AOS-CX 10.07 Diagnostics and Supportability Guide

8320, 8325, 8360 Switch Series

a Hewlett Packard
Enterprise company

Part Number: 5200-7847
Published: April 2021
Edition: 1

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.

Acknowledgments

Bluetooth is a trademark owned by its proprietor and used by Hewlett Packard Enterprise under license.

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 8320 Switch Series (JL479A, JL579A, JL581A)
- Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- Aruba 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A)

Latest version available online

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

Command syntax notation conventions

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

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

About the examples

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

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

Understanding the CLI prompts

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

```
switch>
```

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

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

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

Indicates the configuration context for a feature. For example:

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

Identifies the `interface` context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

member/slot/port

On the 83xx Switch Series

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

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

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

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

Syntax

```
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.

Command context

Manager (#)

Authority

Administrators or local user group members with execution rights for this 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
```

debug {all | <MODULE-NAME>}

Syntax

```
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.

Command context

Manager (`#`)

Parameters

`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.

`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.

Authority

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

Examples

```
switch# debug all
```

debug db

Syntax

```
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.

Command context

Manager (`#`)

Parameters

`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).

Authority

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

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
```

debug destination

Syntax

```
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.

Command context

Manager (`#`)

Parameters

`{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).

Authority

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

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
```

show debug

Syntax

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

Description

Displays the enabled debug types.

Command context

Manager (`#`)

Parameters

`[vsx-peer]`

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

Authority

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

Examples

```
switch# show debug
--------------------------------------------------------------------------------
```

```
module sub_module severity vlan port    ip        mac               instance  vrf

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

show debug buffer

Syntax

```
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.

Command context

Manager (#)

Parameters

<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).

Authority

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

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
```

show debug destination

Syntax

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

Description

Displays the configured debug destination and severity.

Command context

Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Examples

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

Log rotation provides an ability for a system administrator to systematically rotate and archive any log files produced by the system. Log rotation reduces the disk space requirement of an operating system. The feature uses the Linux log-rotate utility for log rotation. Log rotation rotates and compresses the log files either based on size and/or period. Rotated log files are stored locally or transferred to the remote destination using Trivial File Transfer Protocol (TFTP).

By default the log rotation feature rotates the log files daily. If the maximum file size exceeds 100 MB, log rotation is also triggered. Whichever condition occurs first (period or size) triggers the log rotation.

Changing the size of the log rotation file

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

```
logrotate maxsize <10-200 MB>
```

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

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Changing the time frequency for log rotation

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

Prerequisites

You must be in the configuration context:

```
switch(config)#
```

Procedure

At the configuration context, enter:

```
logrotate period {daily | hourly | weekly | monthly }
```

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

hourly: Rotates the log files hourly.

weekly: Rotates the log files every week.

monthly: Rotates the log files every month.

Example command

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

Identifying a remote host for receiving rotated log files

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

Prerequisites

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

Procedure

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

IPv4 Example

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

IPv6 Example

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

Log rotation paths

Only logs stored in the following files are rotated:

- Event logs stored in the `/var/log/event.log` file.
- Authentication logs stored in the `/var/log/auth.log` file.
- Audit logs stored in the `/var/log/audit/audit.log` file

Management of 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.

Remote transfer of rotated log files

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

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

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

Verifying the log rotation parameters

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

Example output

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

Resetting the size of the log rotation file

Prerequisites

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

Procedure

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

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

Resetting the time frequency to daily

Prerequisites

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

Procedure

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

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

Resetting the remote host for receiving rotated log files

Prerequisites

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

Procedure

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

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

Example:

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

Log rotation not occurring immediately after reaching threshold

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 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 regardless of `period` value

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

logrotate maxsize

Syntax

```
logrotate maxsize <MAX-SIZE>

no logrotate maxsize
```

Description

Specifies the maximum allowed log file size.

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

Command context

```
config
```

Parameters

<MAX-SIZE>

Specifies the allowed size the log file can reach before it is compressed and stored locally or transferred to a remote host. The size is a value in the range of 10- 200 MB, and it cannot exceed 32 MB for transferred files.

Authority

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

Usage

A log file that exceeds either the configured *<MAX-SIZE>* value or the `logrotate period`, triggers rotation for that log file. Log rotation occurs during the next hourly maintenance cycle.

Logs are stored locally (event logs in the `/var/log/event.log` file, and authentication logs in the `/var/log/auth.log` file) or transferred to the configured remote destination target using TFTP.

Examples

```
switch(config)# logrotate maxsize 32
```

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

logrotate period

Syntax

```
logrotate period {daily | hourly | monthly | weekly}

no logrotate period
```

Description

Sets the rotate period for the event logs, stored in the `/var/log/event.log` file, and authentication logs, stored in the `/var/log/auth.log` file. Defaults to `daily`.

A log file that exceeds either the `logrotate <MAX-SIZE>` value or the `logrotate period` (whichever happens first), triggers rotation for that log file.

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

Command context

`config`

Parameters

`daily`
Rotates log files on a daily basis (default) at 1:00 am local time.

`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.

`weekly`
Rotates log files once a week on Sunday.

Authority

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

Examples

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

logrotate target

Syntax

```
logrotate target {tftp://<IPV4_ADDR> | tftp://<IPV6_ADDR>}

no logrotate target
```

Description

Specifies the target remote host Universal Resource Identifier (URI) using TFTP protocol to allow transfer of rotated and compressed files to a remote target. Rotated log files are stored locally (event logs in the `/var/log/event.log` file, and authentication logs in the `/var/log/auth.log` file) or transferred to the configured remote destination target.

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

`config`

Parameters

<IPV4_ADDR>

Specifies an IPv4 IP Address location for log file storage.

<IPV6_ADDR>

Specifies an IPv6 IP Address location for log file storage.

Authority

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

Usage

To transfer rotated log files remotely, use the TFTP protocol only, and make sure that the rotated log file is less than 32 MB in size. Use the Linux TFTP command to transfer the file. The rotated log file is removed from the local path `/var/log/` when the log file is moved to a TFTP server.

Examples

Setting an IPv4 target:

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

Setting an IPv6 target:

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

Removing a `logrotate` target :

```
switch(config)# logrotate target tftp://1.1.1.1
switch(config)# do show logrotate
Logrotate configurations :
Period : daily
Maxsize : 10MB
Target : tftp://1.1.1.1

switch(config)# no logrotate target
switch(config)# do show logrotate
Logrotate configurations :
Period : daily
Maxsize : 10MB

switch(config)#
```

show logrotate

Syntax

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

Description

Displays `logrotate` configuration details.

