of the front-end network ports hardware. AOS-CX switches activate TDR on the PHY when a user enters the `diag cable-diagnostic` command. The switch waits for the report about TDR measurements from the PHY. The switch then reads the results and reports the values to the user.

Cable diagnostics tests

The cable diagnostics test will bring down the link, which will take more time to complete the test.

The TDR cable diagnostic test allows an operator to test twisted pair cables for faults without physically disconnecting the cables from the switch. It helps in troubleshooting connectivity or monitoring performance on one or more switch ports.

The `diag cable-diagnostic` command can be used to run cable diagnostic tests and display the test results.

The following table provides the cable status messages and their descriptions.

Status	Meaning
`good`	The MDI pair is good.

Status	Meaning
`open`	The MDI pair is not terminated with a link partner or has an open circuit.
`intra-short`	The MDI pair is shorted within itself.
`inter_short`	The MDI pair is shorted with another pair.
`high_imp`	The MDI pair has high-impedance mismatch and is not guaranteed to link up.
`low_imp`	The MDI pair has low-impedance mismatch and is not guaranteed to link up.
`unknown`	The MDI pair has failed the cable diagnostic test.

The following table provides the possible cable diagnostic failure reasons for port types.

Port Type	Reasons
1GbT	Interface is busy
5G-SmartRate	Interface is busy
10G-SmartRate	Interface is busy

The following table provides the cable length accuracy for port types.

Port Type	Reasons
1GbT	When diagnostic status is "good", cable length is reported.
5G-SmartRate	When diagnostic status is "good", cable length is not reported.
10G-SmartRate	When diagnostic status is "good", cable length is not reported.

The following table provides the distance to fault accuracy for port types.

Port Type	Reasons
1GbT	When diagnostic status is not "good" or "failed", distance to fault is reported within +/-10m.
5G-SmartRate	When diagnostic status is not "good" or "failed", distance to fault is reported within +/-5m.
10G-SmartRate	When diagnostic status is not "good" or "failed", distance to fault is reported within +/-5m.

Cable diagnostic commands

diag cable-diagnostic

```
diag cable-diagnostic
   test <IF-NAME>
   show <IF-NAME>
   clear <IF-NAME>
```

Description

Provides information about the cable health after running a diagnostic test on an interface.

If you run a new cable diagnostic command when a cable diagnostic is in progress for the interface, the new cable diagnostic command fails to execute. In such a scenario, an error message is displayed.

On executing a cable diagnostic test command, it automatically clears the old test results before the new test starts.

Parameter	Description
<IF-NAME>	Specifies the name of the interface.
`test` *<IF-NAME>*	Runs a cable diagnostic test on an interface.
`show` *<IF-NAME>*	Displays the diagnostic test result for an interface.
`clear` *<IF-NAME>*	Clears the cable diagnostic test results for an interface.

Examples

The following example displays running a cable diagnostic test on interface `1/3/1`:

```
switch# diag cable-diagnostic test 1/3/1
This command will cause a loss of link on the port under test and will take
several seconds to complete.
Continue (y/n)? y
```

The following example displays the error message on executing a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic test 1/3/1
A cable diagnostic test for interface 1/3/1 is already in progress.
```

The following example displays the error message when cable diagnostic test is requested for an unsupported port:

```
switch# diag cable-diagnostic test 1/3/1
Cable diagnostic is not supported on interface 1/3/1.
```

The following examples display the cable diagnostic test result for 1GbT interface:

```
switch# diag cable-diagnostic show 1/3/1
                          Cable         Impedance    Distance*    MDI
Interface        Pinout   Status        (Ohms)       (Meters)     Mode
```

```
-----------------------------------------------------------------------
1/3/1            1-2      good         85-115       10 +/- 10  mdi
(1GbT)           3-6      good         85-115       10 +/- 10  mdi
                 4-5      good         85-115        5 +/- 10  mdi
                 7-8      good         85-115        3 +/- 10  mdi

* Full cable length for good cables or distance to fault for faulty cables.

Cable status legend (1GbT):

Cable        Impedance
Status       (Ohms)     Description
-----------------------------------------------------------------
good         85-115     No cable faults found
open         >115       Open circuit detected
intra-short  <85        Short circuit within the same wire pair
inter-short  <85        Short circuit with another wire pair
high-imp     >115       Cable impedance higher than expected
low-imp      <85        Cable impedance lower than expected
unknown      --         Cable test inconclusive
```

The following examples display the cable diagnostic test result for 5G-SmartRate interface:

```
switch# diag cable-diagnostic show 1/1/20
                         Cable        Impedance   Distance*   MDI
Interface        Pinout  Status       (Ohms)      (Meters)    Mode
-----------------------------------------------------------------------
1/1/20           1-2     good         85-115         --       mdi
(5G-SmartRate)   3-6     open         >300          4 +/- 5   mdi
                 4-5     open         >300          4 +/- 5   mdi
                 7-8     high-imp     >115          3 +/- 5   mdi

* Full cable length for good cables or distance to fault for faulty cables.

Cable status legend (5G-SmartRate):

Cable        Impedance
Status       (Ohms)     Description
-----------------------------------------------------------------
good         85-115     No cable faults found
open         >300       Open circuit detected
intra-short  <30        Short circuit within the same wire pair
inter-short  <30        Short circuit with another wire pair
high-imp     >115       Cable impedance higher than expected
low-imp      <85        Cable impedance lower than expected
unknown      --         Cable test inconclusive
```

The following example displays the error message when you execute a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic show 1/3/1
A cable diagnostic test for interface 1/3/1 is currently in progress.
```

The following example displays the error message when cable diagnostic test result is not available:

```
switch# diag cable-diagnostic show 1/3/1
Cable diagnostic test results for interface 1/3/1 are not available.
```

The following example clears the cable diagnostic test results for the specified interface:

```
switch# diag cable-diagnostic clear 1/3/1
```

The following example displays the error message when you execute a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic clear 1/3/1
A cable diagnostic test for interface 1/3/1 is currently in progress.
```

Running a cable diagnostic test will result in a brief interruption in connectivity on all tested ports.

Command History

Release	Modification
10.11	Command introduced.

Command Information

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

Chapter 9
Supportability Copy

To effectively diagnose various issues arising at the switch, different types of data are copied out using copy commands for further analysis.

Use the `copy core-dump` command to copy the core-dump of a daemon crash.

Use the `copy show-tech` command to capture the status of the feature.

If there is feature misbehavior, use the `copy support-files feature` command to copy all feature related information for further analysis. Additionally use `copy support-log` and `copy diag-dump` to copy information that helps to analyze the internal behavior of a feature/daemon.

Use `copy command-output` to copy any `show` command's output to remote destinations or USB storage.

These files can be copied to a remote destination using sftp/tftp, additionally they can also be stored in the USB storage.

TFTP VxLAN Support

TFTP is supported over VxLAN tunnels with IPv4 or IPv6 underlay.

TFTP over VxLAN tunnels with IPv6 underlay is only supported on the Aruba 8100 and 8360 Switch Series.

Limitations

Running-config, check-point config and startup-config will not be copied fully to destination file in TFTP server (only partial configuration will be copied) even though TFTP shows the transfer was successful. This is because fragmentation/ressembly/MTU discovery are not supported on VxLAN paths. Packets exceeding 1500 bytes are dropped when the TFTP transfer is done with default TFTP block size or default MTU size.

Workaround

Increase the MTU size (JUMBO) on all interfaces between the TFTP client and TFTP server or use a custom block size of 1375 or less for TFTP transfers.

Example of a custom blocksize configuration:

```
copy running-config tftp://72.1.1.100;blocksize=1374/runv4 cli vrf vrf1
copy running-config tftp://[20:2:100];blocksize=1374/runv6 cli vrf vrf1
```

Supportability copy commands

copy checkpoint

`copy checkpoint` *<CHECKPOINT-NAME>* {*<STORAGE-URL>* | *<REMOTE-URL>*}

Description

Copies the checkpoint using TFTP, SFTP, SCP, or USB.

Parameter	Description
<CHECKPOINT-NAME>	Specifies the checkpoint name.
{*<STORAGE-URL>* | *<REMOTE-URL>*}	Select either the storage URL or the remote URL for the destination of the copied command output. Required.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***

Examples

Copying checkpoint chpt to a remote URL:

```
switch# copy checkpoint chpt scp://root@10.0.1.1/config vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy command-output

```
copy command-output "<COMMAND>" {<STORAGE-URL> | <REMOTE-URL> [vrf <VRF-NAME>]}
```

Description

Copies the specified command output using TFTP, SFTP, SCP, or USB.

Parameter	Description
<COMMAND>	Specifies the command from which you want to obtain its output. Required. Users with auditor rights can specify these two commands only: **show accounting log**

Parameter	Description
	show events
{*<STORAGE-URL>* | *<REMOTE-URL>* [vrf *<VRF-NAME>*]}	Select either the storage URL or the remote URL for the destination of the copied command output. Required.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.

Examples

Copying the output from the **show events** command to a remote URL:

```
switch# copy command-output "show events" tftp://10.100.0.12/file
```

Copying the output from the **show tech** command to a remote URL with a VRF named *mgmt*:

```
switch# copy command-output "show tech" scp://user@10.100.0.12/file vrf mgmt
```

Copying the output from the **show tech** command to a remote URL with a VRF named *mgmt*:

```
switch# copy command-output "show tech" tftp://10.100.0.12/file vrf mgmt
```

Copying the output from the **show events** command to a file named **events** on a USB drive:

```
switch# copy command-output "show events" usb:/events
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy core-dump daemon

`copy core-dump daemon <DAEMON-NAME>[:<INSTANCE-ID>] <REMOTE-URL> [vrf <VRF-NAME>]`

Description

Copies the core-dump from the specified daemon using TFTP, SFTP, SCP, or USB.

Parameter	Description
<DAEMON-NAME>	Specifies the name of the daemon. Required.
[:*<INSTANCE-ID>*]	Specifies the instance of the daemon core dump. Optional.
<REMOTE_URL>	Specifies the remote destination URL. Required. The syntax of the URL is the following: Syntax: ■ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ■ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Examples

Copying the core dump from daemon ops-vland to a remote URL with a VRF named mgmt:

```
switch# copy core-dump daemon ops-vland sftp://abc@10.0.14.211/vland_coredump.xz
vrf mgmt
```

Copying the core dump from daemon ops-vland to a remote URL with a VRF named mgmt:

```
switch# copy core-dump daemon ops-vland scp://abc@10.0.14.211/vland_coredump.xz
vrf mgmt
```

Copying the core dump from daemon ops-switchd to a USB drive:

```
switch# copy core-dump daemon ops-switchd usb:/switchd
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

Platforms	Command context	Authority
8325 8360 9300 10000		

copy core-dump kernel

```
copy core-dump kernel <REMOTE-URL> [vrf <VRF-NAME>]
```

Description

Copies a kernel core dump using TFTP or SFTP.

Parameter	Description
<REMOTE-URL>	Specifies the URL to copy the command output. Required. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
`vrf` *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.

Examples

Copying the kernel core dump to the URL:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz
```

Copying the kernel core dump to the URL with the VRF named mgmt:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8360 9300 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

copy core-dump kernel *<STORAGE-URL>*

`copy core-dump kernel <STORAGE-URL>`

Description

Copies the kernel core dump to a USB drive.

Parameter	Description
<STORAGE-URL>	Specifies the USB to copy command output. Required. Syntax: **{usb}:/*<FILE>***

Examples

Copying the kernel core dump to a USB drive:

```
switch# copy core-dump kernel usb:/kernel.tar.gz
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8360 9300 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

copy core-dump dsm

`copy core-dump dsm <slot-id> <daemon-name>[:<instance-ID>]`

Description

Copies the core-dump from the selected distributed-services-module using TFTP, SFTP, SCP, or USB.

Parameter	Description
`<slot-id>`	Slot ID of the distributed services module
<DAEMON-NAME>	Specifies the name of the daemon. Required.
`[:`*<INSTANCE-ID>*`]`	Specifies the instance of the daemon core dump. Optional.
<REMOTE_URL>	Specifies the remote destination URL. Required. The syntax of the URL is the following:

Parameter	Description
	Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
`vrf <VRF-NAME>`	Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Examples

Copying the DSM core dump from daemon hpe-snmpd to a remote URL:

```
switch# copy core-dump dsm 1/1 daemon hpe-snmpd sftp://root@10.0.0.2/coredumpdsm
```

Command History

Release	Modification
10.09	Command introduced

Command Information

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

copy diag-dump feature *<FEATURE>*

`copy diag-dump feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

Description

Copies the specified diagnostic information using TFTP, SFTP, SCP, or USB.

Parameter	Description
`<FEATURE>`	The name of a feature, for example **aaa** or **vrrp**. Required.
`{<REMOTE-URL> [vrf <VRF-NAME> |<STORAGE-URL>]}`	Select either the remote URL or the storage URL for the destination of the copied command output. Required.
`<REMOTE-URL>`	Specifies the remote destination URL. Required. The syntax of the URL is the following: Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*} [:*<PORT>*]/*<FILE>***

Parameter	Description
`vrf <VRF-NAME>`	Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.
`<STORAGE-URL>`	Specifies the USB to copy command output. Required. Syntax: `{usb}:/<FILE>`

Examples

Copying the output from the aaa feature to a remote URL with a specified VRF:

```
switch# copy diag-dump feature aaa tftp://10.100.0.12/diagdump.txt vrf mgmt
```

Copying the output from the aaa feature to a remote URL with a specified VRF:

```
switch# copy diag-dump feature aaa scp://user@10.100.0.12/diagdump.txt vrf mgmt
```

Copying the output from the vrrp feature to a USB drive:

```
switch# copy diag-dump feature vrrp usb:/diagdump.txt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy diag-dump local-file

`copy diag-dump local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

Description

Copies the diagnostic information stored in a local file using TFTP, SFTP, SCP, or USB.

Parameter	Description
`{<REMOTE-URL> [vrf <VRF-NAME>] |<STORAGE-URL>}`	Select either the storage URL or the remote URL for the destination of the copied

Parameter	Description
	command output. Required.
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*} [:*<PORT>*]/*<FILE>***
`vrf` *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***

Usage

The **copy diag-dump local-file** command can be used only after the information is captured. Run the **diag-dump *<FEATURE-NAME>* basic local-file** command before you enter the **copy diag-dump local-file** command to capture the diagnostic information for the specified feature into the local file.

Examples

Copying the output from the local file to a remote URL:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file tftp://10.100.0.12/diagdump.txt
```

Copying the output from the local file to a remote URL:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file scp://user@10.100.0.12/diagdump.txt
```

Copying the output from the local file to a USB drive:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file usb:/diagdump.txt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy *<IMAGE>*

`copy <IMAGE> {<STORAGE-URL> | <REMOTE-URL>} <FILE-NAME> [vrf <VRF-NAME>]`

Description

Copies the image using TFTP, SFTP, SCP, or USB.

Parameter	Description
<IMAGE>	Specifies the image.
{*<STORAGE-URL>* | *<REMOTE-URL>*}	Select either the storage URL or the remote URL for the destination of the copied command output. Required.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
<FILE-NAME>	Specifies the file name.
vrf *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.

Examples

Copying the image to a remote URL:

```
switch# copy scp://root@20.0.1.1/primary.swi primary vrf mgmt
```

Copying the secondary image to a remote URL:

```
switch# copy secondary scp://root@20.0.1.1/primary.swi vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy running-config

```
copy running-config {<STORAGE-URL> | <REMOTE-URL>}/config <CONFIG-NAME> [vrf <VRF-NAME>]
```

Description

Copies the running configuration using TFTP, SFTP, SCP, or USB.

