AOS-CX 10.09 Diagnostics and Supportability Guide

4100i, 6000, 6100 Switch Series

a Hewlett Packard Enterprise company

Published: February 2022
Edition: 2

Open Source Code

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

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

Notices

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

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

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

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 4100i Switch Series (JL817A, JL818A)
- Aruba 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A)
- Aruba 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)

Latest version available online

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

Command syntax notation conventions

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

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

About the examples

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

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

Understanding the CLI prompts

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

```
switch>
```

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

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

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

Indicates the configuration context for a feature. For example:

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

Identifies the `interface` context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

member/slot/port

On the 4100i 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.

On the 6000 and 6100 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.

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 above.

Parameter	Description
`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
```

Description

Displays the enabled debug types.

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        default
```

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
```

Description

Displays the configured debug destination and severity.

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.

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

Only logs stored in the following files are rotated:

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

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.

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 | event-log} <THRESHOLD%>
no logging threshold {audit-log | auth-log | event-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 of 90 (percent).

Parameter	Description
`audit-log`	Selects the audit log.
`auth-log`	Selects the authentication log.
`event-log`	Selects the event log.
<THRESHOLD%>	Selects the notification threshold as a percent that the selected logging buffer is full. Available percent values for `auth-log`, `event-log`, `security 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 security log threshold:

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

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 security log threshold to its default of 90:

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

Command History

Release	Modification
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`. `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.
- Log storage locations on the switch included in the log rotate are as follows:
  - Authentication logs are stored in `/var/log/auth.log`.
  - Event logs are stored in `/var/log/audit/audit.log`.
  - Audit logs are stored in `/var/log/event.log`.
  - Logs of bad login attempts are stored in `/var/log/btmp`.
  - Logs of the last login sessions are stored in `/var/log/wtmp`.
  - NTP logs are stored in `/var/log/ntp.log`.

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
```

Description

Shows the log rotate configuration.

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
Switch system and hardware commands

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

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

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.

The Time-Domain Reflectometer (TDR) feature helps characterize and locate cable faults in the twisted wire pairs. 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 1GbT ports.

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.
`open`	The MDI pair is not terminated with a link partner or has an open circuit.
`short`	The MDI pair is shorted within itself (intra-short).
`inter_short`	The MDI pair is shorted with another pair (inter-short).
`high_impedance`	The MDI pair has high-impedance mismatch and is not guaranteed to link up.
`low_impedance`	The MDI pair has low-impedance mismatch and is not guaranteed to link up.
`failed`	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, or link partner is not configured for auto-negotiation, or link partner is busy establishing the link.
2.5G-SmartRate	Interface is busy.
5G-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 within +/-10m.
2.5G-SmartRate	When diagnostic status is "good", cable length is not reported (0m).
5G-SmartRate	When diagnostic status is "good", cable length is not reported (0m).

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 +/-5m.
2.5G-SmartRate	When diagnostic status is not "good" or "failed", distance to fault is reported within +/-5m.
5G-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 <IF-NAME>`

Description

Runs a cable diagnostic test on an interface.

Parameter	Description
<IF-NAME>	Specifies the name of the interface.

Examples

Running a cable diagnostic test on interfaces:

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

           MDI    Cable       Distance   MDI
Interface  Pair   Status      to Fault   Mode
                              (Meters)
-----------------------------------------------
1/1/1      1-2     good       5          mdi
           3-6     good       5          mdi
           4-5     good       5          mdi
           7-8     open       3

switch# diag cable-diagnostic 1/1/2
This command will cause a loss of link on the port under test and will take
several seconds to complete.
Continue (y/n)? y

           MDI    Cable       Distance   MDI
Interface  Pair   Status      to Fault   Mode
                              (Meters)
-----------------------------------------------
1/1/2      1-2     good       5          mdix
           3-6     good       5          mdix
           4-5     short      1
           7-8     good       5          mdix
```

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

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.

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`
	`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://` *<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 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 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`. 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>`
`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
```

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 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.

Parameter	Description
	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

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

Parameter	Description
<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

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.

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 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>}
```

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.
`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` 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.

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 another device is alive. It also measures the amount of time it 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 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}]
```

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).

Parameter	Description
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 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> |
   vrf <VRF-NAME> | source <IPv6-ADDR> | <IFNAME>]
```

Description

Pings the specified IPv6 address or hostname with or without optional parameters.

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.

Parameter	Description
`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.
`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
```

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.