Command context

Manager (`#`)

Parameters

`[vsx-peer]`

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

Authority

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

Examples

```
switch# show logrotate
Logrotate configurations :
Period            : daily
Maxsize           : 100MB
Target            : local
switch#
```

bluetooth disable

Syntax

```
bluetooth disable

no bluetooth disable
```

Description

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

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

Command context

`config`

Authority

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

Example

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

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

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

bluetooth enable

Syntax

```
bluetooth enable

no bluetooth enable
```

Description

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

Default: Bluetooth is enabled by default.

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

Command context

`config`

Authority

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

Usage

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

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

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

Examples

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

clear events

Syntax

`clear events`

Description

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

Command context

Manager (`#`)

Authority

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

Examples

Clearing all generated event logs:

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

switch# clear events
```

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

clear ip errors

Syntax

```
clear ip errors
```

Description

Clears all IP error statistics.

Command context

Manager (#)

Authority

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

Example

Clearing and showing ip errors:

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

domain-name

Syntax

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

Description

Specifies the domain name of the switch.

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

Command context

```
config
```

Parameters

<NAME>

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

Authority

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

Examples

Setting and showing the domain name:

```
switch# show domain-name

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

Setting the domain name to the default value:

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

switch(config)#
```

hostname

Syntax

`hostname <HOSTNAME>`

`no hostname [<HOSTNAME>]`

Description

Sets the host name of the switch.

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

Command context

`config`

Parameters

`<HOSTNAME>`

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

Authority

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

Examples

Setting and showing the host name:

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

Setting the host name to the default value:

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

led locator

Syntax

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

Description

Sets the state of the locator LED.

Command context

Manager (#)

Parameters

`on`
: Turns on the LED.

`off`
: Turns off the LED, which is the default value.

`slow_blink`
: Sets the LED to slow blink on and off.

`flashing`
: Sets the LED to blink on and off repeatedly.

`fast_blink`
: Sets the LED to fast blink on and off.

`half_bright`
: Sets the LED intensity to half bright.

Authority

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

Example

Setting the state of the locator LED:

```
switch# led locator flashing
```

show bluetooth

Syntax

`show bluetooth`

Description

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

Command context

Operator (`>`) or Manager (`#`)

Authority

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

Usage

This command shows status information about the following:

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

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

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

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

Examples

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

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

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

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

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

Example output when Bluetooth is disabled:

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

show capacities

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<FEATURE>

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

`[vsx-peer]`

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

Authority

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

Usage

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

Examples

Showing all available capacities for BGP:

```
switch# show capacities bgp

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

Showing all available capacities for mirroring:

```
switch# show capacities mirroring

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

```
Maximum number of enabled Mirror Sessions in a system                              4
```

Showing all available capacities for MSTP:

```
switch# show capacities mstp

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

Showing all available capacities for VLAN count:

```
switch# show capacities vlan-count

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

show capacities-status

Syntax

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

Description

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

Command context

Manager (`#`)

Parameters

`<FEATURE>`

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

`[vsx-peer]`

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

Authority

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

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

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

Showing the system capacities status for BGP:

```
switch# show capacities-status bgp

System Capacities Status: Filter BGP
Capacities Status Name                                                     Value Maximum
-------------------------------------------------------------------------------------
Number of aspath-lists configured                                          0      64
Number of community-lists configured                                       0      64
Number of neighbors configured across all VRFs                             0      50
Number of peer groups configured across all VRFs                           0      25
Number of prefix-lists configured                                          0      64
Number of route-maps configured                                            0      64
Number of routes in BGP RIB                                                0  256000
Number of route reflector clients configured across all VRFs               0      16
```

show core-dump

Syntax

`show core-dump all`

Description

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

Command context

Manager (`#`)

Parameters

`all`

Shows all available core dumps.

Authority

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

Usage

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

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

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

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

`Daemon Name`

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

`Instance ID`

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

`Present`

Indicates the status of the core dump:

`Yes`

The core dump has completed and available for copying.

`In Progress`

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

`Timestamp`

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

`Build ID`

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

Examples

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

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

Showing all core dumps:

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

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

show domain-name

Syntax

```
show domain-name [vsx-peer]
```

Description

Shows the current domain name.

Command context

Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Usage

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

Example

Setting and showing the domain name:

```
switch# show domain-name

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

show environment fan

Syntax

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

Description

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

Command context

Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Usage

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

`ready`

The fan tray is operating normally.

`fault`

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

`empty`

The fan tray is not installed in the system.

For fans:

`Speed`

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

`Slow`

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

`Normal`

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

`Medium`

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

`Fast`

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

`Max`

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

`N/A`

The fan is not installed.

`Direction`

The direction of airflow through the fan. Values are:

`front-to-back`

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

`N/A`

The fan is not installed.

`Status`

Fan status. Values are:

`uninitialized`

The fan has not completed initialization.

`ok`

The fan is operating normally.

`fault`

The fan is in a fault state.

`empty`

The fan is not installed.

Examples

Showing output for a system without a fan tray:

```
switch# show environment fan

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

show environment led

Syntax

```
show environment led [vsx-peer]
```

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Example

Showing state and status for LED:

```
switch# show environment led
Name           State     Status
-----------------------------------
locator        flashing  ok
```

show environment power-supply

Syntax

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

Description

Shows status information about all power supplies in the switch.

Command context

Operator (>) or Manager (#)

Parameters

`vsf`

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

`[vsx-peer]`

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

Authority

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

Usage

The following information is provided for each power supply:

`Mbr/PSU`

Shows the member and slot number of the power supply.

`Product Number`

Shows the product number of the power supply.

`Serial Number`

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

`PSU Status`

The status of the power supply. Values are:

`OK`

Power supply is operating normally.

`OK*`

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

`Absent`

No power supply is installed in the specified slot.

`Input fault`

The power supply has a fault condition on its input.

`Output fault`

The power supply has a fault condition on its output.

`Warning`

The power supply is not operating normally.

`Wattage Maximum`

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

Example

show environment temperature

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`detail`

Shows detailed information from each temperature sensor.

`[vsx-peer]`

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

Authority

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

Usage

Temperatures are shown in Celsius.

Valid values for status are the following:

`normal`

Sensor is within nominal temperature range.

`min`

Lowest temperature from this sensor.

`max`

Highest temperature from this sensor.

`low_critical`

Lowest threshold temperature for this sensor.

`critical`

Highest threshold temperature for this sensor.

`fault`

Fault event for this sensor.

`emergency`

Over temperature event for this sensor.

Examples

show events

Syntax