Parameter	Description
{<*STORAGE-URL*> | <*REMOTE-URL*>}	Select either the storage URL or the remote URL for the destination of the copied command output. Required.
<*STORAGE-URL*>	Specifies the USB to copy command output. Syntax: **{usb}:/<*FILE*>**
<*REMOTE-URL*>	Specifies the URL to copy the command output. Syntax: ▪ {tftp://}{<*IP*> | <*HOST*>}[:<*PORT*>] [;blocksize=<*VAL*>]/<*FILE*> ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
config <*CONFIG-NAME*>	Specifies the running configuration.
vrf <*VRF-NAME*>	Specifies the VRF name. The default VRF name is default. Optional.

Examples

Copying the running configuration to a remote URL:

```
switch# copy running-config scp://root@10.0.1.1/config cli vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy show-tech feature

`copy show-tech feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

Description

Copies show tech output using TFTP, SFTP, SCP, and USB.

Parameter	Description
`{<REMOTE-URL> [vrf <VRF-NAME> | <STORAGE-URL>]}`	Select either the remote URL or the storage URL for the destination of the copied command output. Required.
`<REMOTE-URL>`	Specifies the URL to copy the command output. Required. Syntax: ▪ **{tftp://}{<*IP*> | <*HOST*>}[:<*PORT*>] [;blocksize=<*VAL*>]/<*FILE*>** ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
`vrf <VRF-NAME>`	Specifies the VRF name. The default VRF name is default. Optional.
`<STORAGE-URL>`	Specifies the USB to copy command output. Required. Syntax: **{usb}:/<*FILE*>**

Example

Copying show tech output of the **aaa** feature using SCP:

```
switch# copy show-tech feature aaa scp://user@10.0.0.12/file.txt vrf mgmt
```

Copying show tech output of the `config` feature using SFTP on the `mgmt` VRF:

```
switch# copy show-tech feature config sftp://root@10.0.0.1/tech.txt vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy show-tech local-file

```
copy show-tech local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

Description

Copies show tech output stored in a local file.

Parameter	Description
{*<REMOTE-URL>* [vrf *<VRF-NAME>*] | *<STORAGE-URL>*]}	Select either the remote URL or the storage URL for the destination of the copied command output. Required.
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ■ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ■ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***

Usage

Before entering the **copy show-tech local-file** command, run the **show tech** command with the **local-file** parameter for the specified feature.

Examples

Copying the output to a remote URL:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt
```

Copying the output to a remote URL:

```
switch# copy show-tech local-file scp://user@10.100.0.12/file.txt
```

Copying the output to a remote URL with a VRF:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt vrf mgmt
```

Copying the output to a USB:

```
switch# copy show-tech local-file usb:/file
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy startup-config

`copy startup-config {<STORAGE-URL> | <REMOTE-URL>}/config <CONFIG-NAME> [vrf <VRF-NAME>]`

Description

Copies the running configuration using TFTP, SFTP, SCP, or USB.

Parameter	Description
{<*STORAGE-URL*> | <*REMOTE-URL*>}	Select either the storage URL or the remote URL for the destination of the copied command output. Required.
<*STORAGE-URL*>	Specifies the USB to copy command output. Syntax: **{usb}:/<*FILE*>**
<*REMOTE-URL*>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{<*IP*> | <*HOST*>}[:<*PORT*>][;blocksize=<*VAL*>]/<*FILE*>** ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
config <*CONFIG-NAME*>	Specifies the startup configuration.
vrf <*VRF-NAME*>	Specifies the VRF name. The default VRF name is default. Optional.

Examples

Copying the startup configuration to a remote URL:

```
switch# copy startup-config scp://root@10.0.1.1/config json vrf mgmt
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy support-files

```
copy support-files
   <REMOTE-URL> [vrf <VRF-NAME>]
   <STORAGE-URL>
   all <REMOTE-URL> [vrf <VRF-NAME>]
   all <STORAGE-URL>
   feature <FEATURE-NAME> <STORAGE-URL>
   previous-boot <REMOTE-URL> [vrf <VRF-NAME>]
   previous-boot <STORAGE-URL>
```

Description

Copies a set of support files to a compressed file in tar.gz format using TFTP, SFTP, SCP, or USB or to a directory over SFTP or USB.

Parameter	Description
<FEATURE-NAME>	The feature name, for example, `aaa`.
{*<REMOTE-URL>* [vrf *<VRF-NAME>*] | *<STORAGE-URL>*]}	Select either the remote URL or the storage URL for the destination of the copied command output. Required.
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. The default VRF name is default. Optional.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***

Usage

If feature name is not provided, the command collects generic system-specific support information. If a feature name is provided, the command collects feature-specific support information.

Examples

Copying the support files to a remote URL:

```
switch# copy support-files tftp://10.100.0.12/file.tar.gz
```

Copying the support files of the **lldp** feature to a remote URL with a specified VRF:

```
switch# copy support-files feature lldp tftp://10.100.0.12/file.tar.gz vrf mgmt
```

Copying the support files from the previous boot to a remote URL with a specified VRF:

```
switch# copy support-files previous-boot scp://user@10.0.14.206/file.tar.gz vrf
mgmt
```

Copying the support files to a USB:

```
switch# copy support-files usb:/file.tar.gz
```

Copying all the support files to a remote URL:

```
switch# copy support-files all sftp://root@10.0.14.216/file.tar.gz vrf mgmt
```

Copying the support files of the `config` feature to a USB:

```
switch# copy support-files feature config usb:/file.tar.gz
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

copy support-files local-file

`copy support-files [feature <FEATURE-NAME> | previous-boot | all ] local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

Description

Stores a set of support files as a compressed file in the switch locally and copies the preserved support files to a directory using TFTP, SFTP, SCP, or USB.

You can store only one copy of the support file locally. When you store a new support file, it overwrites the existing support file.

Parameter	Description
<FEATURE-NAME>	Specifies the feature for the support files.
<SLOT-ID>	Specifies the module slot number identifier for the support files. Range: 1/1-1/4, 1/7-1/10
<MEMBER-ID>	Specifies the VSF member identifier for the support files. Range: 1-10
<REMOTE-URL>	Specifies the URL to copy the support files.
<STORAGE-URL>	Specifies the USB to copy the support files.
<VRF-NAME>	Specifies the VRF name. The default VRF name is default.

Usage

If the copy of the support files to the destination fails, an alternate option is prompted to store the collected data in the local file. This helps us to retry the copy process using **copy support-files local-file *<REMOTE-URL/STORAGE-URL>*** without the need of regenerating the file.

Examples

Copying support file to the local file:

```
switch# copy support-files local-file
switch# copy support-files feature lldp local-file
switch# copy support-files previous-boot local-file
switch# copy support-files all local-file
The operation to copy all support files could take a while to complete.
Do you want to continue (y/n)?
```

Copying local support file to a remote URL and storage URL:

```
switch# copy support-files local-file usb:/support_files_dir_path/
switch# copy support-files local-file scp://root@10.0.14.206//support_files_dir_
path/abc.tar.gz vrf mgmt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy support-log

```
copy support-log <DAEMON-NAME> {<STORAGE-URL> | <REMOTE-URL> [vrf <VRF-NAME>]}
```

Description

Copies the specified support log for a daemon TFTP, SFTP, SCP, or USB.

Parameter	Description
<DAEMON-NAME>	Specifies the name of the daemon. Required.
{*<STORAGE-URL>* | *<REMOTE-URL>* [vrf *<VRF-NAME>*]}	Selects either the storage URL or the remote URL for the destination of the copied command output. Required.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Usage

Fast log is a high performance, per-daemon binary logging infrastructure used to debug daemon level issues by precisely capturing the per daemon/module/functionalities debug traces in real time. Fast log, also referred to as support logs, helps users to understand the feature internals and its specific happenings. The fast logs from one daemon are not overwritten by other daemon logs because fast logs are captured as part of a daemon core dump. Fast logs are enabled by default.

Examples

Copying the support log from the daemon hpe-fand to a remote URL:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file
```

Copying the support log from the daemon fand to a remote URL with a VRF named mgmt:

```
switch# copy support-log fand scp://user@10.100.0.12/file vrf mgmt
```

Copying the support log from the daemon hpe-fand to a remote URL with a VRF named mgmt:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file vrf mgmt
```

Copying the support log from the daemon hpe-fand to a USB:

```
switch# copy support-log hpe-fand usb:/support-log
```

Command History

Release	Modification
10.08	Added SCP support.
10.07 or earlier	--

Command Information

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

Chapter 10
Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Traceroute over VXLAN

Traceroute and traceroute6 are supported over VXLAN from VTEP to VTEP, VTEP to host, and host to VTEP over L2 VNI/L3 VNI. A unique IP on VTEP should be used as the traceroute source and destination. Both source and destination VTEPs require AOS-CX 10.8 or later for this feature to work. Traceroute and traceroute6 over VXLAN cannot be used to track the underlay hops between VTEPs.

Traceroute and traceroute6 are supported on all platforms with non-VXLAN.

Traceroute and traceroute6 are supported on all platforms with VXLAN IPv4 underlay support.

Traceroute and traceroute6 are supported on 6300, 6400, 8100, and 8360 with VXLAN IPv6 underlay.

Traceroute commands

traceroute

```
traceroute {<IPV4-ADDR> | <HOSTNAME>} [ip-option loosesourceroute <IPV4-ADDR>] [dstport
<NUMBER> | maxttl <NUMBER> | minttl <NUMBER> | probes <NUMBER> | timeout <TIME>] [vrf
<VRF-NAME>] source {<IPV4-ADDR> | <IFNAME>}
```

Traceroute over VXLAN with `ip-option loosesourceroute` on L3VNI is not supported.

Description

Uses traceroute for the specified IPv4 address or hostname with or without optional parameters.

Parameter	Description
`IPv4-address <IPV4-ADDR>`	Specifies the IPv4 address.
`hostname`	Specifies the hostname of the device to traceroute.
`ip-option`	Specifies the IP option.
`loosesourceroute <IPV4-ADDR>`	Specifies the route for loose source record route. Enter one or more intermediate router IP addresses separated by ',' for loose source routing.

Parameter	Description
`dstport <NUMBER>`	Specifies the destination port, <*1-34000*>. Default: 33434
`maxttl <NUMBER>`	Specifies the maximum number of hops to reach the destination, <*1-255*>. Default: 30
`minttl <NUMBER>`	Specifies the Minimum number of hops to reach the destination, <*1-255*>. Default: 1
`probes <NUMBER>`	Specifies the number of probes, <*1-5*>. Default: 3
`timeout <TIME>`	Specifies the traceroute timeout in seconds, <*1-60*>. Default: 3 seconds
`vrf <VRF-NAME>`	Specifies the virtual routing and forwarding (VRF) to use .
`source {<IPV4-ADDR> | <IFNAME>}`	Specifies the source IPv4 address or interface name.

Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Examples

```
switch# traceroute 10.0.10.1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute localhost
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   127.0.0.1  0.018ms  0.006ms  0.003ms

switch# traceroute 10.0.10.1 maxttl 20
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 3 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 minttl 1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
```

```
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 probes 2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 2
probes
  1   10.0.40.2  0.002ms  0.002ms
  2   10.0.30.1  0.002ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms

switch# traceroute 10.0.10.1 timeout 5
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 5 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute localhost vrf red
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   127.0.0.1  0.003ms  0.002ms  0.001ms

switch# traceroute localhost mgmt
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   127.0.0.1  0.018ms  0.006ms  0.003ms

switch# traceroute 10.0.10.1 maxttl 20 timeout 5 minttl 1 probes 3 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2 maxttl 20
timeout 5 minttl 1 probes 3 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3
probes
  1   10.0.40.2  0.002ms  0.002ms  0.001ms
  2   10.0.30.1  0.002ms  0.001ms  0.001ms
  3   10.0.10.1  0.001ms  0.002ms  0.002ms

switch# traceroute 10.0.0.2 source 10.0.0.1
traceroute to 10.0.0.2 (10.0.0.2), 30 hops max
  1   10.0.0.2  0.299ms  0.155ms  0.115ms

switch# traceroute 10.0.0.2 source 1/1/1
traceroute to 10.0.0.2 (10.0.0.2), 30 hops max
  1   10.0.0.2  0.479ms  0.222ms  0.171ms
```

Command History

Release	Modification
10.08	Added `source IP address` and `source interface name`

Release	Modification
	parameters.
10.07 or earlier	--

Command Information

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

traceroute6

```
traceroute6 {<IPV6-ADDR> | <HOSTNAME>} [dstport <NUMBER> | maxttl <NUMBER> | probes
<NUMBER> | timeout <TIME>] [vrf <VRF-NAME>] source {<IPV6-ADDR> | <IFNAME>}
```

Description

Uses traceroute for the specified IPv6 address or hostname with or without optional parameters.

Parameter	Description
`IPv6-address <IPV6-ADDR>`	Specifies the IPv6 address.
`hostname`	Specifies the hostname of the device to traceroute.
`dstport <NUMBER>`	Specifies the destination port, <*1-34000*>. Default: 33434
`maxttl <NUMBER>`	Specifies the maximum number of hops to reach the destination, <*1-255*>. Default: 30
`probes <NUMBER>`	Specifies the number of probes, <*1-5*>. Default: 3
`timeout <TIME>`	Specifies the traceroute timeout in seconds, <*1-60*>. Default: 3 seconds
`vrf <VRF-NAME>`	Specifies the virtual routing and forwarding (VRF) to use, <*VRF-NAME*>.
`source {<IPV6-ADDR> | <IFNAME>}`	Specifies the source IPv6 address or interface name.

Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

Examples

```
switch# traceroute6 0:0::0:1
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
```