Action

1. Modify the ACL to allow the ping traffic.
2. Unapply the ACL from egress (8400/8320/8325 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.

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.

Remote syslog commands

logging

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

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.

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.
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
include-auditable-events	Specifies that auditable messages are also logged to the remote syslog server.
severity *<LEVEL>*	Specifies the severity of the syslog messages: ■ `alert`: Forwards syslog messages with the severity of `alert (6)` and `emergency (7)`. ■ `crit`: Forwards syslog messages with the severity of `critical (5)` and above. ■ `debug`: Forwards syslog messages with the severity of

Parameter	Description
	`debug (0)` and above. ■ `emerg`: Forwards syslog messages with the severity of `emergency (7)` only. ■ `err`: Forwards syslog messages with the severity of `err (4)` and above ■ `info`: Forwards syslog messages with the severity of `info (1)` and above. Default. ■ `notice`: Forwards syslog messages with the severity of `notice (2)` and above. ■ `warning`: Forwards syslog messages with the severity of `warning (3)` and above.
`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.
`legacy-tls-renegotiation`	Enables the TLS connection with a remote syslog server supporting legacy renegotiation.
`filter <FILTER-NAME>`	Specifies the name of the filter to be applied on the syslog messages.
`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
`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
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 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`

Parameter	Description
	■ 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) ■ 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.

Parameter	Description
	▪ `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.

Run Time diagnostics framework is intended to monitor and validate the health of different hardware components present in the system. It uses a set of safe hardware diagnostics test cases to validate the health of different hardware components. These diagnostics test cases are run periodically at every predetermined interval. Additionally, these hardware diagnostics test cases can be run on demand.

Runtime diagnostic commands

diagnostic monitor

```
diagnostic monitor {line-module | management-module} [<SLOT-ID>]
no diagnostic monitor {line-module | management-module} [<SLOT-ID>]
```

Description

Enables runtime diagnostics for all modules or for a specified module. This feature is enabled by default for all modules.

The `no` form of this command disables runtime diagnostics for all modules or for a specified module.

Parameter	Description
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the slot ID of a module. Format: member/slot.

Usage

When no parameters are used in the command (`diagnostic monitor` or `no diagnostic monitor`), the command applies to all modules. This command impacts the diagnostics that run periodically. It does not affect on-demand diagnostics.

Example

Enabling runtime diagnostics for a specified module:

```
switch(config)# diagnostic monitor management-module 1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

diag on-demand

`diag on-demand {line-module | management-module} [<SLOT-ID>]`

Description

Runs the diagnostic tests for all modules or for a specified module.

Parameter	Description
`[line-module | management-module]`	Selects the options for enabling or disabling runtime diagnostics for a specific module.
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the member/slot for management modules (1/1) and line modules (1/1).

Usage

When no parameters are used in the command (`diag on-demand`), the command applies to all modules.

Examples

Running diagnostic tests for all modules on a 6100 switch:

```
switch# diag on-demand
Fetching Test results.  Please wait ...

Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
LineModule           1/1           13     100%
ManagementModule     1/1           13     100%
```

Running diagnostic tests for a specific module on a 6100 switch:

```
switch# diag on-demand management-module 1/1
Performing diagnostic tests.  Please wait ...
Fetching Test results.  Please wait ...

Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
ManagementModule     1/1           13     100%
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show diagnostic

`show diagnostic {line-module | management-module} [<SLOT-ID>] {brief | detail}`

Description

Displays the diagnostic test results for all modules or for a specified module.

Parameter	Description
`[line-module | management-module]`	Selects the options for enabling or disabling runtime diagnostics for a specific module.
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the member/slot for management modules (1/1) and line modules (1/1)

Usage

When no parameters are used in the command (`show diagnostic`), the command applies to all modules.