```
show events [ -e <EVENT-ID> |
    -s {alert | crit | debug | emer | err | info | notice | warn} |
    -r | -a | -n <count> |
    -c {lldp | ospf | ... | } |
    -d {lldpd | hpe-fand | ... |}]
```

Description

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

Command context

Manager (#)

Parameters

`-e <EVENT-ID>`

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

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

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

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

`-r`

Shows the most recent event logs first.

`-a`

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

`-n <count>`

Displays the specified number of event logs.

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

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

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

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

Authority

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

Examples

Showing event logs:

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

Showing the most recent event logs first:

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

Showing all event logs:

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

Showing event logs related to the DHCP relay agent:

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

Showing event logs related to the DHCPv6 relay agent:

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

Showing event logs related to IRDP:

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

Showing event logs related to LACP:

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

Showing event logs as per the specified process:

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

Displaying the specified number of event logs:

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

show hostname

Syntax

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

Description

Shows the current host name.

Command context

Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Example

Setting and showing the host name:

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

show images

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Example

Showing the primary and secondary images on a 8320 switch:

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

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

Default Image : primary

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

show ip errors

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Usage

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

Drop reasons are the following:

Malformed packet

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

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

IP address error

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

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

Invalid TTLs

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

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

Example

Showing ip error statistics for packets received by the switch:

```
switch# show ip errors
---------------------------------
Drop reason                Packets
---------------------------------
```

```
Malformed packets                1
IP address errors               10
...
```

show module

Syntax

```
show module [vsx-peer]
```

Description

Shows information about installed line modules and management modules.

Although this switch does not have removable modules, this command will still return information about the switch, referring to management modules and line modules.

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Usage

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

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

Status is one of the following values:

`Active`

This switch is the active management module.

`Standby`

This switch is the standby management module.

`Deinitializing`

The switch is being deinitialized.

`Diagnostic`

The switch is in a state used for troubleshooting.

`Down`

The switch is physically present but is powered down.

`Empty`

The switch hardware is not installed in the chassis.

`Failed`

The switch has experienced an error and failed.

`Failover`

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

`Initializing`

The switch is being initialized.

`Present`

The switch hardware is installed in the chassis.

`Ready`

The switch is available for use.

`Updating`

A firmware update is being applied to the switch.

Examples

Showing all installed modules:

```
switch(config)# show module

Management Modules
==================

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL581A  8320 Mgmt Mod                      TW87KCW00X Ready


Line Modules
============

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL581A  8320                               TW87KCW00X Ready
```

show running-config

Syntax

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

Description

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

Command context

Manager (`#`)

Parameters

`<FEATURE>`

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

`all`

Shows all default values for the current running configuration.

`[vsx-peer]`

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

Authority

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

Examples

Showing the current running configuration:

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

interface vlan30
    no shutdown
    vrf attach green
    ip address 30.0.0.44/24
```

```
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable

    ip pim-sparse hello-interval 100
```

Showing the current running configuration in json format:

```
switch> show running-config json
Running-configuration in JSON:
{
    "Monitoring_Policy_Script": {
        "system_resource_monitor_mm1.1.0": {
            "Monitoring_Policy_Instance": {
                "system_resource_monitor_mm1.1.0/system_resource_monitor_
mm1.1.0.default": {
                    "name": "system_resource_monitor_mm1.1.0.default",
                    "origin": "system",
                    "parameters_values": {
                        "long_term_high_threshold": "70",
                        "long_term_normal_threshold": "60",
                        "long_term_time_period": "480",
                        "medium_term_high_threshold": "80",
                        "medium_term_normal_threshold": "60",
                        "medium_term_time_period": "120",
                        "short_term_high_threshold": "90",
                        "short_term_normal_threshold": "80",
                        "short_term_time_period": "5"
                    }
                }
            },
...
...
...
...
```

Show the current running configuration without default values:

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

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

Show the current running configuration with default values:

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

show running-config current-context

Syntax

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

Description

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

Command context

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

Authority

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

Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (`config`) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance. Support for this command is provided for one level below the `config` context. For example, entering this command for a child of a child of the `config` context not supported. If you enter the command on a child of the `config` context, the current configuration of that context and the children of that context are displayed.
- The global configuration (`config`) context. If you enter this command in the global configuration (`config`) context, it shows the running configuration of the entire switch. Use the `show running-configuration` command instead.

Examples

Showing the running configuration for the current interface:

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

Showing the current running configuration for the management interface:

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

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

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

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

```
switch(config-vsx)# show run current-context
vsx
    inter-switch-link 1/1/1
    role secondary
    vsx-sync sflow time
```

show startup-config

Syntax

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

Description

Shows the contents of the startup configuration.

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

Command context

Manager (#)

Parameters

`json`

Display output in JSON format.

Authority

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

Examples

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

```
Leaf2(config)# show startup-config
Startup configuration:
!
!Version ArubaOS-CX TL.xx.xx.xxxx
hostname Leaf2
user admin group administrators password ciphertext

AQBapaGi+KZp4g8gw63UqK+zCtvO5zigFLv2DFBEH+lztqjdYgAAABwrJ+5GayUWArgv9tVFo9AzMY6gmI7
x/

KBEkGBJDXjpFson2qM83CXBUI673qWHDQ0pEIZXeuig0XogCVuId4oZiQVZlOe2MfxnqZL+E9hXaMNVowBwb
D0
cli-session
    timeout 0
!
!
!
ssh server vrf mgmt
```

Showing the startup-configuration in JSON format:

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

show system

Syntax

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

Description

Shows general status information about the system.