```
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 localhost
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.089 ms  0.03 ms  0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 0:0::0:1 dsrport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 0:0::0:1 probes 2
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 2 probes, 24
byte packets
 1  localhost (::1)  0.117 ms  0.032 ms

switch# traceroute6 0:0::0:1 timeout 3
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 localhost vrf red
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.077 ms  0.051 ms  0.054 ms

switch# traceroute6 localhost mgmt
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.089 ms  0.03 ms  0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30 timeout 3 probes 3 dstport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1  localhost (::1)  0.117 ms  0.032 ms  0.021 ms

switch# traceroute6 2001::2 source 2001::1
traceroute to 2001::2 (2001::2) from 2001::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
1  2001::2 (2001::2)  0.4331 ms  0.3186 ms  0.1874 ms

switch# traceroute6 2001::2 source 1/1/1
traceroute to 2001::2 (2001::2) from 2001::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte  packets
1  2001::2 (2001::2)  0.6145 ms  0.4165 ms  0.1620 ms
```

Command History

Release	Modification
10.08	Added **source IP address** and **source interface name** parameters.
10.07 or earlier	--

Command Information

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

Chapter 11
Ping

The ping (Packet Internet Groper) command is a common method for troubleshooting the accessibility of devices. It uses Internet Control Message Protocol (ICMP) echo requests and ICMP echo replies to determine if the other device is alive. It also measures the amount of time the request takes to receive a reply from the specified destination. The ping command is mostly used to verify IP connectivity between two endpoints which could be switch to switch, host to host, or host to switch. The reply packet tells if the host received the ping and the amount of time it took to return the packet.

Ping over VXLAN

Ping and ping6 are supported over VXLAN (with both IPv4 and IPv6 underlay) from VTEP to VTEP, VTEP to host, and host to VTEP over L2 VNI/L3 VNI. A unique IP on VTEP should be used as the source and destination. Both source and destination VTEPs require AOS-CX 10.8 or later for this feature to work. Ping and ping6 over VXLAN with IPv4 underlay is supported on all platforms with VXLAN support.

Ping and ping6 over VXLAN with IPv6 underlay is supported on 6300, 6400, 8100, and 8360 Switch Series. IPv6 underlay is supported starting from 10.12.1000 version.

Ping with a large datagram size will not work as fragmentation, reassembly, and MTU discovery on the VXLAN paths are not supported. The default MTU size for an underlay port is 1500. When a packet is encapsulated via VXLAN , a VXLAN header of 50 bytes is added. With the default MTU size set on ports, packets larger than 1422 size is not expected to go over the VXLAN tunnel and is dropped. To user larger datagram size packets, the MTU must be increased.

Ping with `ip-option` as `record-route` is not supported.

Ping commands

ping

```
ping <IPv4-ADDR> | <hostname> [data-fill <pattern> | datagram-size <size> |
   interval <time> | repetitions <number> | timeout <time> | tos <number> |
   ip-option {include-timestamp | include-timestamp-and-address | record-route} |
   vrf <vrfname> | do-not-fragment][source {IPv4-ADDR | IFNAME}]
```

Ping on VXLAN with `ip-option` such as `include-timestamp-and-address`, `include-timestamp` and `record-route` is not supported.

Description

Pings the specified IPv4 address or hostname with or without optional parameters.

Parameter	Description
`ping <IPv4-ADDR>`	Selects the IPv4 address to ping.
`<HOSTNAME>`	Selects the hostname to ping. Range: 1-256 characters
`data-fill <PATTERN>`	Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB
`datagram-size <SIZE>`	Specifies the ping datagram size. Range: 0-65399, default: 100.
`interval <TIME>`	Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.
`repetitions <NUMBER>`	Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.
`timeout <TIME>`	Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.
`tos <NUMBER>`	Specifies the IP Type of Service to be used in Ping request. Range: 0-255
`ip-option {include-timestamp | include-timestamp-and-address | record-route}`	Specifies an IP option (**record-route** or **timestamp** option).
`include-timestamp`	Specifies the intermediate router time stamp.
`include-timestamp-and-address`	Specifies the intermediate router time stamp and IP address.
`record-route`	Specifies the intermediate router addresses.
`vrf <VRF-NAME>`	Specifies the virtual routing and forwarding (VRF) to use. When VRF option is not given, the default VRF is used.
`source {IPv4-ADDR | IFNAME}`	Specifies the source IPv4 address or interface to use.
`do-not-fragment`	Specifies the do-not-fragment (DF) bit in IP header of the Ping packet. This option does not allow the packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU).

Examples

Pinging an IPv4 address:

```
switch# ping 10.0.0.0
PING 10.0.0.0 (10.0.0.0) 100(128) bytes of data.
108 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.035 ms
108 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.033 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.033/0.034/0.035/0.000 ms
```

Pinging the localhost:

```
switch# ping localhost
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.060 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.035 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.043 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.041 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.034 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.034/0.042/0.060/0.011 ms
```

Pinging a server with a data pattern:

```
switch# ping 10.0.0.2 data-fill 1234123412341234acde123456789012
PATTERN: 0x1234123412341234acde123456789012
PING 10.0.0.2 (10.0.0.2) 100(128) bytes of data.
108 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.207 ms
108 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.187 ms
108 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.225 ms
108 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.197 ms
108 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.210 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.187/0.205/0.225/0.015 ms
```

Pinging a server with a datagram size:

```
switch# ping 10.0.0.0 datagram-size 200
PING 10.0.0.0 (10.0.0.0) 200(228) bytes of data.
208 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.202 ms
208 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.194 ms
208 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.201 ms
208 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.200 ms
208 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.186 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.186/0.196/0.202/0.016 ms
```

Pinging a server with an interval specified:

```
switch# ping 9.0.0.2 interval 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.199 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.208 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.182 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.194 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 7999ms
rtt min/avg/max/mdev = 0.182/0.195/0.208/0.008 ms
```

Pinging a server with a specified number of packets to send:

```
switch# ping 9.0.0.2 repetitions 10
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.213 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.204 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.201 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.202 ms
108 bytes from 9.0.0.2: icmp_seq=6 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=7 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=8 ttl=64 time=0.196 ms
108 bytes from 9.0.0.2: icmp_seq=9 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=10 ttl=64 time=0.200 ms

--- 9.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.184/0.197/0.213/0.008 ms
```

Pinging a server with a specified timeout:

```
switch# ping 9.0.0.2 timeout 3
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.175 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.190 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.181 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.197 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.175/0.187/0.197/0.007 ms
```

Pinging a server with the specified IP Type of Service:

```
switch# ping 9.0.0.2 tos 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.033 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.031 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.031 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.032/0.034/0.006 ms
```

Pinging a local host with the specified VRF.

```
switch# ping localhost vrf red
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.048 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.044 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.055 ms

--- localhost ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.036/0.047/0.055/0.006 ms
```

Pinging the localhost with the default VRF:

```
switch# ping localhost vrf mgmt
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.085 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.057 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.047 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.038 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.059 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.057/0.085/0.016 ms
```

Pinging a server with the intermediate router time stamp:

```
switch# ping 9.0.0.2 ip-option include-timestamp
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.031 ms
TS:     59909005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
TS:     59910005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.038 ms
TS:     59911005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.035 ms
TS:     59912005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.037 ms
TS:     59913005 absolute
        0
        0
        0


--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.035/0.038/0.002 ms
```

Pinging a server with the intermediate router time stamp and address:

```
switch# ping 9.0.0.2 ip-option include-timestamp-and-address
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.030 ms
TS:     9.0.0.2 60007355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.037 ms
TS:     9.0.0.2 60008355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.037 ms
TS:     9.0.0.2 60009355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.038 ms
TS:     9.0.0.2 60010355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.039 ms
TS:     9.0.0.2 60011355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0


--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.030/0.036/0.039/0.005 ms
```

Pinging a server with the intermediate router address:

```
switch# ping 9.0.0.2 ip-option record-route
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.034 ms
RR:     9.0.0.2
        9.0.0.2
        9.0.0.2
        9.0.0.2

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.038 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.036 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.037 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.035 ms (same route)

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.001 ms
```

Pinging a server with do-not-fragment:

```
switch# ping 192.168.1.8 datagram-size 2000 do-not-fragment
```

```
PING 192.168.1.8 (192.168.1.8) 2000(2028) bytes of data.
2008 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=0.721 ms
2008 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.792 ms
2008 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=0.857 ms
2008 bytes from 192.168.1.8: icmp_seq=4 ttl=64 time=0.833 ms
2008 bytes from 192.168.1.8: icmp_seq=5 ttl=64 time=0.836 ms

--- 192.168.1.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.721/0.807/0.857/0.048 ms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ping6

```
ping6 {<IPv6-ADDR> | <HOSTNAME>} [data-fill <PATTERN> | datagram-size <SIZE> |
   interval <TIME> | repetitions <NUMBER> | timeout <TIME> | vrrp <VRID> |
   vrf <VRF-NAME> | source <IPv6-ADDR> | <IFNAME>]
```

Description

Pings the specified IPv6 address or hostname with or without optional parameters. The VRRP option is provided to self-ping the configured link-local address on the VRRP group.

Parameter	Description
`IPv6-ADDR`	Selects the IPv6 address to ping.
`HOSTNAME`	Selects the hostname to ping. Range: 1-256 characters
`data-fill <PATTERN>`	Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB
`datagram-size <SIZE>`	Specifies the ping datagram size. Range: 0-65399, default: 100.
`interval <TIME>`	Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.
`repetitions <NUMBER>`	Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.
`timeout <TIME>`	Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.

Parameter	Description
`vrrp <VRID>`	Specifies the VRRP group ID.
`vrf <VRF-NAME>`	Specifies the virtual routing and forwarding (VRF) to use. When this option is not provided, the default VRF is used.
`source <IPv6-ADDR> | <IFNAME>`	Specifies the source IPv6 address or interface to use.

Examples

Pinging an IPv6 address:

```
switch# ping6 2020::2
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.386 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.235 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.249 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.240 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.252 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.235/0.272/0.386/0.059 ms
```

Pinging the localhost:

```
switch# ping6 localhost
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.093 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.051 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.055 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.046 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.048 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.046/0.058/0.093/0.019 ms
```

Pinging a server with a data pattern:

```
switch# ping6 2020::2 data-fill ab
PATTERN: 0xab
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.077 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.068/0.077/0.015 ms
```

Pinging a server with a datagram size:

```
switch# ping6 2020::2 datagram-size 200
PING 2020::2(2020::2) 200 data bytes
208 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.037 ms
208 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.077 ms
208 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.066 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.037/0.066/0.077/0.016 ms
```

Pinging a server with an interval specified:

```
switch# ping6 2020::2 interval 5
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.043 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.075 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 19999ms
rtt min/avg/max/mdev = 0.043/0.068/0.075/0.014 ms
```

Pinging a server with a specified number of packets to send:

```
switch# ping6 2020::2 repetitions 6
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.039 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.070 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.071 ms
108 bytes from 2020::2: icmp_seq=6 ttl=64 time=0.078 ms

--- 2020::2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.039/0.068/0.078/0.015 ms
```

Pinging a local host with the specified VRF.

```
switch# ping6 localhost vrf red
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.050 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.039 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.027 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.027/0.038/0.050/0.010 ms
```

Pinging the localhost with the default VRF:

```
switch# ping6 localhost vrf mgmt
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.032 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.046 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.022/0.032/0.046/0.010 ms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Troubleshooting

Operation not permitted

Symptom

The switch displays an `operation not permitted` message when a user attempts to send a ping request.

Example:

```
switch# ping 100.1.2.10
PING 100.1.2.10 (100.1.2.10) 100(128) bytes of data
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted


--- 100.1.2.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms
```

Cause

When an ACL is applied to the Control Plane, sending a ping request may be denied. If the ping packet matches a drop entry in the ACL, applying a Control Plane may block traffic sent from the switch CLI ping command.

When this situation occurs, the following error message is displayed: `ping: sendmsg: Operation not permitted`. The message indicates that the ICMP echo request packet has not been sent and is blocked by the Control Plane ACL.

When this message is not displayed, the ping request packet has been sent correctly. A ping failure in this case represents a failure to receive the ICMP echo reply packet.

This message may also be displayed on 8320, 8325, or 9300 Series switches when an egress ACL is applied and is blocking the ping.

Action

1. Modify the ACL to allow the ping traffic.
2. Unapply the ACL from egress (8400/8320/8325/9300 switches) or Control Plane.
3. Ping a destination which is not matched by the ACL. For example, if the ACL is blocking traffic based on destination IP. Depending on the ACL content, this might not always be possible like when the ACL blocks all ICMP packets.

Network is unreachable

Symptom

User receives a "network is unreachable" message on sending a ping request.

Cause

The ping packet did not get sent, because the switch cannot find an interface with a route that leads to the destination for one of the following reasons:

- A configuration error, such as an interface having an incorrect IP address or subnet defined.
- DHCP having failed to assign an address at all.
- The user meant to ping out the management vrf, but forgot to add `vrf mgmt` to the ping command.

Action

Adjust the switch configuration to ensure that a route to the destination network exists.

Destination host unreachable

Symptom

User receives a `Destination host unreachable` message on sending a ping request.

Cause

This issue typically indicates that the host is down or otherwise not returning ICMP echo requests. It is also possible that an intermediate network hop is dropping the packets.

Action

Investigate whether an intermediate hop is not returning pings by using the `traceroute` command. Check the intermediate hop, and then the endpoint. If the destination is another Aruba switch, it is

possible that Ingress ACLs on that switch are blocking ping packets. In such cases, the configuration option on the destination switch should be examined.

Chapter 12

Using classifier policies for traffic capture and analysis

AOS-CX can use a classifier policy to troubleshooting network issues by mirroring packets for capture and analysis.

The process to filter mirrored traffic requires hardware resources, and this process may compete for these resources with other configured features, including existing Classifier Policies and Access Control Lists (ACLs). Prior to configuring and installing a policy for troubleshooting purposes, issue the **show policy** commands and **show resources** commands to determine what existing features are consuming hardware resources on the switch. This will also help to ensure that configurations created for troubleshooting are not overriding existing configurations. If a switch already has a classifier policy applied to one context (applied globally, interface, VLAN), consider adding entries to that policy, temporarily unapplying the existing policy, or applying the troubleshooting policy to a different context.

Classifier Policies cannot capture traffic on the out-of-band management port. If the port is out-of-band, its packets do not enter or leave through the switch ASIC, which is required for mirroring operations.

Step one: create a traffic class

The following example creates a traffic class to match traffic to be mirrored for future evaluation. In this example:

- TCP and UDP protocols should include entries for both source and destination port matches in order to mirror traffic either to or from that port number.
- Aruba Central traffic utilizes HTTPS and therefore will match that entry.
- In this example, the **count** keyword is included so that hit counts can be monitored to verify that traffic is matching the class entries.
- The last entry **(ignore any any any count**) is included to count packets of all other traffic types passing through the device, and to confirm other traffic is reaching the policy for evaluation, and not being mirrored.
- Sequence numbers (for example, 10, 20, 30) are not mandatory when creating class entries, and will be auto-generated if not manually specified.
- Comment lines are optional for functionality but included for clarity.