Example

Showing diagnostic test results in brief format for all modules on a 6100 switch:

```
switch# show diagnostic brief
Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
ManagementModule     1/1           13     100%
LineModule           1/1           13     100%
```

Showing diagnostic test results in brief format for a specified module on a 6100 switch:

```
switch# show diagnostic line-module brief
```

```
Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
LineModule           1/1           13     100%
```

Showing diagnostic test results in detail format for all modules on a 6100 switch:

```
switch# show diagnostic detail

Module : ManagementModule 1/1

Diagnostic     Status Error Code History Code Successive    Total Failure Total
Last Run Timestamp   First Run Timestamp
                                              Failure Count Count         Iteration
-------------- ------ ---------- ------------ ------------- ------------- ---------
-------------------- -------------------
ddr_cecount    Pass   0x0        0x0                      0             0       109
2019-07-31 16:43:38  2019-07-31 07:44:55
emmc           Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
fan_ctrlr      Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
fepld          Pass   0x0        0x0                      0             0       109
2019-07-31 16:43:38  2019-07-31 07:44:54
fru_eeprom     Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:54
fru_eeprom_ul  Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:54
mm_lcb         Pass   0x0        0x0                      0             0       109
2019-07-31 16:43:37  2019-07-31 07:44:54
pmc            Pass   0x0        0x0                      0             0       109
2019-07-31 16:43:37  2019-07-31 07:44:54
rdimm_spd      Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
rdimm_tmp      Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
rtc            Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
tmp1           Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55
tmp2           Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:04  2019-07-31 07:44:55


Module : LineModule 1/1

Diagnostic     Status Error Code History Code Successive    Total Failure Total
Last Run Timestamp   First Run Timestamp
                                              Failure Count Count         Iteration
-------------- ------ ---------- ------------ ------------- ------------- ---------
-------------------- -------------------
lc_asic        Pass   0x0        0x0                      0             0       108
2019-07-31 16:43:37  2019-07-31 07:46:03
poe_ctrlr_1_q1 Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:16  2019-07-31 07:46:03
poe_ctrlr_1_q2 Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:16  2019-07-31 07:46:04
poe_ctrlr_1_q3 Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:16  2019-07-31 07:46:04
poe_ctrlr_2_q1 Pass   0x0        0x0                      0             0         4
2019-07-31 16:08:16  2019-07-31 07:46:05
```

```
poe_ctrlr_2_q2 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:16  2019-07-31 07:46:05
poe_ctrlr_2_q3 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:16  2019-07-31 07:46:05
poe_ctrlr_3_q1 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:16  2019-07-31 07:46:06
poe_ctrlr_3_q2 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:16  2019-07-31 07:46:06
poe_ctrlr_3_q3 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:17  2019-07-31 07:46:06
poe_ctrlr_4_q1 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:17  2019-07-31 07:46:07
poe_ctrlr_4_q2 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:17  2019-07-31 07:46:07
poe_ctrlr_4_q3 Pass    0x0         0x0                    0             0          4
2019-07-31 16:08:17  2019-07-31 07:46:08
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show diagnostic events

```
show diagnostic events
```

Description

Displays the diagnostic related event logs.

Example

Showing diagnostic related event logs:

```
switch# show diagnostic events
2019-08-07:17:19:21.214532|hhmd|106001|ERR|
Diagnostic mm_mcbe failed with error code 0x380 on management module 1/1
2019-08-07:17:19:21.214554|hhmd|106001|ERR|
Diagnostic pmc failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.215532|hhmd|106001|ERR|
Diagnostic ledpld failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.353221|hhmd|106001|ERR|
Diagnostic mm_mcbe failed with error code 0x380 on management module 1/1
2019-08-07:17:19:21.354421|hhmd|106001|ERR|
Diagnostic pmc failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.453221|hhmd|106001|ERR|
Diagnostic ledpld failed with error code 0x4 on management module 1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

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

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

ServiceOS login: admin
SVOS>
-----------
-----------
To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login: reboot
reboot: Restarting system
.
.
Looking for SVOS.

Primary SvOS:  Checking...Loading...Finding...Verifying...Booting...
ServiceOS Information:
```

```
    Version:          PL.01.07.0004-internal
    Build Date:       2020-11-23 18:07:42 PST
    Build ID:         ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA:              133137f635dff5778bf3e109eb75825b68d64789

------------------
------------------

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

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: CN9ZKRK273
  * 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:          PL.01.07.0004-internal
    Build Date:       2020-11-23 18:07:42 PST
    Build ID:         ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA:              133137f635dff5778bf3e109eb75825b68d64789

Boot Profiles:

0. Service OS Console
1. Primary Software Image [PL.10.xx.xxxxx]
2. Secondary Software Image [PL.10.xx.xxxxx]

Select profile(secondary):
```

```
ServiceOS Information:
    Version:          RL.01.07.0004-internal
    Build Date:       2020-11-23 18:07:42 PST
    Build ID:         ServiceOS:RL.01.07.0004-internal:133137f635df:202011231807
    SHA:              133137f635dff5778bf3e109eb75825b68d64789