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Usage

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

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

Examples

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

```
vsx-primary# show system
Hostname           : vsx-primary
System Description : TL.10.xx.xxxxx
System Contact     :
System Location    :

Vendor             : Aruba
Product Name       : JL479A 8320
Chassis Serial Nbr : TW82K7200Q
Base MAC Address   : 98f2b3-68792e
```

```
ArubaOS-CX Version : TL.10.xx.xxxxx

Time Zone          : UTC

Up Time            : 19 hours, 51 minutes
CPU Util (%)       : 50
Memory Usage (%)   : 36

vsx-primary# show system vsx-peer
Hostname           : vsx-secondary
System Description : TL.10.xx.xxxxx
System Contact     :
System Location    :

Vendor             : Aruba
Product Name       : JL479A 8320
Chassis Serial Nbr : TW73JQH024
Base MAC Address   : e0071b-cb72e4
ArubaOS-CX Version : TL.10.xx.xxxxx

Time Zone          : UTC

Up Time            : 21 hours, 23 minutes
CPU Util (%)       : 14
Memory Usage (%)   : 36
```

show system resource-utilization

Syntax

`show system resource-utilization [daemon <DAEMON-NAME>] [vsx-peer]`

Description

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

Command context

Manager (#)

Parameters

`daemon <DAEMON-NAME>`

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

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

`[vsx-peer]`

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

Authority

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

Examples

Showing all system resource utilization data:

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

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

Showing the resource utilization data for the pmd process:

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

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

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

Showing resource utilization data for a line module:

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

show tech

Syntax

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

Description

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

Command context

Manager (`#`)

Parameters

`basic`

Specifies showing a basic set of information.

`<FEATURE>`

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

`local-file`

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

Authority

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

Usage

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

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

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

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

Example

Showing the basic set of system information:

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

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

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

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

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

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

show usb

Syntax

```
show usb [vsx-peer]
```

Description

Shows the USB port configuration and mount settings.

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Examples

If USB has not been enabled:

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

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

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

If USB has been enabled and a device mounted:

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

show version

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`[vsx-peer]`

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

Authority

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

Example

Showing version information for an 8320 switch:

```
switch(config)# show version
--------------------------------------------------------------------------------
ArubaOS-CX
(c) Copyright 2017-2020 Hewlett Packard Enterprise Development LP
--------------------------------------------------------------------------------
Version      : TL.xx.xx.xxxx
Build Date   : 2020-08-20 10:56:02 PDT
Build ID     : ArubaOS-CX:xx.xx.xxxx:feb590a400a5:201908201736
Build SHA    : feb590a400a57ed818b01614f92010d74fbc9a4b
Active Image : secondary

Service OS Version : TL.01.03.0008
BIOS Version       : TL-01-0013
```

system resource-utilization poll-interval

Syntax

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

Description

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

Command context

`config`

Parameters

<SECONDS>

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

Authority

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

Example

Configuring the system resource utilization poll interval:

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

top cpu

Syntax

```
top cpu
```

Description

Shows CPU utilization information.

Command context

Manager (#)

Authority

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

Example

Showing top CPU information:

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

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

top memory

Syntax

```
top memory
```

Description

Shows memory utilization information.

Command context

Manager (#)

Authority

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

Example

Showing top memory:

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

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

usb

Syntax

```
usb
no usb
```

Description

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

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

Command context

`config`

Authority

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

Example

Enabling USB ports:

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

Disabling USB ports when a USB drive is mounted:

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

usb mount | unmount

Syntax

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

Description

Enables or disables the inserted USB drive.

Command context

Manager (`#`)

Parameters

`mount`

Enables the inserted USB drive.

`unmount`

Disables the inserted USB drive in preparation for removal.

Authority

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

Usage

If USB has been enabled in the configuration, the USB port on the active management module is available for mounting a USB drive. The USB port on the standby management module is not available.

An inserted USB drive must be mounted each time the switch boots or fails over to a different management module.

A USB drive must be unmounted before removal.

The supported USB file systems are FAT16 and FAT32.

Examples

Mounting a USB drive in the USB port:

```
switch# usb mount
```

Unmounting a USB drive:

```
switch# usb unmount
```

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

Reboot reasons for management module

Reboots handled through database

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

Uncontrolled reboots

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

The resets are not applicable for 8320 and 8325 Switch series.

- switchd_agent crashed

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 various event commands are listed in the following table:

Task	Command or procedure
Clearing events	clear events
Showing events	show events

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.

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 command-output

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<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:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE> vrf <VRF-NAME>`

Specifies the VRF name. The default VRF name is default. Optional.

Authority

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

Examples

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" tftp://10.100.0.12/file vrf mgmt
```

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

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

copy core-dump daemon

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<DAEMON-NAME>

Specifies the name of the daemon. Required.

`[:<INSTANCE-ID>]`

Specifies the instance of the daemon core dump. Optional.

<REMOTE_URL>

Specifies the remote destination URL. Required. The syntax of the URL is the following:

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`

`vrf <VRF-NAME>`

Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.

Authority

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

Examples

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

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

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

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

copy core-dump kernel

Syntax

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

Description

Copies a kernel core dump using TFTP or SFTP.

Command context

Manager (#)

Parameters

<REMOTE-URL>

Specifies the URL to copy the command output. Required.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<FILE>`
`vrf <VRF-NAME>`

Specifies the VRF name. The default VRF name is default. Optional.

Authority

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

Examples

Copying the kernel core dump to the URL:

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

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

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

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

Syntax

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

Description

Copies the kernel core dump to a USB drive.

Command context

Manager (#)

Parameters

<STORAGE-URL>

Specifies the USB to copy command output. Required.

Syntax: `{usb}:/<FILE>`

Authority

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

Examples

Copying the kernel core dump to a USB drive:

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

copy diag-dump feature *<FEATURE>*

Syntax

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

Description

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

Command context

Manager (`#`)

Parameters

<FEATURE>

The name of a feature, for example `aaa` or `vrrp`. Required.

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

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the remote destination URL. Required. The syntax of the URL is the following:

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<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>`

Authority

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

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 vrrp feature to a USB drive:

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

copy diag-dump local-file

Syntax

`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, or USB.

Command context

Manager (`#`)

Parameters

`{<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:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<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>`

Authority

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

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 USB drive:

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

copy show-tech feature

Syntax

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

Description

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

Command context

Manager (#)

Parameters

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

Select either the remote URL or the storage URL for the destination of the copied command output. Required.

<REMOTE-URL>

Specifies the URL to copy the command output. Required.

Syntax: `{tftp:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<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>`

Authority

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

Example

Copying show tech output of the `aaa` feature using SFTP:

```
switch# copy show-tech feature aaa sftp://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
```

copy show-tech local-file

Syntax

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

Description

Copies show tech output stored in a local file.

Command context

Manager (#)

Parameters

`{<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:// | sftp://<USER>@}{<IP> | <HOST>}[:<PORT>][;blocksize=<VAL>]/<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>`

Authority

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

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 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
```

copy support-files

Syntax

```
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, or USB.

Command context

Manager (#)

Parameters

<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:// | sftp://*<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<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.

Authority

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

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 sftp://root@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
```

copy support-files local-file

Syntax

```
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, 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.

Command context

Manager (#)

Parameters

<FEATURE-NAME>

Specifies the feature for the support files.

<SLOT-ID>

Specifies the module slot number identifier for the support files. Range: 1/1-1/4, 1/7-1/10

<MEMBER-ID>

Specifies the VSF member identifier for the support files. Range: 1-10

<REMOTE-URL>

Specifies the URL to copy the support files.

<STORAGE-URL>

Specifies the USB to copy the support files.

<VRF-NAME>

Specifies the VRF name. The default VRF name is default.

Authority

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

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 sftp://root@10.0.14.206//support_files_dir_
path/abc.tar.gz vrf mgmt
```

copy support-log

Syntax

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

Description

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

Command context

Manager (#)

Parameters

<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:// | sftp://*<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<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.