```
switch(config)# class ip support-mirror
  10 comment OSPF protocol
  10 match ospf any any count
  20 comment GRE protocol
  20 match gre any any count
  30 comment BGP dst port
  30 match tcp any any eq bgp count
  40 comment BGP src port
  40 match tcp any eq bgp any count
  50 comment VxLAN dst port
  50 match udp any any eq vxlan count
  60 comment VxLAN src port
```

```
  60 match udp any eq vxlan any count
  70 comment RADIUS authentication dst port
  70 match udp any any eq radius count
  80 comment RADIUS authentication src port
  80 match udp any eq radius any count
  90 comment HTTPS dst port
  90 match tcp any any eq https count
  100 comment HTTPS src port
  100 match tcp any eq https any count
  110 comment HTTP dst port
  110 match tcp any any eq http count
  120 comment HTTP src port
  120 match tcp any eq http any count
  130 comment ICMP Echo (Ping)
  130 match icmp any any icmp-type echo count
  140 comment ICMP Echo (Ping) Reply
  140 match icmp any any icmp-type echo-reply count
  150 comment Count all other traffic
  150 ignore any any any count
exit
```

Step two: create a policy

Create a policy that uses the class created in the previous step and sends matching traffic to mirror session 1:

```
switch(config)# policy support-mirror
10 class ip support-mirror action mirror 1
exit
```

Step three: apply the policy

If you do not know which interface or VLAN the relevant traffic uses to enter the switch, apply the policy globally. Alternatively, you can apply the policy to one ore more specific contexts. Note that while it is possible to apply policies to multiple interfaces, interface types, and directions, each application consume a hardware resources and may not be successful if resources are exhausted.

Apply the policy globally in the ingress (in) direction:

```
apply policy support-mirror in
```

AOS-CX does not allow you to apply a policy globally in the egress direction; apply a policy to a specific interface, VLAN, or LAG if egress traffic is required.

Apply a policy to a specific physical interface in the ingress (in) direction:

```
switch (config)# interface 1/1/1
switch(config-if)# apply policy support-mirror in
```

Apply a policy to a specific physical interface in Egress (out) direction:

```
switch (config)#interface 1/1/1
switch(config-if)# apply policy support-mirror out
```

Apply a policy to a specific LAG in Ingress (in) direction:

```
switch (config)# interface lag 1
switch(config-lag-if)# apply policy support-mirror in
```

Apply a policy to a specific LAG in Egress (out) direction:

```
switch (config)# interface lag 1
switch(config-lag-if)# apply policy support-mirror out
```

Apply a policy to a specific VLAN in Ingress (in) direction:

```
switch (config)# vlan 100
switch(config-if-vlan)# apply policy support-mirror in
```

Apply a policy to a specific VLAN in Egress (out) direction:

```
switch (config)# vlan 100
switch(config-if-vlan)# apply policy support-mirror out
```

Step four: confirm policy Installation

The output of the **show class** and **show policy** commands should include the configuration that was configured in the previous steps. The output must **not** include any lines starting with an exclamation point (**!**), such as:

```
! policy support-mirror user configuration does not match active configuration.
```

A message that starts with exclamation point (**!**), indicates a policy installation failure, possibly due to hardware resource limitations.

Step five: confirm policy resource consumption

Next, confirm that the ingress global policy lookup process is consuming TCAM entries. If the switch is a chassis, each module should show resources consumed, as this policy is installed on the ASIC in each line card. The following example of shows the output of a **show resources** command issued on a 6300 switch:

```
6300(config)# show resources
Resource Usage:
Mod  Description
Resource                                    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Ingress Global Policy Lookup
```

```
Ingress TCAM Entries                          35     2048
Total
Ingress TCAM Entries                          35     2048   18432
Egress TCAM Entries                            0        0    8192
Ingress Lookups                                1                8
Ingress Flex Lookups                           0                1
Egress Lookups                                 0                4
Ingress Policers                               0             2047
Egress Policers                                0             2047
```

Hardware resources will be consumed on each module that has a policy applied to an interface. Ingress and egress policies consume separate hardware resources. The following example shows the output of a **show resources** command issued on a 6300 switch with a policy applied to a physical interface in both **in** and **out** directions:

```
6300(config)# show resources
Resource Usage:
Mod  Description
Resource                                    Used Reserved    Free
------------------------------------------------------------------------------
1/1  Ingress Port Policy Lookup
Ingress TCAM Entries                          37     2048
Egress Port Policy Lookup
Egress TCAM Entries                           37     2048
Total
Ingress TCAM Entries                          37     2048   18432
Egress TCAM Entries                           37     2048    6144
Ingress Lookups                                1                8
Ingress Flex Lookups                           0                1
Egress Lookups                                 1                3
Ingress Policers                               0             2047
Egress Policers                                0             2047
```

Step six: configure a mirror session

In this example, the mirror session will be configured to send traffic to the switch CPU for capture:

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

You may also choose to mirror packets to an external capture host, such as a workstation running Wireshark for live packet analysis and further filtering. See Step eight: capture packets to a file or mirror it to a host.

Step seven: start packet capture

Start a packet capture using TShark.

```
switch# diag utilities tshark
```

Traffic should be captured and dumped to screen. The following example displays partial TShark output when a ping packet is sent through the switch:

```
switch# diag utilities tshark
Inspecting traffic mirrored to the CPU until Ctrl-C is entered.
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
MirrorRxNet, id 0
Interface id: 0 (MirrorRxNet)
Interface name: MirrorRxNet
Encapsulation type: Ethernet (1)
Arrival Time: Jul 18, 2023 22:45:21.213862080 UTC
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1689720321.213862080 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
...
```

Step eight: capture packets to a file or mirror it to a host

Once basic policy configuration is confirmed as working as expected, you can use the **diag utilities tshark file** command to capture the TShark output to a file.

```
switch# diag utilities tshark file
```

This command will store packets to a circular file; only the most recent 32MB of traffic will be captured.

Use the following command to copy a pcap file to a remote device:

```
switch# copy tshark-pcap ?
REMOTE_URL  URL syntax - sftp://USER@{IP|HOST}[:PORT]/FILE or
tftp://{IP|HOST}[:PORT][;blocksize=VAL]/FILE
```

If you do not want to capture the TShark output to a file, you can mirror it to an external capture host. In the following example, packets are mirrored to external capture host (such as a workstation with WireShark) is connected to interface 1/1/2:

```
switch(config)# mirror session 1
switch(config-mirror-1)# destination interface 1/1/2
switch(config-mirror-1)# enable
```

Step nine: check packet hit counts

Use the **show policy hitcounts** command to confirm that the policy is evaluating traffic.

```
switch(config)# show policy hitcounts
```

In the following example, no ICMP echo reply packets are captured, as the policy globally is applied to ingress traffic only. Remember, AOS-CX does not support applying policies globally in the egress direction; You must apply a policy to a specific context (an interface, VLAN, or LAG) to monitor egress traffic.

```
switch# show policy hitcounts support-mirror
Statistics for Policy support-mirror:
global (in):
Matched Packets  Configuration
10 class ip support-mirror action mirror 1
0  10 match ospf any any count
0  20 match gre any any count
0  30 match tcp any any eq bgp count
0  40 match tcp any eq bgp any count
0  50 match udp any any eq vxlan count
0  60 match udp any eq vxlan any count
0  70 match udp any any eq radius count
0  80 match udp any eq radius any count
0  90 match tcp any any eq https count
0  100 match tcp any eq https any count
0  110 match tcp any any eq http count
0  120 match tcp any eq http any count
5  130 match icmp any any icmp-type echo count
0  140 match icmp any any icmp-type echo-reply count
0  150 ignore any any any count
```

In this example, hit counts will be shown separately for each application of a policy and will reflect the direction of the traffic (that is, ICMP echo packets entering the switch and ICMP echo reply packets leaving the switch.)

```
6300(config-if)# show policy hitcounts support-mirror
 Statistics for Policy support-mirror:
 Interface 1/1/1 (in):
 Matched Packets  Configuration
     0    10 class ip support-mirror action mirror 1
     0  10 match ospf any any count
     0  20 match gre any any count
     0  30 match tcp any any eq bgp count
     0  40 match tcp any eq bgp any count
     0  50 match udp any any eq vxlan count
     0  60 match udp any eq vxlan any count
     0  70 match udp any any eq radius count
     0  80 match udp any eq radius any count
     0  90 match tcp any any eq https count
     0  100 match tcp any eq https any count
     0  110 match tcp any any eq http count
     0  120 match tcp any eq http any count
     0  130 match icmp any any icmp-type echo count
     0  140 match icmp any any icmp-type echo-reply count
     0  150 ignore any any any count
 Interface 1/1/1 (out):
 Matched Packets  Configuration
     10 class ip support-mirror action mirror 1
     0  10 match ospf any any count
     0  20 match gre any any count
     0  30 match tcp any any eq bgp count
```

```
    0  40 match tcp any eq bgp any count
    0  50 match udp any any eq vxlan count
    0  60 match udp any eq vxlan any count
    0  70 match udp any any eq radius count
    0  80 match udp any eq radius any count
    0  90 match tcp any any eq https count
    0  100 match tcp any eq https any count
    0  110 match tcp any any eq http count
    0  120 match tcp any eq http any count
    0  130 match icmp any any icmp-type echo count
    5  140 match icmp any any icmp-type echo-reply count
    0  150 ignore any any any count
```

Chapter 13
Packet forwarding information

Packet forwarding information is supported only on the 8325 and 10000 Switch Series.

The packet forwarding information feature shows the forwarding information of a packet given packet header details and ingress information. This helps validate system configuration without actual traffic flowing into the system. In the case of the packet egressing out of LAG or ECMP, this feature also shows the physical interface the packet is egressed out on, based on the load balance setting configured in the system.

Packet forwarding information commands

show forwarding-info

```
show forwarding-info mac ingress-interface <IFNAME> source-mac-address <MAC-ADDR>
     destination-mac-address <MAC-ADDR> [vlan <VLAN-ID>] [timeout <TIMEOUT>]

show forwarding-info mac-ip ingress-interface <IFNAME> source-mac-address <MAC-ADDR>
     destination-mac-address <MAC-ADDR>
     {source-ip-address <IP-ADDR> destination-ip-address <IP-ADDR>] |
     source-ipv6-address <IPV6-ADDR> destination-ipv6-address <IPV6-ADDR>}
     [vlan <VLAN-ID>] [transport-protocol <TR-PROT-NUM>]
     [source-l4-port <L4-PORT> destination-l4-port <L4-PORT>]
     [vrf <VRF-NAME>] [timeout <TIMEOUT>]

show forwarding-info ip
     {source-ip-address <IP-ADDR> destination-ip-address <IP-ADDR>] |
     source-ipv6-address <IPV6-ADDR> destination-ipV6-address <IPV6-ADDR>}
     [ingress-interface <IFNAME>][transport-protocol <TR-PROT-NUM>]
     [source-l4-port <L4-PORT> destination-l4-port <L4-PORT>]
     [vrf <VRF-NAME>] [timeout <TIMEOUT>]
```

Description

Shows the forwarding information based on current system configurations and hardware states for forwarding lookups. Given the user packet information, this command shows the egress physical interface of the packet. L3 hash mode and L4 hash mode are supported for LAG.

Parameter	Description
`ingress-interface <IFNAME>`	Specifies the ingress interface (for example: **1/1/1**).
`source-mac-address <MAC-ADDR>`	Specifies the source MAC address. Format: **AA:BB:CC:DD:EE:FF.**
`destination-mac-address <MAC-ADDR>`	Specifies the destination MAC address. Format: **AA:BB:CC:DD:EE:FF.**

Parameter	Description
`vlan <VLAN-ID>`	Specifies the egress VLAN. Default 1. Range: 1 to 4094.
`timeout <TIMEOUT>`	Specifies the response timeout in seconds. Default: 3. Range: 1 to 60.
`source-ip-address <IP-ADDR>`	Specifies the source IPv4 address. Format: **`A.B.C.D`**
`destination-ip-address <IP-ADDR>]`	Specifies the destination IPv4 address. Format: **`A.B.C.D`**
`source-ipv6-address <IPV6-ADDR>`	Specifies the source IPv6 address. Format: **`X:X::X:X`**
`destination-ipv6-address <IPV6-ADDR>`	Specifies the destination IPv6 address. Format: **`X:X::X:X`**
`transport-protocol <TR-PROT-NUM>`	Specifies the transport protocol number. Range 1 to 255. For example, use **`6`** for TCP, **`17`** for UDP, **`1`** for ICMP, **`2`** for IGMP.
`source-l4-port <L4-PORT>`	Specifies the L4 source port. Range 1 to 65535.
`destination-l4-port <L4-PORT>`	Specifies the L4 destination port. Range 1 to 65535.
`vrf <VRF-NAME>`	Specifies the egress VRF name. Default: **`default`**.

Usage

The following limitations need to be considered:

- The forwarding-information feature is not applicable for broadcast, multicast, and unknown packets.
- Sub-interfaces and tunnel interfaces (VXLAN and MPLS) in both ingress and egress are not supported.
- Ingress interfaces are limited to the physical interfaces.
- The **vlan** and **vrf** parameters must be used for packet forwarding information wherever applicable. If these parameters are not specified, their indicated defaults are used.
- The **mac** and **mac-ip** parameters are not supported for LAGs in L2 hash mode for both bridged and routed traffic.
- When LAG is in L3 hash mode, the L2 data is not used for hashing.
- For bridged traffic, the **mac** or **mac-ip** parameters must be used. For routed traffic, the **ip** or **mac-ip** parameters must be used.
- For bridged traffic, ensure that the VLAN membership of the ingress port parameter matches the value of the VLAN parameter.
- When using L3 hashing, the **show forwarding-info mac** form of this command is not applicable.
- **When** a LAG is in L3 hashing mode it will only hash L3 data. As a result, the L2 data displayed in the output of the **show forwarding-info mac-ip** command is ignored.
- **This** command does not display data for unsupported egress interfaces, such as a tunnel or sub-interface. The egress interface must be a physical port or a LAG.
- When ISL redirection is happening for a packet, the forwarding information does not show the correct egress interface in the VSX MCLAG.
- The forwarding information output of this command does not honor the PBR policy for the destination route.

Examples

Showing forwarding information when LAG is in L3 hash mode (the default):

```
interface lag 1
    no shutdown
    no routing
    vlan access 1
    exit

show forwarding-info mac ingress-interface 1/1/4 source-mac-address
     00:00:00:00:00:01 destination-mac-address 00:00:00:00:00:02 vlan 1

Ingress-interface: 1/1/4
Source mac-address: 00:00:00:00:00:01
Destination mac-address: 00:00:00:00:00:02
VLAN: 1

Forwarding info lookup needs IP inputs when lag is in L3 hash mode.
```

Showing forwarding information when LAG is in L4 hash mode:

```
interface lag 1
    no shutdown
    no routing
    vlan access 1
    hash l4-src-dst
    exit

show forwarding-info mac ingress-interface 1/1/4 source-mac-address
     00:00:00:00:00:01 destination-mac-address 00:00:00:00:00:02 vlan 1

Ingress-interface: 1/1/4
Source mac-address: 00:00:00:00:00:01
Destination mac-address: 00:00:00:00:00:02
VLAN: 1

Egress interface: lag1 -> 1/1/1
```

Showing forwarding information when LAG is in L2 hash mode:

```
interface lag 1
    no shutdown
    no routing
    vlan access 1
    hash l2-src-dst
    exit

show forwarding-info mac ingress-interface 1/1/4 source-mac-address
     00:00:00:00:00:01 destination-mac-address 00:00:00:00:00:02 vlan 1

Ingress-interface: 1/1/4
Source mac-address: 00:00:00:00:00:01
Destination mac-address: 00:00:00:00:00:02
VLAN: 1

Forwarding info lookup on lag port is unsupported when lag is in L2 hash mode.
```

Showing forwarding information when the egress interface is a physical port:

```
show mac-address-table
MAC age-time             : 300 seconds
Number of MAC addresses : 1

MAC Address          VLAN     Type                        Port
-------------------------------------------------------------
00:00:00:00:00:02    1        static                      lag1
00:00:00:00:00:03    1        static                      1/1/5

show forwarding-info mac ingress-interface 1/1/4 source-mac-address
      00:00:00:00:00:01 destination-mac-address 00:00:00:00:00:03 vlan 1

Ingress-interface: 1/1/4
Source mac-address: 00:00:00:00:00:01
Destination mac-address: 00:00:00:00:00:03
VLAN: 1

Egress interface: 1/1/5
```

Showing forwarding information for when the ingress interface is ROP:

```
show forwarding-info mac-ip ingress-interface 1/1/14
   source-mac-address 00:11:01:00:00:01 destination-mac-address b8:d4:e7:dd:d3:00
   source-ip-address 101.0.0.2 destination-ip-address 201.0.0.2 vrf default

Ingress-interface: 1/1/14
Source mac-address: 00:11:01:00:00:01
Destination mac-address: b8:d4:e7:dd:d3:00
VLAN: 1
VRF: default
Source IP: 101.0.0.2
Destination IP: 201.0.0.2

L2 Warning: Port is routing enabled.  Please use the 'show forwarding-info ip'
command.