Boot Profiles:

0. Service OS Console
1. Primary Software Image [RL.10.xx.xxxxx]
2. Secondary Software Image [RL.10.xx.xxxxx]

Select profile(secondary):
```

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 USB console port 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.

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 eMMC 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 eMMC to a USB storage device or upload files using TFTP. Copying files from the eMMC 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 eMMC 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
allow-unsafe-updates - Allow non-failsafe updates for a limited amount of time
                boot - Boot a product image
        config-clear - Clears the startup-config
                diag - Run diagnostic commands
               erase - Securely erase storage devices on the management module
              format - Formats and partitions the primary storage device
            identify - Prints hardware identification information
               mount - Mount a storage device
            password - Set the admin account password
              reboot - Reboots the Management Module
         secure-mode - Set or retrieve 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
                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:          PL.01.07.0004-internal
    Build Date:       2020-11-23 18:07:42 PST
    Build ID:         ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA:              133137f635dff5778bf3e109eb75825b68d64789

Boot Profiles:

0. Service OS Console
1. Primary Software Image [PL.10.06.0001]
2. Secondary Software Image [PL.10.08.0000-168-g3089099c34e6]

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.

Parameter	Description
-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.
-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

Parameter	Description
	than N.
-c	Shows the total disk space usage of all files or directories or both.
-l	Shows the count sizes if hard linked.
-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 eMMC or other storage devices on the management module.

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

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: PL.01.07.0004-internal
    Build Date: 2020-11-23 18:07:42 PST
    Build ID: ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA: 133137f635dff5778bf3e109eb75825b68d64789

################ 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 (svos)

`exit`

Description

Logs the user out from the SVOS> prompt.

Example

Loging the user out from the SVOS> prompt:

```
SVOS> exit

(C) Copyright 2022 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.

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.

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.

Parameter	Description
`-x`	Shows output list by lines.
`-d`	Shows listing of directory entries instead of contents
`-L`	Follows symlinks.
`-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 eMMC 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 eMMC 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.

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.

umount

`umount <DEVICE>`

Description

Unmounts the eMMC 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.

version (ServiceOS)

```
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.

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.

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:

- **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 PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
```

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 PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show selftest

```
show selftest [brief]
show selftest line-module <SLOT-ID>
show selftest line-module <SLOT-ID> interface [brief]
show selftest interface [<PORT-NUM>]
```

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.

Examples

Displaying the output when fastboot is enabled:

```
switch# show selftest
Name        Id   Status          ErrorCode  LastRunTime
----------- ---- --------------- ---------- --------------------
LineModule 1/1  passed          0x0
LineModule 1/2  passed          0x0

switch# show selftest line-module
Name        Id   Status          ErrorCode LastRunTime
----------- ---- --------------- --------- --------------------
LineModule 1/1  passed          0x0
LineModule 1/2  passed          0x0

switch# show selftest line-module 1/1
Name        Id   Status          ErrorCode LastRunTime
----------- ---- --------------- --------- --------------------
LineModule 1/1  passed          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:

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.

Device zeroization lets you remove all user files from flash storage, including embedded MultiMediaCard (eMMC). 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 eMMC. Zeroization also preserves manufacturing information.

The sensitive user files stored on an eMMC or SPI flash/EEPROM storage or both include:

- Switch configurations.
- System generated private keys.
- User installed private keys.
- Admin/operator password files.

For more information on password requirements, see *Password requirements* in the *Security Guide*.

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.

Back up all data before running this command as all configuration settings will be lost.

Example

Restoring the switch to factory default configuration:

```
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


switch login: admin
Password:


Please configure the 'admin' user account password.
Enter new password: *****
Confirm new password: *****
```

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 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. The 6100 switch does not have a `mgmt` VRF, so `https-server` is enabled on the `default` VRF.

Action

Use the `https-server vrf` command to enable REST API access on the specified VRF.

For example:

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

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.

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Hardware Documentation and Translations	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

Portal	
Aruba software	https://asp.arubanetworks.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP account.

Warranty Information

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

Regulatory Information

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

Additional regulatory information

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

Documentation Feedback

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.