Authority

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

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 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
```

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

Syntax

```
traceroute {IPv4-address | hostname} [ip-option loosesourceroute <IPV4-ADDR>] [dstport
<NUMBER> | maxttl <NUMBER> | minttl <NUMBER> | probes <NUMBER> | timeout <TIME>] [vrf {<VRF-
NAME> | mgmt}]
```

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`IPv4-address`

Specifies the IPv4 address of the device to use traceroute.

`hostname`

Specifies the hostname of the device to use 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, `<VRF-NAME>`.

`mgmt`

Specifies use of the management interface.

Authority

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

Usage

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
```

traceroute6

Syntax

```
traceroute6 {IPv6-address | hostname} [dstport <NUMBER> | maxttl <NUMBER> |
 probes <NUMBER> | timeout <TIME>] [vrf {<VRF-NAME> | mgmt}]
```

Description

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

Command context

Operator (>) or Manager (#)

Parameters

`IPv6-address`

Specifies the IPv6 address of the device to use traceroute.

`hostname`

Specifies the hostname of the device to use 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>*.

`mgmt`

Specifies use of the management interface.

Authority

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

Usage

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
```

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

Syntax

```
ping <IPv4-address | 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>]
```

Description

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

Command context

Operator (`>`) or Manager (`#`)

Parameters

`<IPv4-ADDR>`

Selects the IPv4 address to ping.

`<HOSTNAME>`

Selects the hostname to ping. Range: 1-256 characters

`data-fill` *`<PATTERN>`*

Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB

`datagram-size` *`<SIZE>`*

Specifies the ping datagram size. Range: 0-65399, default: 100.

`interval` *`<TIME>`*

Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.

`repetitions` *`<NUMBER>`*

Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.

`timeout` *`<TIME>`*

Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.

`tos` *`<NUMBER>`*

Specifies the IP Type of Service to be used in Ping request. Range: 0-255

`ip-option [include-timestamp | include-timestamp-and-address | record-route]`

Specifies an IP option (`record-route` or `timestamp` option).

`include-timestamp`

Specifies the intermediate router time stamp.

`include-timestamp-and-address`

Specifies the intermediate router time stamp and IP address.

`record-route`

Specifies the intermediate router addresses.

`vrf <VRF-NAME>`

Specifies the virtual routing and forwarding (VRF) to use. When VRF option is not given, the default VRF is used.

Authority

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

Examples

Pinging an IPv4 address:

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

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

Pinging the localhost:

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

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

Pinging a server with a data pattern:

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

--- 10.0.0.2 ping statistics ---
```

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

Pinging a server with a datagram size:

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

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

Pinging a server with an interval specified:

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

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

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

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

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

Pinging a server with a specified timeout:

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

```
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.190 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.181 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.197 ms

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

Pinging a server with the specified IP Type of Service:

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

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

Pinging a local host with the specified VRF.

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

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

Pinging the localhost with the default VRF:

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

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

Pinging a server with the intermediate router time stamp:

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

```
        0
        0
        0

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

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

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

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


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

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

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

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

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

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

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


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

Pinging a server with the intermediate router address:

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

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

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

ping6

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

IPv6-ADDR

Selects the IPv6 address to ping.

HOSTNAME

Selects the hostname to ping. Range: 1-256 characters

data-fill *<PATTERN>*

Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB

datagram-size *<SIZE>*

Specifies the ping datagram size. Range: 0-65399, default: 100.

interval *<TIME>*

Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.

`repetitions <NUMBER>`

Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.

`timeout <TIME>`

Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.

`vrrp <VRID>`

Specifies the VRRP group ID.

`vrf <VRF-NAME>`

Specifies the virtual routing and forwarding (VRF) to use. When this option is not provided, the default VRF is used.

Authority

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

Examples

Pinging an IPv6 address:

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

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

Pinging the localhost:

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

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

Pinging a server with a data pattern:

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

```
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.077 ms

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

Pinging a server with a datagram size:

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

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

Pinging a server with an interval specified:

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

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

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

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

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

Pinging a local host with the specified VRF.

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

```
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.027 ms

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

Pinging the localhost with the default VRF:

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

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

Troubleshooting

Operation not permitted

Symptom

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

Example:

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


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

Cause

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

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

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

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

Action

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

Syntax

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

logging {<IPV4-ADDR> | <IPV6-ADDR> | <FQDN | HOSTNAME>} [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.

Command context

```
config
```

Parameters

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

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

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

Authority

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

Examples

Enabling the syslog forwarding to remote syslog server 10.0.10.2:

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

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

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

Disabling syslog forwarding to a remote syslog server:

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

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
```

logging filter

Syntax

```
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.

Command context

`config` and `config-logging-filter`

Parameters

<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)`.

Authority

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

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
```

logging facility

Syntax

```
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.

Command context

`config`

Parameters

`{local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}`

Selects the logging facility to be used for remote syslog messages. Required.

Specifies the severity of the syslog messages:

- `local0`
- `local1`
- `local2`
- `local3`
- `local4`
- `local5`
- `local6`
- `local7`

Authority

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

Examples

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

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

logging persistent-storage

Syntax

```
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.

Command context

`config`

Parameters

`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.
- `notice`: Preserves syslog messages with the severity of `notice (2)` and above.
- `warning`: Preserves syslog messages with the severity of `warning (3)` and above.

Authority

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

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
```

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

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

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

Service OS CLI login

Description

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

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

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

Example

```
ServiceOS GT.01.01.0001 switch ttyS0

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

switch login: admin

   Hewlett Packard
   Enterprise
SVOS>
```

```
ServiceOS GT.01.01.0001 switch ttyS0

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

```
switch login: reboot

   Hewlett Packard
   Enterprise
reboot: Restarting system
```

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

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

Continue (y/n)? y

reboot: Restarting system
```

Service OS user accounts

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

Service OS boot menu

Description

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

The user is then shown the boot image profiles.