Egress interface: ECMP 1/1/17
```

Showing forwarding information with ROP and SVI:

```
interface 1/1/4
    no routing
    no shutdown
    vlan trunk native 1
    vlan trunk allowed all
interface 1/1/6
     no shutdown
     ip address 10.10.10.2/24


show ip route

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
```

```
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix           Nexthop     Interface  VRF(egress)   Origin/   Distance/    Age
                                                      Type      Metric
-------------------------------------------------------------------------------
-
10.10.10.0/24    -           1/1/6      -             C         [0/0]        -
10.10.10.2/32    -           1/1/6      -             L         [0/0]        -

show forwarding-info ip source-ip-address 10.10.10.1 destination-ip-address
      10.10.10.4
Source IP: 10.10.10.1
Destination IP: 10.10.10.4

Egress interface: 1/1/6


interface 1/1/4
    no routing
    no shutdown
    vlan trunk native 1
    vlan trunk allowed all
interface 1/1/7
     no routing
     no shutdown
     vlan access 2
interface vlan 2
     ip address 2.2.2.2/24interface 1/1/4
    no routing
    no shutdown
    vlan trunk native 1
    vlan trunk allowed all
interface 1/1/7
     no routing
     no shutdown
     vlan access 2
interface vlan 2
     ip address 2.2.2.2/24


show ip route

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix           Nexthop     Interface  VRF(egress)   Origin/   Distance/    Age
                                                      Type      Metric
-------------------------------------------------------------------------------
-
2.2.2.0/24       -           vlan2      -             C         [0/0]        -
2.2.2.2/32       -           vlan2      -             L         [0/0]        -
```

```
show forwarding-info ip source-ip-address 2.2.2.1 destination-ip-address 2.2.2.4

Source IP: 2.2.2.1
Destination IP: 2.2.2.4

Egress interface: vlan2 -> 1/1/7
```

Showing forwarding information in L4 hash mode with ROP LAG:

```
switch# show forwarding-info mac-ip ingress-interface 1/1/1
source-mac-address 00:00:00:00:01 destination-mac-address 00:00:00:00:00:02
source-ip-address 10.10.10.10 destination-ip-address 10.10.10.11
transport-protocol 6 source-l4-port 1234 destination-l4-port 5678 vrf default

Ingress interface: 1/1/1
Source MAC address: 00:00:00:00:00:01
Destination MAC address: 00:00:00:00:00:02
VLAN: 1
VRF: default
Source IP: 10.10.10.10
Destination IP: 10.10.10.11
Protocol: TCP(6)
Source L4 Port: 1234
Destination L4 Port: 5678

Egress interface: lag1 -> 1/1/2
```

Showing forwarding information in ECMP hash mode with ROP LAG:

```
switch# show forwarding-info mac-ip ingress-interface 1/1/1
source-mac-address 00:00:00:00:01 destination-mac-address 00:00:00:00:00:02
source-ip-address 10.10.10.10 destination-ip-address 200.0.0.1
transport-protocol 6 source-l4-port 1234 destination-l4-port 5678 vrf default

Ingress interface: 1/1/1
Source MAC address: 00:00:00:00:00:01
Destination MAC address: 00:00:00:00:00:02
VLAN: 1
VRF: default
Source IP: 10.10.10.10
Destination IP: 200.0.0.1
Protocol: TCP(6)
Source L4 Port: 1234
Destination L4 Port: 5678

Egress interface: ECMP lag1 -> 1/1/2
```

Attempting to show forwarding information but with the request timed out:

```
switch# show forwarding-info mac-ip ingress-interface 1/1/1
source-mac-address 00:00:00:00:01 destination-mac-address 00:00:00:00:00:02
source-ip-address 10.10.10.10 destination-ip-address 200.0.0.1
transport-protocol 6 source-l4-port 1234 destination-l4-port 5678 vrf default

Ingress interface: 1/1/1
Source MAC address: 00:00:00:00:00:01
Destination MAC address: 00:00:00:00:00:02
VLAN: 1
VRF: default
Source IP: 10.10.10.10
Destination IP: 200.0.0.1
Protocol: TCP(6)
Source L4 Port: 1234
Destination L4 Port: 5678

Request timed out
```

Command History

Release	Modification
10.11	Introduced on the 8325, 10000 Switch Series.

Command Information

Platforms	Command context	Authority
8325 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 14
Remote syslog

Remote syslog enables the forwarding of syslog messages to the remote syslog server. The feature supports a maximum of four remote syslog servers. Only one configuration per remote syslog server is allowed. The remote syslog server supports TCP and UDP transport protocols and TLS to establish a connection. In addition to forwarding logs to the remote server, they can also be preserved in local storage.

When the client certificate associated with the syslog client is updated, the syslog client is restarted and a new TLS connection is established using the updated client certificate.

Syslog over VXLAN support

Syslog message is supported over VxLAN with IPv4 or IPv6 underlay.

Remote syslog commands

clear accounting-logs

```
clear accounting-logs
```

Description

Use this command to clear accounting logs. Once issued, only logs generated after this command is run will be displayed in the output of the **show accounting log** commands.

This command will not clear logs when the logging accounting-format-native feature is configured. To clear accounting logs on switches with this feature enabled, users should first revert the native accounting format back to the default AOS-CX format by executing the **no logging accounting-format-native** command.

Example

```
switch(config)# clear accounting-logs
```

The following example shows that accounting logs cannot be cleared using the clear accounting-logs command if the **logging accounting-native-format** command has been enabled, and that disabling this option with the **no logging accounting-format-native** command again allows the accounting logs to be cleared.

```
switch# logging audit-format-native
switch# clear accounting-logs
Warning: Clear accounting-logs is not supported for 'audit-format-native'.
switch# no logging audit-format-native
switch# clear accounting-logs
```

```
switch# show accounting log last 5
-------------------------------------------------
Command logs from current boot
-------------------------------------------------
No command logs has been logged in the system
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

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

logging

```
logging {<IPV4-ADDR> | <IPV6-ADDR> | <FQDN | HOSTNAME>} {udp [<PORT-NUM>]}|{tcp [<PORT-NUM>]}|{|tls [<PORT-NUM>]}
   auth-mode {certificate|subject-name}
   disable
   filter <FILTER-NAME>
   include-auditable-events
   legacy-tls-renegotiation]
   rate-limit-burst <BURST>
   rate-limit-interval <INTERVAL>] ]
   severity <LEVEL>]
   vrf <VRF-NAME>]

no logging {<IPV4-ADDR> | <IPV6-ADDR> | <FQDN | HOSTNAME> }
```

Description

Enables syslog forwarding to a remote syslog server.

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

Starting with AOS-CX 10.11, payload information is present in accounting logs.

The maximum REST payload that can be sent to RADIUS/TACACS server is 1024 characters, and the maximum of REST payload that can be sent to syslog server is 3500 characters. If this limit is is reached, the log will display three dots (...) to indicate that the log an exceeded the character limit and is incomplete.

Parameter	Description
{*<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>* | tls [*<PORT-NUM>*]]	Specifies the UDP port, TCP port, or TLS port of the remote syslog server to receive the forwarded syslog messages.

Parameter	Description
`udp [<PORT-NUM>]`	Range: 1 to 65535. Default: 514
`tcp [<PORT-NUM>]`	Range: 1 to 65535. Default: 1470
`tls [<PORT-NUM>]`	Range: 1 to 65535. Default: 6514
`auth-mode`	Specifies the TLS authentication mode used to validate the certificate. ■ **certificate**: Validates the peer using trust anchor certificate based authentication. Default. ■ **subject-name**: Validates the peer using trust anchor certificates as well as subject-name based authentication.
`disable`	Disable remote syslog confguration. This does not delete the configuration, just disables/pauses the forwarding of syslog messagesto the remote server. The config/forwarding can be reenabled (un-paused) again using the **no logging <hostname> disable** command.
`filter <FILTER-NAME>`	Specifies the name of the filter to be applied on the syslog messages.
`include-auditable-events`	Specifies that auditable messages are also logged to the remote syslog server.
`legacy-tls-renegotiation`	Enables the TLS connection with a remote syslog server supporting legacy renegotiation.
`rate-limit-burst <BURST>`	Specifies the rate limit for the messages sent to the remote syslog server.
`rate-limit-interval <INTERVAL>`	Specifies the rate limit interval in seconds. Default: 30 Seconds
`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

Parameter	Description
	severity of **warning (3)** and above.
`vrf <VRF-NAME>`	Specifies the VRF used to connect to the syslog server. Optional. Default: `default`

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
```

Enabling syslog forwarding over TLS to a remote syslog server using subject-name authentication mode:

```
switch(config)#logging example.com tls auth-mode subject-name
```

Applying log filtering for syslog server forwarding:

```
switch(config)# logging 10.0.10.6 severity info filter filter_lldp_logs vrf mgmt
```

Applying log filtering and enabling the rate limit for syslog server forwarding over TCP port:

```
switch(config)# logging 10.0.10.2 tcp 3440 severity err vrf mgmt include-
auditable-events filter filter_lldp_logs rate-limit-burst 3 rate-limit-interval 35
```

Command History

Release	Modification
	The disable parameter is introduced
10.07 or earlier	--

Command Information

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

logging accounting-format-native

```
logging accounting-format-native
[no] logging accounting-format-native
```

Description

Change the accounting log message format to native Linux format. (Default: ArubaOS-CX format)

The 'no' form of this command will change the accounting log message format to ArubaOS-CX format.

Usage

This option enables the switch to show all types of accounting records to the user. When configured, the same format will be used while sending messages to syslog servers. When upgrading from an earlier version of AOS-CX to AOS-CX 10.11 or later versions, if native accounting logs are preferred, then best practices is to issue this command as a part of the upgrade. If the switch upgrades from an earlier version to AOS-CX 10.11 or later without configuring this setting, by default, the accounting log message format will be ArubaOS-CX Format.

Example

This example changes the accounting log message format to native Linux format.

```
switch(config)# logging accounting-format-native
```

The following example returns the accounting log message format to the default ArubaOS-CX format.

```
switch(config)# no logging accounting-format-native
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

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

logging filter

```
logging filter <FILTER-NAME>

   [{enable | disable}]

   [<SEQUENCE-ID>] {permit | deny} [event-id <EVENT-ID-RANGE>] [includes <REGEX>]
   [severity <COMPARISON-OPERATOR> <LEVEL>]

   no <SEQUENCE-ID>

   resequence <OLD-SEQUENCE-ID> <NEW-SEQUENCE-ID>
```

```
no logging filter <FILTER-NAME>
```

Description

Creates a filter to restrict what event or debug logs are logged. A filter can be used to either permit or deny:

- The event logs from being generated on the switch, or
- The event or debug logs generated on the switch from being forwarded to a syslog server.

A filter is identified by a filter name and can have up to 20 rules or entries, each with a different sequence number, matching criteria, and corresponding action (deny or permit). When a filter is applied on a log, the log is matched against the criteria mentioned in the rules or entries in ascending numerical order of their sequence numbers until a matching entry is found. Once a matching entry is found, its corresponding action is applied on the log. If no matching rule is found, the default action (permit) is applied.

The **no** form of this command removes the filter.

Parameter	Description
<FILTER-NAME>	Specifies the unique name to identify the filter.
`enable`	Filter event logs generated on the switch.
<SEQUENCE-ID>	Specifies the filter criteria sequence number. Default: Increments by 10 from the largest sequence-id currently used in this filter.
`deny`	Prevents the matching log from being logged.
`permit`	Allows the matching log.
<event-id>	Matches logs by event ID. Specify an event ID or a range of event IDs. It supports a maximum of 100 event IDs.
`includes` *<REGEX>*	Matches the log message against a regular expression string.
`severity`	Matches the logs by severity level. The following options are used to compare the severity: ■ **eq**: Match events of severity equal to the specified. ■ **ge**: Match events of severity greater than or equal to the specified. ■ **gt**: Match events of severity greater than the specified. ■ **le**: Match events of severity lesser than or equal to the specified. ■ **lt**: Match events of severity lesser than the specified. The following are the severity levels: ■ **alert**: Logs with the severity **alert (6)**. ■ **crit**: Logs with the severity **critical (5)**. ■ **debug**: Logs with the severity **debug (0)**. ■ **emerg**: Logs with the severity **emergency (7)**. ■ **err**: Logs with the severity **err (4)**. ■ **info**: Logs with the severity **info (1)**. ■ **notice**: Logs with the severity **notice (2)**. ■ **warning**: Logs with the severity **warning (3)**.

Usage

Filtering event logs on the switch: To permit or deny event logs from being generated on the switch. In this case, the matching event logs are filtered at generation. The denied event logs are neither logged to the switch events nor forwarded to any remote syslog servers. Multiple filters can be configured, but only one filter can be applied to filter the events on the switch. Such a filter can be chosen by adding the **enable** command under its configuration. Configuring the **enable** command under a new filter automatically removes it from the filter where it was previously used.

For example:

```
logging filter low_severity_logs

enable

10 deny severity lt info
```

This configuration denies the event logs which have a severity less than info.