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

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

Example

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

Boot Profiles:

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

Select profile(primary):
```

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

Console configuration

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

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

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

AOS-CX boot

Description

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

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

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

Service OS will then present status and boot the image.

Example

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

        Name: ArubaOS-CX
     Version: XL.01.01.0001
```

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


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

File system access

Description

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

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

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

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

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

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

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

The root / directory displays viewable directories:

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

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

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

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

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

Service OS mount failure

Description

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

Example

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

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

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

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

ServiceOS login:
```

Service OS CLI command list

Description

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

Example

```
SVOS> ?
Available Commands:

           ? - Display help screen
          cd - Change the working directory
         pwd - Print the current working directory
        help - Display help screen
        boot - Boot a product image
config-clear - Clears the startup-config
       erase - Securely erase storage devices on the management module
      format - Formats and partitions the primary storage device
    identify - Prints hardware identification information
          ip - Sets the OOBM Port Network Configuration
       mount - Mount a storage device
        ping - Send ICMP ECHO_REQUEST to network hosts (IPv4)
      reboot - Reboots the Management Module
    password - Set the admin account password
 secure-mode - Sets or retrieves the secure mode setting
          sh - Launch support shell
      umount - Unmounts a storage device
```

```
      update - Update a product image
     version - Prints ServiceOS release version information
         cat - Prints files to stdout
          cp - Copy files and directories
          du - Estimate file space usage
          ls - List directory contents
       md5sum - Compute and check md5 message digest
        mkdir - Make directories
           mv - Move (rename) files
           rm - Remove files or directories
        rmdir - Remove empty directories
         tftp - Allows transfer of files to/from a remote machine
         exit - Logout

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

Service OS CLI features and limitations

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

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

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

The following common features are available:

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

Service OS CLI commands

boot

Syntax

`boot`

Description

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

Command context

ServiceOS (`SVOS>`)

Authority

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

Example

Presenting the boot menu prompt:

```
SVOS> boot

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

Boot Profiles:

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

Select profile(primary):
```

cat

Syntax

`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.

Command context

ServiceOS (`SVOS>`)

Parameters

`<FILENAME/DIRECTORY-NAME>`

Shows the contents of the specified file or directory.

Authority

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

Example

Showing the contents of /nos/hosts:

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

SVOS>
```

cd path

Syntax

`cd path`

Description

Changes the current working directory.

Command context

ServiceOS (`SVOS>`)

Authority

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

Example

Changing the current working directory:

```
cd /
```

config-clear

Syntax

`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.

Command context

ServiceOS (`SVOS>`)

Authority

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

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>
```

cp

Syntax

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

Description

Copies files or directories.

Command context

ServiceOS (`SVOS>`)

Parameters

`[options]`

Selects the options for the command.

`-d,-P`

Specifies the preservation of symlinks (default if `-R`).

`-a`

Same as `-dpR`.

`R,-r`

Specifies recursiveness, all files, and subdirectories are copied.

`-L`

Specifies the following of all symlinks.

`-H`

Specifies the following of symlinks on command line.

`-p`

Specifies the preservation of file attributes if possible.

`-f`

Specifies the overwriting of a file or directory.

`-i`

Specifies the prompting before an overwrite.

`-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.

Authority

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

Example

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

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

du

Syntax

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

Description

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

Command context

ServiceOS (SVOS>)

Parameters

[options]

Selects the options for the command.

-a

Show file sizes.

-L

Shows all symlinks.

-H

Shows symlinks on a command line.

-d, N

Shows limited output to directories (and files with -a) of depth less than N.

-c

Shows the total disk space usage of all files or directories or both.

-l

Shows the count sizes if hard linked.

-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.

Authority

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

Example

Estimating disk space for the /nos directory:

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

erase zeroize

Syntax

```
erase zeroize
```

Description

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

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

Command context

ServiceOS (SVOS>)

Authority

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

Example

Erasing user data:

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

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

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

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

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

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

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

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

exit

Syntax

```
exit
```

Description

Logs the user out from the SVOS> prompt.

Command context

ServiceOS (SVOS>)

Authority

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

Example

Loging the user out from the `SVOS>` prompt:

```
SVOS> exit

(C) Copyright 2021 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:
```

format

Syntax

`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.

Command context

ServiceOS (`SVOS>`)

Authority

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

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...
```

identify

Syntax

identify

Description

Prints the version of the SVOS and of the UEFI BIOS.

Command context

ServiceOS (SVOS>)

Authority

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

Example

Printing the version of the SVOS and of the UEFI BIOS:

Output from an 8320 switch:

```
SVOS> identify
mc svos_primary           : TL.01.01.0004
mc svos_secondary         : TL.01.01.0004
mc cpld/1                 : 8
mc cpld/2                 : 7
mc cpld/3                 : 7
mc uefi                   : TL-01-0013
mc uefi_capsule           : TL-01-0013
Support Info              : SE:0
```

Output from an 8325 switch:

```
SVOS> identify
SVOS> identify
mc svos_primary           : GL.01.01.0004
mc svos_secondary         : GL.01.01.0004
mc uefi                   : GL-01-0010
mc uefi_capsule           : GL-01-0010
Support Info              : SE:0
SVOS>
```

ip

Syntax

```
ip {show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}
```

Description

Shows or configures the port with a static IP address (IPv4 only) or enables the DHCP client on the port. An address is set only if a DHCP server is available to provide one.

Command context

ServiceOS (SVOS>)

Parameters

{show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}

Selects the options for the OOBM port.

show

Shows the OOBM port.

`dhcp`

Configures the port with a DHCP address.

`disable`

Disables the OOBM port.

`addr` **`<addr netmask gateway>`**

Configures the port with a static IP address (IPv4 only). Specify address, netmask, and gateway as A.B.C.D.

Authority

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

Example

Configuring the port with a DHCP IP address:

```
SVOS> ip dhcp
SVOS> ip show
Interface  : Link Up
IP Address : 10.0.26.17
Subnet Mask: 255.255.252.0
Gateway    : 10.0.24.1

SVOS> ip disable
SVOS> ip show
Interface : Disabled
SVOS>
```

ls

Syntax

`ls [<OPTIONS>] [<FILE-NME>]`

Description

This command lists directory contents.

Command context

ServiceOS (`SVOS>`)

Parameters

`<OPTIONS>`

Specifies options for the command.

`-1`

Shows one-column output.

`-a`

Shows entries which start with a period (.).

`-A`

Shows output similar to `-a`, but excludes a period (.) and a double period (..).

`-C`

Shows output list by columns.

`-x`

Shows output list by lines.

`-d`

Shows listing of directory entries instead of contents

`-L`

Follows symlinks.

`-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.

Authority

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

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>
```

md5sum

Syntax

`md5sum [-c | -s | -w] [<FILE-NAME>]`

Description

This command computes and checks the MD5 message digest.

Command context

ServiceOS (`SVOS>`)

Parameters

`[-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.

Authority

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

Example

Computing and checking the MD5 message digest for /nos/primary.swi:

```
SVOS> md5sum /nos/primary.swi
93ffc89e7ec357854704d8e450c4b7ab  /nos/primary.swi
SVOS>
```

mkdir

Syntax

`mkdir [-m | -p] [<DIRECTORY-NAME>]`

Description

This command makes directories.

Command context

ServiceOS (`SVOS>`)

Parameters

`[-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.

Authority

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

Example

Making the dir directory:

```
SVOS> mkdir dir
```

mount

Syntax

`mount` *`<DEVICE>`*

Description

This command mounts the SSD partitions to the following locations: `/coredump`, `/logs`, `/nos`, `/selftest`, and mounts the USB device to `/mnt/usb`.

Users can mount USB flash drives formatted as either FAT16 or FAT32 with a single partition.

Command context

ServiceOS (`SVOS>`)

Parameters

`<DEVICE>`

Specifies the device to be mounted. Supported device options include `all` and `usb`.

Authority

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

Examples

Mounting all of the SSD partitions:

```
SVOS> mount all
SVOS> mount usb
```

mv

Syntax

```
mv [-f | -i | -n] <TARGET-DIRECTORY>
```

Description

This command moves (renames) files.

Command context

ServiceOS (SVOS>)

Parameters

-f
: Specifies not to prompt before overwriting.

-i
: Specifies to prompt before overwriting.

-n
: Specifies to not overwrite an existing file.

Authority

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

Example

Moving the file named myfile:

```
SVOS> mv myfile
```

password

Syntax

```
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.

Command context

ServiceOS (SVOS>)

Authority

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

Example

Setting the admin account password:

```
SVOS> password
Enter password:********
Confirm password:********
SVOS>
```

ping

Syntax

```
ping <HOST-IP-ADDRESS>
```

Description

Pings network hosts for debug purposes.

Command context

ServiceOS (SVOS>)

Parameters

<HOST-IP-ADDRESS>

Specifies the host IP address.

Authority

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

Example

Pinging a network host:

```
SVOS> ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10): 56 data bytes
64 bytes from 10.0.8.10: seq=0 ttl=63 time=3.496 ms
64 bytes from 10.0.8.10: seq=1 ttl=63 time=0.367 ms
64 bytes from 10.0.8.10: seq=2 ttl=63 time=0.380 ms
64 bytes from 10.0.8.10: seq=3 ttl=63 time=0.282 ms
64 bytes from 10.0.8.10: seq=4 ttl=63 time=0.669 ms
^C
--- 10.0.8.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.282/1.038/3.496 ms
SVOS>
```

pwd

Syntax

```
pwd
```

Description

Displays the current working directory.

Command context

ServiceOS (SVOS>)

Authority

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

Example

Displaying the current working directory:

```
SVOS> pwd
/home
SVOS>
```

reboot

Syntax

`reboot`

Description

Reboots the Management Module.

Command context

ServiceOS (`SVOS>`)

Authority

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

Example

Rebooting the management module:

```
SVOS> reboot
reboot: Restarting system
```

rm

Syntax

`rm [-f | -i | -R | -r] <FILE-NAME>`

Description

Removes files or directories.

Command context

ServiceOS (`SVOS>`)

Parameters

`[-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.

Authority

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

Example

Removing the file named `foo`:

```
SVOS> rm foo
```

rmdir

Syntax

`rmdir [-p] <DIRECTORY-NAME>`

Description

Removes empty directories.

Command context

ServiceOS (`SVOS>`)

Parameters

`-p`

Specifies to remove parent directories.

Authority

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

Example

Removing the empty `foo` directory:

```
SVOS> rmdir foo
SVOS>
```

secure-mode

Syntax

`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.

Command context

ServiceOS (`SVOS>`)

Authority

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

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>
```

sh

```
Syntax
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.

Command context

ServiceOS (`SVOS>`)

Authority

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

Example

Launching a bash shell:

```
SVOS> sh
switch:/cli/fs/home#
```

umount

Syntax

`umount <DEVICE>`

Description

Unmounts the SSD partitions mounted to the following locations: `/coredump`, `/logs`, `/nos`, `/selftest`, and unmounts the USB device mounted to `/mnt/usb`.

Command context

ServiceOS (`SVOS>`)

Parameters

`<DEVICE>`

Specifies the device to be unmounted. Supported device options include `all` and `usb`.

Authority

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

Examples

Unmounting all devices:

```
SVOS> umount all
SVOS> umount usb
```

Unmounting a USB device:

```
SVOS> umount all
SVOS> umount usb
```

update

Syntax

`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.

Command context

ServiceOS (`SVOS>`)

Parameters

`{primary | secondary}`

Selects either the primary or secondary image.

`<IMAGE>`

Specifies the image name.

Authority

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

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
```

tftp

Syntax

```
tftp {-b | -g | -l <LOCAL-FILE> | -p | -r <REMOTE-FILE>} host [<PORT>]
```

Description

Transfers files to and from a remote machine (TFTP a file).

Command context

ServiceOS (`SVOS>`)

Parameters

`{-b | -g | -l | -p | -r <REMOTE-FILE>}`

Selects the options for transferring a file.

`-b`

Specifies the transfer blocks of size octets. The default blocksize is set to 1468, which can be overridden with the -b option.

`-g`

Specifies to get a file.

`-l`

Specifies a local file.

`-p`

Specifies to put a file in remote location.

`-r <REMOTE-FILE>`

Specifies a remote file.

`<PORT>`

Specifies the port for transfer. If no port option is specified, TFTP uses the standard UDP port 69 by default.

Authority

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

Example

Transfering files:

```
SVOS> tftp -b 65464 -g -r XL.10.00.0002.swi.swi 192.0.2.1
XL.10.00.0002 100% |*******************************|   178M  0:00:00 ETA
SVOS>
```

version

Syntax

`version`

Description

Displays the following build strings:

- Version.
- Build date.
- Build time.
- Build ID.
- SHA.