If a filter contains **enable** command, it is not recommended to configure this filter in the **logging** command used for remote syslog server configuration. This is because, any event logs denied by the filter are already not available for forwarding to a remote server.

A filter with **enable** command will not affect debug logs. Consider the configuration in the following example of a filter with **enable** command and two rules applied **10 permit severity ge info** and **20 deny**. This implies permit only those event logs which have severity greater than or equal to **info**.
Example:

```
logging filter low_severity_logs
enable
10 permit severity ge info
20 deny
```

Filtering event or debug logs when forwarding to a remote syslog server: The filter name must be configured in the logging command that is used to configure remote syslog server. The logs will be generated on the switch and the filter only decides whether to deny or permit the syslog forwarding for the matching log. For example: **logging 10.0.10.6 filter filter_lldp_logs**

The filter affects debug logs only when the command **debug destination syslog** is configured on the switch.

The severity mentioned in the remote syslog server configuration using logging command under configuration context has more precedence than the severity mentioned in a filter entry. If a log with **warning** severity is permitted by a filter, but the remote syslog configuration has severity **err** mentioned in it, the log will not be forwarded to the remote syslog server (since warning(3) is lesser than err(4)). On the other hand, if a log with **err** severity is permitted by a filter and the remote syslog configuration has severity **warning** mentioned in it, the log will be forwarded to the remote syslog server.

Examples

Configuring a new logging filter:

```
switch(config)# logging filter example_filter
```

To deny logs having event ID 1301 and a range of event IDs from 1305 to 1309:

```
switch(config-logging-filter)# 20 deny event-id 1301,1305-1309
```

To permit logs having event ID 1300:

```
switch(config-logging-filter)# 30 permit event-id 1300
```

To permit logs with severity greater than or equal to `err`:

```
switch(config-logging-filter)# 30 permit severity ge err
```

To deny logs with severity greater than info:

```
switch(config-logging-filter)# 30 deny severity gt info
```

To deny logs with event ID 1024 and a message matching the regular expression LLDP:

```
switch(config-logging-filter)# 40 deny event-id 1024 includes LLDP
```

Denying all logs:

```
switch(config-logging-filter)# 40 deny
```

Changing the sequence ID of an existing rule:

```
switch(config-logging-filter)# resequence 20 70
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

logging facility

```
logging facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}
no logging facility
```

Description

Sets the logging facility to be used for remote syslog messages. Default: `local7`

The **no** form of this command disables the logging facility to be used for remote syslog messages.

Parameter	Description
`{local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}`	Selects the logging facility to be used for remote syslog messages. Required. Specifies the severity of the syslog messages: ▪ **local0** ▪ **local1** ▪ **local2** ▪ **local3** ▪ **local4** ▪ **local5** ▪ **local6** ▪ **local7**

Examples

Sets the local5 logging facility to be used for remote syslog messages:

```
switch(config)# logging facility local5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

logging persistent-storage

```
logging persistent-storage [severity {alert|crit|debug|emerg|err|info|notice|warning}]
no logging persistent-storage
```

Description

Enables or disables storage of logs in storage. Only logs of the specified severity and above will be preserved in the storage.

The **no** form of this command disables storage of logs in storage.

Parameter	Description
`severity <LEVEL>`	Specifies the severity of the syslog messages: ▪ **alert**: Preserves syslog messages with the severity of **alert (6)** and **emergency (7)**

Parameter	Description
	■ **crit**: Preserves syslog messages with the severity of **critical (5)** and above. Default. ■ **debug**: Preserves syslog messages with the severity of **debug (0)** and above. ■ **emerg**: Preserves syslog messages with the severity of **emergency (7)** only. ■ **err**: Preserves syslog messages with the severity of **err (4)** and above. ■ **info**: Preserves syslog messages with the severity of **info (1)** and above. ■ **notice**: Preserves syslog messages with the severity of **notice (2)** and above. ■ **warning**: Preserves syslog messages with the severity of **warning (3)** and above.

Usage

These logs can be copied out by using the **copy support-files all** or **copy support-files previous-boot**.

Examples

Enabling storage of logs in storage with severity **info**:

```
switch(config)#logging persistent-storage severity info
Logs will be written to storage and made available across reboot.
Do you want to continue (y/n)?
```

Disabling storage of logs in storage:

```
switch(config)# no logging persistent-storage
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Chapter 15
Service OS

Service OS is an operating system that the customer only uses to fix filesystem corruption, download and update firmware, and other support related issues. HPE Service OS is a Linux distribution that acts as a standalone bootloader and recovery OS for AOS-CX-based switches. It is only accessible if the user is consoled into the switch. The main high level features provided include:

- Access to file system partitions for retrieval of logs, coredumps, and configuration for supportability purposes.
- Filesystem utilities to format and partition a corrupted storage disk.
- Management interface networking with TFTP to download and update a product image.
- Ability to boot primary and secondary firmware images (.SWI file) on the storage disk.
- Support for clearing the AOS-CX startup-config.
- Ability to not only clear the admin password for AOS-CX, but also change it in SVOS.
- Ability to set the secure mode to enhanced or standard.

This document covers the customer CLI commands available in Service OS, as well as a few non-CLI features.

Service OS CLI login

Description

If the user enters 0 at the boot menu prompt, they will be presented with a Service OS CLI login prompt. The user must enter the login account "admin" to log in. By default, Service OS does not require a password.

To reboot without logging in, enter **reboot** as the login user name.

There are two additional login accounts that execute a command without requiring a password: **reboot** and **zeroize**. Enter the login account **reboot** to reboot the management module and **zeroize** to initiate a zeroization process. The zeroize user account helps a user reset the admin user account's password.

Example

```
ServiceOS GT.01.01.0001 switch ttyS0

To reboot without logging in, enter 'reboot' as the login user name.

switch login: admin

   Hewlett Packard
   Enterprise
SVOS>
```

```
ServiceOS GT.01.01.0001 switch ttyS0
```

```
To reboot without logging in, enter 'reboot' as the login user name.

switch login: reboot

   Hewlett Packard
   Enterprise
reboot: Restarting system
```

```
ServiceOS login: zeroize
This will securely erase all customer data, including passwords, and
reset the switch to factory defaults.
This action requires proof of physical access via a USB drive.
  * Create a FAT32 formatted USB drive
  * Create a file in the root directory of the USB drive named zeroize.txt
  * Type the following serial number into the zeroize.txt file: 772632X1830018
  * Insert the USB drive into the target module
  * Confirm the following prompt to continue

Continue (y/n)? y
############################WARNING############################
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
############################WARNING############################

Continue (y/n)? y

reboot: Restarting system
```

Service OS user accounts

Service OS provides a single admin login account. By default, no password is required to log in. Service OS will require a password if the Service OS admin user account password feature is enabled. This setting can be enabled or disabled in AOS-CX.

Service OS boot menu

Description

On boot, the user is presented with a Service OS version banner with version, build date, build time, build ID, and SHA strings.

The user is then shown the boot image profiles.

- Enter 0 to boot the Service OS login CLI.
- Enter 1 to boot the primary firmware image.
- Enter 2 to boot the secondary firmware image.
- If no input is given within 5 seconds, the default boot profile is selected. Alternatively, press Enter to select the default boot profile.

The image selected by the user during boot is a run-time decision only and will not persist across reboots. The default image can be configured using the `boot set-default` command.

Example

```
ServiceOS Information:
    Version:          GT.01.01.0001
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.10.xx.xxxx]
2. Secondary Software Image [XL.10.xx.xxxx]

Select profile(primary):
```

The (primary) string in the boot menu displays the default boot profile that will be booted after the timeout period. This string will change to (secondary) or (Service OS) depending on the current default boot option.

Console configuration

During boot, Service OS communicates with the RJ45 serial console with a baud rate of 115200. There is no option to change the baud rate during boot.

Additionally, if a USB console is connected to the management module console port, input will automatically be switched over to use the USB console. Automatic switching to USB is consistent with the AOS-CX USB console behavior.

Console output always displays on both the RJ45 console port and the USB console port.

AOS-CX boot

Description

After the user has input a boot profile selection at the boot menu or the 5-second selection timeout has expired, Service OS will boot an AOS-CX image.

Service OS displays the following boot strings embedded in the product image header:

- Image name
- Image version
- Build ID
- Build date

Service OS will then present status and boot the image.

Example

```
Booting primary software image...
Verifying Image...
Image Info:
```

```
        Name: AOS-CX
     Version: XL.01.01.0001
    Build Id: AOS-CX:XL.01.01.0001:1a36111da4e0:201707171452
  Build Date: 2017-07-17 14:52:27 PDT


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

File system access

Description

When the user logs in to the Service OS CLI, they are presented with a limited file system. The user can use standard file system commands of cd, ls, and pwd to view and move through the file system.

On login, the user is first placed in the /home directory:

```
(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP 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.

To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login: admin
SVOS> pwd
/home
SVOS>
```

The home directory and the USB device (/mnt/usb and any sub directory) are the only writable directories available. These directories can be used as a staging location for downloading product images using TFTP. /home can also be used as temporary storage before copying files from the management module through TFTP or USB. Any changes made to /home will not persist across reboots or after booting an AOS-CX image.

The root / directory displays viewable directories:

```
SVOS> ls /
bin       coredump  lib       mnt       selftest
cli       home      logs      nos
SVOS>
```

The directories coredump, selftest, nos, and logs each provide the user access to an SSD partition mount. The user may read, but not write any file on these partitions.

These mount points allow the user to copy files on the SSD to a USB storage device or upload files using TFTP. Copying files from the SSD is intended to be used under the guidance of a support engineer (to upload logs or coredumps to HPE support).

USB storage device access is provided through the mount at /mnt/usb.

The remaining directories in the root file system bin, cli, and lib are not intended to be used by the customer.

Service OS mount failure

Description

If the SSD is detected as missing or any of the partitions could not be mounted, Service OS will force the user to boot to the Service OS console and display an error message indicating that recovery should be attempted using the format command.

Example

```
(C) Copyright 2017 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP 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.

To reboot without logging in, enter 'reboot' as the login user name.

 Error, Could not mount the primary storage device.
 This may be due to filesystem or device corruption.
 Please attempt to recover using the "format" command.

ServiceOS login:
```

Service OS CLI command list

Description

After login to Service OS CLI, the user may enter the commands help or ? to get a full list of commands and a terse description for each command. The user may also enter <command> followed by --help to get more detailed help and usage for a specific command.

Example

```
SVOS> ?
Available Commands:

           ? - Display help screen
          cd - Change the working directory
         pwd - Print the current working directory
        help - Display help screen
        boot - Boot a product image
config-clear - Clears the startup-config
       erase - Securely erase storage devices on the management module
      format - Formats and partitions the primary storage device
    identify - Prints hardware identification information
          ip - Sets the OOBM Port Network Configuration
       mount - Mount a storage device
        ping - Send ICMP ECHO_REQUEST to network hosts (IPv4)
```

```
      reboot - Reboots the Management Module
    password - Set the admin account password
 secure-mode - Sets or retrieves the secure mode setting
          sh - Launch support shell
      umount - Unmounts a storage device
      update - Update a product image
     version - Prints ServiceOS release version information
         cat - Prints files to stdout
          cp - Copy files and directories
          du - Estimate file space usage
          ls - List directory contents
       md5sum - Compute and check md5 message digest
        mkdir - Make directories
          mv - Move (rename) files
          rm - Remove files or directories
       rmdir - Remove empty directories
        tftp - Allows transfer of files to/from a remote machine
        exit - Logout

Enter '<command> --help' for more info
```

Service OS CLI features and limitations

The Service OS CLI provides basic shell functionality that allows you to execute commands and pass arguments to those commands only. The following features are not available:

- Input/output redirection (<, >, >>)
- Job control (&, fg, bg)
- Process piping (|)
- File globbing (*)

Even though the Service OS CLI does not provide file globbing capabilities, some commands may provide this functionality internally. An example is the `ls` command.

The following common features are available:

- Command history (Up Arrow) and search (Ctrl-R)
- Tab completion for file and folder names (not CLI commands)
- Command abort using Ctrl-C

Service OS CLI commands

boot

`boot`

Description

Presents you with the boot menu prompt. You can then specify which boot profile: primary, secondary, or Service OS console.

Example

Presenting the boot menu prompt:

```
SVOS> boot

ServiceOS Information:
    Version:          GT.01.01.0005
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.01.01.0001]
2. Secondary Software Image [XL.01.01.0001]

Select profile(primary):
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

cat

`cat <FILENAME/DIRECTORY-NAME>`

Description

Prints the contents of a file to the console. The Service OS does not allow command output redirection, so this command is only useful for reading short text files.

Parameter	Description
<FILENAME/DIRECTORY-NAME>	Shows the contents of the specified file or directory.

Example

Showing the contents of /nos/hosts:

```
SVOS> cat /nos/hosts
127.0.0.1       localhost.localdomain           localhost

SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

cd path

`cd path`

Description

Changes the current working directory.

Example

Changing the current working directory:

```
cd /
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

config-clear

`config-clear`

Description

Configures the switch to set all configuration settings to factory default when the switch is restarted. The next time the switch starts, the current **startup-config** is renamed to **startup-config-fixme**, and a new **startup-config** is created with factory default settings.

Using this command is not the same as performing zeroization, which securely erases the entire primary storage and other devices, and not just the configuration.

Example

Configuring the system to clear the switch configuration:

```
SVOS> config-clear

The switch configuration will be cleared.

Continue (y/n)? y
The system has been configured to clear the startup-config on the next
boot. Please execute the 'boot' command to complete this action.
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

cp

`cp [options] <SOURCE-FILENAME/SOURCE-DIRECTORY> <DESTINATION-FLENAME/DESTINATION-DIRECTORY>`

Description

Copies files or directories.

Parameter	Description
[options]	Selects the options for the command.
-d,-P	Specifies the preservation of symlinks (default if **-R**).
-a	Same as **-dpR**.
R,-r	Specifies recursiveness, all files, and subdirectories are copied.
-L	Specifies the following of all symlinks.
-H	Specifies the following of symlinks on command line.
-p	Specifies the preservation of file attributes if possible.
-f	Specifies the overwriting of a file or directory.
-i	Specifies the prompting before an overwrite.

Parameter	Description
`-l,-s`	Specifies the creation of (sym) links.
<SOURCE-FILENAME/SOURCE-DIRECTORY>	Specifies the name of the source file or directory.
<DESTINATION-FLENAME/DESTINATION-DIRECTORY>	Specifies the name of the destination file or directory.

Example

Copying /home/customers directory to the /home/clients directory:

```
SVOS> cp /home/customers /home/clients
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

du

`du [options] <FILENAME/DIRECTORY-NAME>...`

Description

Shows estimated disk space used for each file or directory or both.

Parameter	Description
`[options]`	Selects the options for the command.
`-a`	Show file sizes.
`-L`	Shows all symlinks.
`-H`	Shows symlinks on a command line.
`-d, N`	Shows limited output to directories (and files with **-a**) of depth less than **N**.
`-c`	Shows the total disk space usage of all files or directories or both.
`-l`	Shows the count sizes if hard linked.

Parameter	Description
`-s`	Shows only a total for each argument.
`-x`	Does not show directories on different file systems.
`-h`	Show sizes in human readable format (1K, 243M, and 2G).
`-m`	Show sizes in megabytes.
`-k`	Show sizes in kilobytes (default).
<FILENAME/DIRECTORY-NAME>	Specifies the file or directory or both for displaying a size estimate.

Example

Estimating disk space for the /nos directory:

```
SVOS> du -ah /nos
196.4M  /nos/primary.swi
196.4M  /nos
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

erase zeroize

`erase zeroize`

Description

Securely erases any user data contained on the SSD or other storage devices on the management module.

Back up all data before running this command or all user/config data will be lost.

Usage

Use this command to securely erase all customer data and restore the software environment to factory default. When you issue this command:

- Software images are copied to RAM to be restored on completion.
- All bits undergo a 0>1>0 transition to completely zeroize data. This data is not recoverable.
- This feature can be used to remove all configuration settings or system alterations for debugging or troubleshooting.
- The zeroization process takes approximately two minutes.

All logs and data are lost in the zeroization process. Best practices is to collect all applicable data before performing zeroization.

Example

Erasing user data:

```
SVOS> SVOS> erase --help
Usage: erase zeroize

Securely erases storage devices on the management module.
SVOS>
```

```
SVOS> erase zeroize
##############################WARNING###############################
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
##############################WARNING###############################

Continue (y/n)? y
reboot: Restarting system

ServiceOS Information:
    Version:          GT.01.01.0001
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193

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

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

################ Restoring files ############################
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

exit

`exit`

Description

Logs the user out from the `SVOS>` prompt.

Example

Loging the user out from the `SVOS>` prompt:

```
SVOS> exit

(C) Copyright 2024 Hewlett Packard Enterprise Development LP

                      RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP 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.

To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login:
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

format

`format`

Description

Configures the primary storage device with the correct partition and file system formatting. This command removes all pre-existing data on the primary storage device.

Example

Configuring the primary storage device with the correct partition and file system formatting:

```
SVOS> format
###################WARNING####################
The following action will cause all data on
the primary storage device to be lost. After
formatting has completed, a reboot will be
initiated to complete storage initialization.
###################WARNING####################

Continue? (y/n): y

Working...This may take a few minutes...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

identify

identify

Description

Prints the version of the SVOS and of the UEFI BIOS.

Example

Printing the version of the SVOS and of the UEFI BIOS:

Output from an 8320 switch:

```
SVOS> identify
mc svos_primary           : TL.01.01.0004
mc svos_secondary         : TL.01.01.0004
mc cpld/1                 : 8
mc cpld/2                 : 7
mc cpld/3                 : 7
mc uefi                   : TL-01-0013
mc uefi_capsule           : TL-01-0013
Support Info              : SE:0
```

Output from an 8325 switch:

```
SVOS> identify
mc svos_primary           : GL.01.01.0004
mc svos_secondary         : GL.01.01.0004
mc uefi                   : GL-01-0010
```

```
mc uefi_capsule            : GL-01-0010
Support Info               : SE:0
```

Output from a 9300 switch:

```
SVOS> identify
mc svos_primary            : CL.01.01.0004
mc svos_secondary          : CL.01.01.0004
mc uefi                    : CL-01-0010
mc uefi_capsule            : CL-01-0010
Support Info               : SE:0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip

`ip {show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}`

Description

Shows or configures the port with a static IP address (IPv4 only) or enables the DHCP client on the port. An address is set only if a DHCP server is available to provide one.

Parameter	Description
`{show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}`	Selects the options for the OOBM port.
`show`	Shows the OOBM port.
`dhcp`	Configures the port with a DHCP address.
`disable`	Disables the OOBM port.
`addr <ADDR-NETMASK-GATEWAY>`	Configures the port with a static IP address (IPv4 only). Specify address, netmask, and gateway as A.B.C.D.

Example

Configuring the port with a DHCP IP address:

```
SVOS> ip dhcp
SVOS> ip show
Interface  : Link Up
IP Address : 10.0.26.17
Subnet Mask: 255.255.252.0
Gateway    : 10.0.24.1

SVOS> ip disable
SVOS> ip show
Interface : Disabled
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8360 9300 10000	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

ls

`ls [<OPTIONS>] [<FILE-NME>]`

Description

This command lists directory contents.

Parameter	Description
<OPTIONS>	Specifies options for the command.
`-1`	Shows one-column output.
`-a`	Shows entries which start with a period (.).
`-A`	Shows output similar to **-a**, but excludes a period (.) and a double period (..).
`-C`	Shows output list by columns.
`-x`	Shows output list by lines.
`-d`	Shows listing of directory entries instead of contents
`-L`	Follows symlinks.

Parameter	Description
`-H`	Follows symlinks on the command line.
`-R`	Recurse.
`-p`	Appends a slash (/) to directory entries.
`-F`	Appends an indicator to entries. An indicator can be as an asterisk (*) or slash (/) or equal sign (=) or at sign (@) or pipe (|).
`-l`	Shows the output in a long listing format.
`-i`	Shows the list inode numbers.
`-n`	Shows a list of numeric UIDs and GIDs instead of names.
`-s`	Shows a list of allocated blocks.
`-e`	Shows in one column a list with the full date and time.
`-h`	Shows list sizes in human readable format (1K, 243M, 2G) with a one-column output.
`-r`	Shows in one column a sort in reverse order.
`-S`	Shows in one column a sort by size.
`-X`	Shows in the output sort by extension.
`-v`	Shows in one column a sort by version.
`-c`	With **-l**, it shows a sort in one column by **ctime**.
`-t`	With **-l**, it shows a sort by **mtime**.
`-u`	With **-l**, sort by **atime**.
`-c`	With **-l**, it shows a sort in one column by **ctime**
`-w <N>`	Assumes that the terminal has the number of columns wide as specified by <*N*>.
`--color[={always | never | auto}]`	Controls color in the output.
<FILE-NAME>	Specifies the name of the file to list.

Example

Listing directory contents:

```
SVOS> ls -la /nos
drwxr-xr-x    3 0        0             4096 Nov 21 03:19 .
drwxr-xr-x   11 0        0              220 Nov 21 03:21 ..
drwx------    2 0        0            16384 Nov 21 03:20 lost+found
-rwxr-xr-x    1 0        0        205957424 Nov 21 03:19 primary.swi
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

md5sum

`md5sum [-c | -s | -w] [<FILE-NAME>]`

Description

This command computes and checks the MD5 message digest.

Parameter	Description
`[-c | -s | -w]`	Selects the options for the command.
`-c`	Specifies to check the sums against the list in files.
`-s`	Specifies not output anything, status code shows success.
`-w`	Specifies to warn about improperly formatted checksum lines.
<FILE-NAME>	Specifies the file name to run the checksum against.

Example

Computing and checking the MD5 message digest for /nos/primary.swi:

```
SVOS> md5sum /nos/primary.swi
93ffc89e7ec357854704d8e450c4b7ab  /nos/primary.swi
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

mkdir

`mkdir [-m | -p] [<DIRECTORY-NAME>]`

Description

This command makes directories.

Parameter	Description
`[-m | -p]`	Specifies the options for the command.
`-m`	Specifies the mode.
`-p`	Specifies to make parent directories as needed with no errors for pre-existing directories.
<DIRECTORY-NAME>	Specifies the directory to create.

Example

Making the dir directory:

```
SVOS> mkdir dir
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

mount

`mount <DEVICE>`

Description

This command mounts the SSD partitions to the following locations: **/coredump**, **/logs**, **/nos**, **/selftest**, and mounts the USB device to **/mnt/usb**.

Users can mount USB flash drives formatted as either FAT16 or FAT32 with a single partition.

Parameter	Description
<DEVICE>	Specifies the device to be mounted. Supported device options include `all` and `usb`.

Examples

Mounting all of the SSD partitions:

```
SVOS> mount all
SVOS> mount usb
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

mv

`mv [-f | -i | -n] <TARGET-DIRECTORY>`

Description

This command moves (renames) files.

Parameter	Description
`-f`	Specifies not to prompt before overwriting.
`-i`	Specifies to prompt before overwriting.
`-n`	Specifies to not overwrite an existing file.

Example

Moving the file named myfile:

```
SVOS> mv myfile
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

password (svos)

```
password
```

Description

Sets the admin user account password for both Service OS and AOS-CX once the user boots into AOS-CX and saves the configuration. This will overwrite the previous password if one exists. User input is masked with asterisks.

This command is not available if enhanced secure mode is set.

Example

Setting the admin account password:

```
SVOS> password
Enter password:********
Confirm password:********
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ping

```
ping <HOST-IP-ADDRESS>
```

Description

Pings network hosts for debug purposes.

Parameter	Description
<HOST-IP-ADDRESS>	Specifies the host IP address.

Example

Pinging a network host:

```
SVOS> ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10): 56 data bytes
64 bytes from 10.0.8.10: seq=0 ttl=63 time=3.496 ms
64 bytes from 10.0.8.10: seq=1 ttl=63 time=0.367 ms
64 bytes from 10.0.8.10: seq=2 ttl=63 time=0.380 ms
```

```
64 bytes from 10.0.8.10: seq=3 ttl=63 time=0.282 ms
64 bytes from 10.0.8.10: seq=4 ttl=63 time=0.669 ms
^C
--- 10.0.8.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.282/1.038/3.496 ms
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8360 9300 10000	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

pwd

`pwd`

Description

Displays the current working directory.

Example

Displaying the current working directory:

```
SVOS> pwd
/home
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

reboot

`reboot`

Description

Reboots the Management Module.

Example

Rebooting the management module:

```
SVOS> reboot
reboot: Restarting system
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

rm

`rm [-f | -i | -R | -r] <FILE-NAME>`

Description

Removes files or directories.

Parameter	Description
`[-f | -i | -R | -r]`	Selects the options for removing files or directories.
`-f`	Never prompt before removing files or directories.
`-i`	Always prompt before removing files or directories.
`-R | -r`	Recursive.

Example

Removing the file named **foo**:

```
SVOS> rm foo
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

rmdir

`rmdir [-p] <DIRECTORY-NAME>`

Description

Removes empty directories.

Parameter	Description
-p	Specifies to remove parent directories.

Example

Removing the empty **foo** directory:

```
SVOS> rmdir foo
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

secure-mode

`secure-mode <enhanced | standard | status>`

Description

Sets the secure mode to enhanced or standard secure mode. Also can display the current secure mode. A zeroization is required before switching between enhanced and standard secure modes.

The command also displays a message notifying the user that they are already in the targeted secure mode.

Example

Setting the secure mode to enhanced or standard:

```
SVOS> secure-mode --help
Usage: secure-mode <enhanced | standard | status>

Set or retrieve the secure mode setting. Requires a zeroization to change modes.
SVOS>
```

```
SVOS> secure-mode enhanced
############################WARNING############################
This will set the switch into enhanced secure mode.  Before
enhanced secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
############################WARNING############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode standard
############################WARNING############################
This will set the switch into standard secure mode.  Before
standard secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
############################WARNING############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode standard
############################WARNING############################
Secure mode is already set to standard.  Setting it again will
repeat the zeroization process.  The switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
############################WARNING############################

Continue (y/n)? y
reboot: Restarting system
```

```
SVOS> secure-mode status
enhanced secure mode is set.
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

sh

```
sh
```

Description

Launches a bash shell for support purposes. To quit bash, enter **exit**.

This command is not available if enhanced secure mode is set.

Example

Launching a bash shell:

```
SVOS> sh
switch:/cli/fs/home#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

system serviceos password-prompt

```
system serviceos password-prompt
no system serviceos password-prompt
```

Description

Use this command to enable password authentication for ServiceOS. By default, the ServiceOS shell (accessible only from the local switch console port) requires no password to login as an admin use.

When this setting is enabled, the same password used to authenticate the admin user in the AOS-CX CLI or WeUI can be used to log in to the ServiceOS shell. If this setting is enabled, a forgotten admin user password cannot be reset using ServiceOS; if there are no other local or RADIUS/TACACS user accounts

with administrator-level access, the switch must be zeroized by entering the **username zeroize** command at the ServiceOS login prompt to restore administrator access.

Example

Enablling password authentication for ServiceOS

```
switch(config)# system serviceos password-prompt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

umount

`umount <DEVICE>`

Description

Unmounts the SSD partitions mounted to the following locations: **/coredump**, **/logs**, **/nos**, **/selftest**, and unmounts the USB device mounted to **/mnt/usb**.

Parameter	Description
<DEVICE>	Specifies the device to be unmounted. Supported device options include **all** and **usb**.

Examples

Unmounting all devices:

```
SVOS> umount all
SVOS> umount usb
```

Unmounting a USB device:

```
SVOS> umount all
SVOS> umount usb
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

update

`update {primary | secondary} <IMAGE>`

Description

Verifies and installs a product image. The user can select the primary or secondary boot profile to update and the location of the file.

Parameter	Description
`{primary | secondary}`	Selects either the primary or secondary image.
<IMAGE>	Specifies the image name.

Examples

Updating the software image using TFTP:

The OOBM port is disabled on first boot and must be enabled using the **ip** command.

```
SVOS> ip dhcp
SVOS> ip show
Interface  : Link Up
IP Address : 192.0.2.22
Subnet Mask: 255.255.200.20
Gateway    : 10.0.24.1
SVOS> tftp -g -r XL.10.00.0001.swi -l image.swi 192.4.8.10
XL.10.00.0001.swi 100% |******************************|   178M  0:00:00 ETA
SVOS> ls
image.swi
SVOS> update primary image.swi
Updating primary software image...
Verifying image...
Done
```

Update the software image using USB:

This example assumes that the user has preloaded a USB flash drive with the image to be updated. The image name on the flash drive is not important.

```
SVOS> mount usb
SVOS> ls /mnt/usb
image.swi
SVOS> update primary /mnt/usb/image.swi
Updating primary software image...
Verifying image...
Done
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

tftp

`tftp {-b | -g | -l <LOCAL-FILE> | -p | -r <REMOTE-FILE>} host [<PORT>]`

Description

Transfers files to and from a remote machine (TFTP a file).

Parameter	Description
`{-b | -g | -l | -p | -r <REMOTE-FILE>}`	Selects the options for transferring a file.
`-b`	Specifies the transfer blocks of size octets. The default blocksize is set to 1468, which can be overridden with the -b option.
`-g`	Specifies to get a file.
`-l`	Specifies a local file.
`-p`	Specifies to put a file in remote location.
`-r <REMOTE-FILE>`	Specifies a remote file.
<PORT>	Specifies the port for transfer. If no port option is specified, TFTP uses the standard UDP port 69 by default.

Example

Transferring files:

```
SVOS> tftp -b 65464 -g -r XL.10.00.0002.swi.swi 192.0.2.1
XL.10.00.0002 100% |*******************************|   178M  0:00:00 ETA
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8360 9300 10000	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

version

`version`

Description

Displays the following build strings:

- Version.
- Build date.
- Build time.
- Build ID.
- SHA.