Command context

ServiceOS (`SVOS>`)

Authority

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

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>
```

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

Syntax

```
clear update-log
```

Description

Clears stored log files of any In-System Programming updates on the system.

Command context

Manager (#)

Authority

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

show needed-updates

Syntax

```
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 context

Manager (`#`)

Authority

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

The 8320 switch only supports Boot-up Diagnostics (Power On Selftest aka POST).

Power On Self Test (POST) is the first task which verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST comprises of the following:

- **Register read/write**

  This test checks for the registers and tables in the ingress pipeline of ASIC. It is always run during platform initialization only.

- **Front-end Port Loopback tests**

  This is to verify the physical port front-end interface.

  These tests check if a particular interface can function properly. A test failure would mean that the particular interface is marked as "Failed" and thus it would become unavailable for use.

  This test is run when "no fastboot" is configured.

Selftest commands

fastboot

Syntax

```
fastboot
no fastboot
```

Description

Enables fastboot for the system.

The `no` form of this command disables fastboot for the system.

Command context

```
config
```

Authority

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

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 ArubaOS-CX XL.10.00.0002
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
  no routing
```

Disabling fastboot:

```
switch# configure terminal
switch(config)# no fastboot
switch(config)# end
switch(config)# write mem
Configuration changes will take time to process, please be patient.
switch# show running-config
Current configuration:
!
!Version ArubaOS-CX XL.10.00.0002
module 1/1 product-number jl363a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
  no routing
```

show selftest

Syntax

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

Description

Displays selftest results.

Command context

Manager (#)

Parameters

`[brief]`

Shows the selftest results as a brief description. Default.

`line-module`

Shows the selftest results for a line module.

`<SLOT-ID>`

Shows the selftest results for the slot ID of the line or fabric module.

`<PORT-NUM>`

Shows the selftest results for the port number.

`[vsx-peer]`

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

Authority

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

Examples

Displaying the output when fastboot is disabled on an 8320 switch:

```
switch# show selftest interface



Name       Status            ErrorCode        LastRunTime

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

1/1/2      skipped           0x0

1/1/44     skipped           0x0

1/1/46     skipped           0x0

switch# show selftest interface 1/1/1
```

```
Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- --------------------
1/1/1      skipped           0x0
```

Displaying the output when fastboot is enabled:

```
switch# show selftest interface 1/1/2
Name    Status         ErrorCode LastRunTime
------- -------------- --------- --------------------
1/1/2   skipped        0x0

switch# show selftest line-module 1/1 interface
Name    Status         ErrorCode LastRunTime
------- -------------- --------- --------------------
1/1/1   skipped        0x0
1/1/2   skipped        0x0
1/1/3   skipped        0x0
1/1/31  skipped        0x0
```

Displaying the output when fastboot is disabled:

```
switch# show selftest interface

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- --------------------
1/1/12     passed            0x0              2018-02-16 18:15:53
1/1/47     passed            0x0              2018-02-16 18:15:53
1/1/15     passed            0x0              2018-02-16 18:15:53

switch# show selftest interface 1/1/1

Name       Status            ErrorCode        LastRunTime
---------- ----------------- ---------------- --------------------
1/1/1      passed            0x0              2018-02-16 18:15:53
```

Testing to register read/write:

This test is run irrespective of fastboot being enabled or disabled.

```
switch# show selftest

Name       Id   Status         ErrorCode  LastRunTime
---------- ---- -------------- ---------- --------------------
LineModule 1/1  passed         0x0        2018-02-16 18:15:53
```

Device zeroization lets you remove all user files from flash storage, including solid-state drives (SSDs). User files cannot be retrieved after the zeroization is complete.

Zeroization can occur in both AOS-CX and Service OS. This section covers zeroization and AOS-CX. For information about zeroization and Support OS, see erase zeroize.

Zeroization preserves the primary and secondary software images on the SSD. Zeroization also preserves manufacturing information.

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

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

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

Zeroization commands

erase all zeroize

Syntax

```
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.

Command context

Manager (#)

Authority

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

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: *****
```

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 only on the SSH 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. If the SSH session is terminated, the terminal monitor is no longer valid. In the new SSH session, you need to run the command again.

Terminal monitor commands

terminal-monitor {notify | severity | filter}

Syntax

```
terminal-monitor {notify <event|debug|all> | severity <level> | filter keyword}

no terminal-monitor
```

Description

Enables the terminal monitor feature in the SSH session. It display 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 disables the terminal monitor configuration.

Parameters

`notify <event|debug|all>`

Specifies the type of log notification.

- **Event:** Displays the event log messages.
- **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 (default), warning, notice, information, 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 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
```

show terminal-monitor

Syntax

```
show terminal-monitor
```

Description

Shows whether the terminal monitoring is enabled or disabled.

Authority

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

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
```

The following section describes symptoms, causes and corrective actions for 401 or 404 errors.

HTTP 404 error when accessing the switch URL

Symptom

The switch is operational and you are using the correct URL for the switch, but attempts to access the REST API or Web UI result in an HTTP 404 "Page not found" error.

Cause

REST API access is not enabled on the VRF that corresponds to the access port you are using. For example, you are attempting to access the REST API or Web UI from the management (OOBM) port, and access is not enabled on the `mgmt` VRF.

Action

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

For example:

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

HTTP 401 error "Login failed: session limit reached"

Symptom

A REST request or Web UI login attempt returns response code 401 and the response body contains the following text string:

```
Login failed: session limit reached
```

Cause

A user attempted to log into the REST API or the Web UI, but that user already has the maximum number of concurrent sessions running.

Action

1. Log out from one of the existing sessions.

   Browsers share a single session cookie across multiple tabs or even windows. However, scripts that POST to the login resource and later do not POST to the logout resource can easily create the maximum number of concurrent sessions.
2. If the session cookie is lost and it is not possible to log out of the session, then wait for the session idle time limit to expire.

   When the session idle timeout expires, the session is terminated automatically.

3. If it is required to stop all HTTPS sessions on the switch instead of waiting for the session idle time limit to expire, you can stop all HTTPS sessions using the `https-server session close all` command.

   This command stops and starts the `hpe-restd` service, so using this command affects all existing REST sessions, Web UI sessions, and real-time notification subscriptions.

Accessing Aruba Support

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

Be sure to collect the following information before contacting Support:

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

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba software and documentation	https://asp.arubanetworks.com/downloads

Accessing Updates

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.