Example

Displaying version build strings:

```
SVOS> version
ServiceOS Information:
    Version:          GT.01.01.0001
    Build Date:       2017-07-19 14:52:31 PDT
    Build ID:         ServiceOS:GT.01.01.0001:461519208911:201707191452
    SHA:              46151920891195cdb2267ea6889a3c6cbc3d4193
SVOS>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (`SVOS>`)	Administrators or local user group members with execution rights for this command.

Chapter 16
In-System Programming

The ISP (In-System Programming) feature provides an automated way to roll out updates to various programmable devices in an AOS-CX network switch, after the product has shipped. ISP is intended to run automatically either at boot time or as new modules are inserted into the chassis at runtime.

Show tech command list for the ISP feature

Task	Command
Displaying versions of all present programmable devices.	`show tech isp`
Displaying stored log files from any ISP updates on the system.	`show tech update-log`

See the *Command-Line Interface Guide* for additional information about the `show tech` commands.

In-System Programming commands

clear update-log

```
clear update-log
```

Description

Clears stored log files of any In-System Programming updates on the system.

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show needed-updates

```
show needed-updates [next-boot [primary|secondary]]
```

Description

Displays whether any programmable devices are in need of an update.

Without the **next-boot** parameter, this command displays needed updates relative to the currently running AOS-CX image.

With the **next-boot** parameter, this command displays needed updates relative to an AOS-CX image file in the persistent storage of the switch, which might be different from the currently running image. If either the **primary** or **secondary** parameter is specified, this command queries that specific AOS-CX image file. Otherwise, it queries the default AOS-CX image file as set by the most recent **boot system** or **boot set-default** command.

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Chapter 17
Selftest

The 8320 switch only supports Boot-up Diagnostics (Power On Selftest aka POST).

Power On Self Test (POST) is the first task which verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST comprises of the following:

- **Register read/write**

  This test checks for the registers and tables in the ingress pipeline of ASIC. It is always run during platform initialization only.
- **Front-end Port Loopback tests**

  This is to verify the physical port front-end interface.

  These tests check if a particular interface can function properly. A test failure would mean that the particular interface is marked as "Failed" and thus it would become unavailable for use.

  This test is run when "no fastboot" is configured.

Selftest commands

fastboot

```
fastboot
no fastboot
```

Description

Enables fastboot for the system.

The **no** form of this command disables fastboot for the system.

Usage

When fastboot is enabled, most tests under a Power On Self Test (POST) are skipped. By default, fastboot is enabled.

After disabling fastboot, save switch configurations and then reboot for POST to run. POST verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST runs memory built-in selftest (BISTs) and front-end port loopback tests. Memory BISTs verify the internal and external memory blocks present in the module. The memory tables are critical for proper functionality of the system so any failures in these tests results in the corresponding subsystem to be marked as "Failed" and thus that subsystem is not available for use.

Front-end port loopback tests verify the physical port front-end interface. These tests check if a particular interface can function properly. A test failure means that a particular interface has been marked as "Failed" and is now unavailable for use.

Examples

Enabling fastboot:

```
switch# configure terminal
switch(config)# fastboot
switch(config)# end
switch# show running-config
Current configuration:
!
!Version AOS-CX ML.10.06.0001
module 1/1 product-number jl726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number jl661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number jl363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
    no routing
```

Disabling fastboot:

```
switch# configure terminal
switch(config)# no fastboot
switch(config)# end
switch(config)# write mem
Configuration changes will take time to process, please be patient.
switch# show running-config
Current configuration:
!
!Version AOS-CX ML.10.06.0001
module 1/1 product-number jl726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number jl661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number jl363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
    no routing
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show selftest

```
show selftest [brief] [vsx-peer]
show selftest line-module <SLOT-ID>
show selftest line-module <SLOT-ID> interface [brief] [vsx-peer]
show selftest interface [<PORT-NUM>] [vsx-peer]
```

Description

Displays selftest results.

Parameter	Description
`[brief]`	Shows the selftest results as a brief description. Default.
`line-module`	Shows the selftest results for a line module.
<SLOT-ID>	Shows the selftest results for the slot ID of the line or fabric module.
<PORT-NUM>	Shows the selftest results for the port number.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying the output when fastboot is disabled on an 8320 switch:

```
switch# show selftest interface



Name       Status            ErrorCode        LastRunTime

---------- ----------------- ---------------- -------------------

1/1/2      skipped           0x0

1/1/44     skipped           0x0

1/1/46     skipped           0x0
```

```
switch# show selftest interface 1/1/1

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- -------------------
1/1/1      skipped           0x0
```

Displaying the output when fastboot is enabled:

```
switch# show selftest interface 1/1/2
Name    Status         ErrorCode LastRunTime
------- -------------- --------- -------------------
1/1/2   skipped        0x0

switch# show selftest line-module 1/1 interface
Name    Status         ErrorCode LastRunTime
------- -------------- --------- -------------------
1/1/1   skipped        0x0
1/1/2   skipped        0x0
1/1/3   skipped        0x0
1/1/31  skipped        0x0
```

Displaying the output when fastboot is disabled:

```
switch# show selftest interface

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- -------------------
1/1/12     passed            0x0              2018-02-16 18:15:53
1/1/47     passed            0x0              2018-02-16 18:15:53
1/1/15     passed            0x0              2018-02-16 18:15:53

switch# show selftest interface 1/1/1

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- -------------------
1/1/1      passed            0x0              2018-02-16 18:15:53
```

Testing to register read/write:

This test is run irrespective of fastboot being enabled or disabled.

```
switch# show selftest

Name       Id   Status         ErrorCode  LastRunTime
---------- ---- -------------- ---------- -------------------
LineModule 1/1  passed         0x0        2018-02-16 18:15:53
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Chapter 18
Zeroization

Device zeroization lets you remove all user files from flash storage, including solid-state drives (SSDs). User files cannot be retrieved after the zeroization is complete.

Zeroization can occur in both AOS-CX and Service OS. This section covers zeroization and AOS-CX. For information about zeroization and Support OS, see erase zeroize.

Zeroization preserves the primary and secondary software images on the SSD. Zeroization also preserves manufacturing information.

The sensitive user files stored on an SSD or SPI flash/EEPROM storage or both include:

- Switch configurations.
- System generated private keys.
- User installed private keys.
- Admin/operator password files.

Using CLI, you can change the switch settings from standard secure mode to enhanced secure mode. Setting the switch back to standard secure mode can only be performed through Service OS. For more information on how to change switch settings using Server OS, see Service OS.

Enhance secure mode is used to enhance the switch security. In enhanced security mode, the switch (Product OS) `start-shell` command is disabled for security purpose except through ServiceOS.

Zeroization commands

erase all zeroize

```
erase [all] zeroize
```

Description

Restores the switch to its factory default configuration. You will be prompted before the procedure starts. Once complete, the switch will restart from the primary image with factory default settings.

Usage

The **erase all** command is always available in the CLI. On running the **erase all** command, the switch is restored to a factory default settings, but retains the enhanced secure mode settings.

The **erase all zeroize** command is not available in the CLI when enhanced secure mode is enabled. This command restore the switch to a factory default settings. On running the **erase all zeroize** command in enhanced secure mode, displays a notification stating that the command is unavailable in enhanced secure mode.

Back up all data before running this command as all configuration settings will be lost.

Example

Restoring the switch to factory default configuration, except for the enhance secure mode settings:

```
switch# erase all
This command will erase all data and reset the switch to factory
defaults, with the exception of the secure mode setting. This process
will take several minutes to an hour to complete and the switch will
be unavailable during that time.
Continue (y/n)?
ServiceOS Information:
Version: GT.01.01.0007
Build Date: 2017-12-07 11:48:44 PST
Build ID: ServiceOS:GT.01.01.0007:42c7d15cf7e5:201712071148
SHA: 42c7d15cf7e5af5bf1c7d8764ff673471084c2a4
################ Preparing for zeroization #################
################ Storage zeroization #######################
################ WARNING: DO NOT POWER OFF UNTIL ##########
################ ZEROIZATION IS COMPLETE ##########
################ This should take several minutes ##########
################ to one hour to complete ##########
################ Restoring files ###########################
```

Restoring the switch to factory default configuration only when enhance secure mode settings is disabled.

```
switch# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)? y
The system is going down for zeroization.

...

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


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


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

...

We'd like to keep you up to date about:
  * Software feature updates
  * New product announcements
  * Special events
Please register your products now at: https://asp.arubanetworks.com
```

When you log in after zeroization, you get a prompt to create a password for the administrator account. You can set the password as blank (to set the password as blank, hit enter at the prompt) or type 1 to 32 printable ASCII characters, excluding spaces and question marks (?). For more information on password requirements, see *Password requirements* in the *Security Guide*.

```
switch login: admin
Password:


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

Command History

Release	Modification
10.11.1010	Introduced **erase all** CLI command
10.07 or earlier	--

Command Information

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

Chapter 19
Terminal Monitor

The terminal monitor is used to display selective logs dynamically on the VTYSH session. When the terminal monitor feature is enabled on the switch, it displays only the live or active logs. These logs are displayed on the SSH session or console session. If required, you can enable the terminal monitoring on multiple sessions.

It is important to monitor the logs dynamically while debugging, so that you can co-relate the issues. The logs can be filtered by type (event or debug), severity, or keyword. The terminal monitor runs in synchronous mode, where the user enters any command, the log display pauses until the command execution is complete. This ensures that the logs will not appear in between other CLI outputs or while the user is typing.

Terminal monitoring is not persistent in the SSH session. If the SSH session is terminated, the terminal monitor is no longer valid. However, logging console is persistent and is added to the switch configuration, so it will persist between telnet sessions.

Terminal monitor commands

logging console {notify | severity | filter}

```
logging console{notify <event|debug|all> | severity <level> | filter keyword}

no logging console
```

Description

Enables the logging console feature in the console session. It display all debug log or event log or both debug and event log messages. Monitoring can be filtered with the severity options or with the help of keywords. Enabling terminal monitor without options displays both debug and event log with a severity error. This command is persistent across reboot.

The **no** form of this command disables the terminal monitor configuration.

Parameter	Description
`notify <event|debug|all>`	Specifies the type of log notification. ■ **Event:** Displays the event log messages. (Default) ■ **Debug:** Displays the debug log messages. ■ **All:** Displays both event and debug log messages.
`severity <level>`	Specifies the severity level for the logs. The different severity levels are emergency, critical, error, warning, notice, information (default), alert, and debug (shows all severities).
`filter <keyword>`	Specifies the filter by applying keyword for the logs.

Authority

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

Examples

Configuring console logging in the console session:

```
switch(config)# logging console
Terminal-monitor is enabled successfully

switch(config)# logging console notify all
Terminal-monitor is enabled successfully

switch(config)# logging console notify event severity info
Terminal-monitor is enabled successfully

switch(config)# logging console filter lldp
Terminal-monitor is enabled successfully
```

Command History

Release	Modification
10.08	Feature introduced.

Command Information

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

show terminal-monitor

`show terminal-monitor`

Description

Shows whether the terminal monitoring is enabled or disabled.

This command will not show any information about console logging.

Examples

Displaying terminal monitor when enabled:

```
switch# show terminal-monitor

Terminal-monitor is enabled
-------------------------------------
Notify     | Severity   | Filter
-------------------------------------
event        debug        lldp
-------------------------------------
```

Displaying terminal monitor when disabled:

```
switch# show terminal-monitor

Terminal-monitor is disabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

terminal-monitor {notify | severity | filter}

```
terminal-monitor {notify <event|debug|all> | severity <level> | filter <keyword>}

no terminal-monitor
```

Description

Enables and saves the terminal monitor feature in the switch configuration. It displays all debug log or event log or both debug and event log messages. Terminal monitoring can be filtered with the severity options or with the help of keywords. Enabling terminal monitor without options displays both debug and event log with a severity error.

The **no** form of this command removes the terminal monitor feature from the switch configuration and the command will not persist.

Parameter	Description
`notify <event|debug|all>`	Specifies the type of log notification. ▪ **Event:** Displays the event log messages. (Default) ▪ **Debug:** Displays the debug log messages. ▪ **All:** Displays both event and debug log messages.
`severity <level>`	Specifies the severity level for the logs. The different severity levels are emergency, critical, error, warning, notice, information (default), alert, and debug (shows all severities).
`filter <keyword>`	Specifies the filter by applying keyword for the logs.

Authority

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

Examples

Enabling terminal monitor:

```
switch# terminal-monitor
Terminal-monitor is enabled successfully

switch# terminal-monitor notify all
Terminal-monitor is enabled successfully

switch# terminal-monitor notify event severity info
Terminal-monitor is enabled successfully

switch# terminal-monitor filter lldp
Terminal-monitor is enabled successfully
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

The following section describes symptoms, causes and corrective actions for 401 or 404 errors.

HTTP 404 error when accessing the switch URL

Symptom

The switch is operational and you are using the correct URL for the switch, but attempts to access the REST API or Web UI result in an HTTP 404 "Page not found" error.

Cause

REST API access is not enabled on the VRF that corresponds to the access port you are using. For example, you are attempting to access the REST API or Web UI from the management (OOBM) port, and access is not enabled on the `mgmt` VRF.

Action

Use the `https-server vrf` command to enable REST API access on the specified VRF.

For example:

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

HTTP 401 error "Login failed: session limit reached"

Symptom

A REST request or Web UI login attempt returns response code 401 and the response body contains the following text string:

```
Login failed: session limit reached
```

Cause

A user attempted to log into the REST API or the Web UI, but that user already has the maximum number of concurrent sessions running.

Action

1. Log out from one of the existing sessions.

   Browsers share a single session cookie across multiple tabs or even windows. However, scripts that POST to the login resource and later do not POST to the logout resource can easily create the maximum number of concurrent sessions.
2. If the session cookie is lost and it is not possible to log out of the session, then wait for the session idle time limit to expire.

   When the session idle timeout expires, the session is terminated automatically.

3. If it is required to stop all HTTPS sessions on the switch instead of waiting for the session idle time limit to expire, you can stop all HTTPS sessions using the `https-server session close all` command.

   This command stops and starts the `hpe-restd` service, so using this command affects all existing REST sessions, Web UI sessions, and real-time notification subscriptions.

Chapter 21

Support and Other Resources

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
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:

HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about
Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Software Technical Update channel on	Videos on new features introduced in this release: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

YouTube.	
HPE Aruba Networking Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm
HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://licensemanagement.hpe.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://networkingsupport.hpe.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://networkingsupport.hpe.com/notifications/subscriptions (requires an active HPE Aruba Networking support account to manage subscriptions). Security notices are viewable without a networking support 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.