

ArubaOS-Switch Basic Operation Guide for 16.04



Part Number: 5200-3114b
Published: September 2017
Edition: 3

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

Intel[®], Itanium[®], Pentium[®], Intel Inside[®], and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

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

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

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

UNIX[®] is a registered trademark of The Open Group.

Chapter 1 About this guide	9
Applicable products.....	9
Switch prompts used in this guide.....	9
Chapter 2 Getting Started	11
Using the switch setup screen.....	11
Configuring and displaying a nondefault banner.....	13
Example: Configuring and displaying a banner.....	13
Example: Setting the user-configurable banner message after authentication.....	14
Physical installation.....	15
Initial switch set-up.....	15
Recommended minimal configuration.....	16
Login banners.....	16
Custom log in banners.....	16
Banner operation with telnet, serial, or SSHv2 access.....	16
Banner operation with the WebAgent.....	16
Banner operating notes.....	16
banner motd command with non-interactive mode.....	17
Chapter 3 Using the Menu Interface	19
Starting a menu interface session.....	19
Ending a menu session and exiting the console.....	20
Rebooting the switch.....	21
Configuring ports on HPE 3800 switches with stacking enabled.....	22
Using individual features of the menu interface.....	23
Main Menu features.....	23
Overview of the Menu Interface.....	24
Screen structure and navigation.....	25
Privilege levels and password security.....	27
Menu interaction with other interfaces.....	27
Chapter 4 ArubaOS-Switch UI	28
Accessing the ArubaOS-Switch Next Generation UI.....	28
Using HTTPS secure connection.....	28
Improved UI functionality.....	31
System — Status.....	34
System — Events.....	35
System — Stack.....	36
System — Monitor.....	38
System — SNMP.....	39
System — Firmware Update.....	40
Interfaces — Ports.....	41
Interfaces — PoE.....	42
Interfaces — Monitor.....	43
Interfaces — VLANs.....	44
Interfaces — Trunks.....	45
Traffic — Spanning Tree.....	46

Security — Clients.....	47
Security — User Roles.....	48
Security — Intrusion Log.....	49
Security — Port Security.....	49
Security — IP Authorization.....	50
Configurations — Config Report.....	51
Configurations — Management.....	52
Chapter 5 Operating in Preview Mode.....	53
Overview of Preview Mode.....	53
Enabling Preview Mode.....	53
Viewing features in Preview Mode.....	54
Multicast Offload Engine.....	54
Enabling MOE.....	55
Chapter 6 Using the Command Line Interface (CLI).....	56
Listing available commands.....	56
Listing command options.....	57
Displaying CLI “Help”.....	58
Enabling and disabling CLI message prefixes.....	59
Enabling and disabling CLI interactive command mode.....	59
Interactive commands requiring additional options.....	60
Menu commands.....	61
SNMPv3 special cases.....	61
Simplifying entry of commands at the command line.....	61
Finding or completing a command.....	61
redo.....	62
repeat.....	63
alias.....	64
CLI shortcut keystrokes.....	65
Overview of the CLI.....	66
Privilege levels for CLI access.....	67
Privilege levels at log on.....	67
Privilege level operation.....	68
Operator privileges.....	69
Manager privileges.....	69
Configuration commands and context configuration modes.....	71
Chapter 7 Configuring the switch.....	74
Using the CLI to implement configuration changes.....	74
Creating a custom default configuration.....	77
Copying an existing configuration file to the custom default configuration file.....	78
Copying the custom default config file onto the switch.....	78
Copying the custom default config file off the switch.....	78
Using SFTP and SCP to transfer the custom configuration.....	79
Erasing a configuration file.....	79
Displaying the configuration files.....	80
Troubleshooting custom default configuration files.....	83
Using the menu and WebAgent to implement configuration changes configuration file.....	83
Zeroizing the file storage of the management module.....	86
Zeroizing the management module files.....	86
Zeroizing from the ROM console.....	87
Zeroization.....	87

Using Primary and Secondary flash image options.....	88
Displaying the current flash image data.....	88
Switch software downloads.....	89
Replacing or removing local switch software.....	90
Rebooting the switch.....	91
Setting the default flash for bootup.....	91
Booting from the default flash or configuration file.....	92
Booting from a specified flash.....	93
Enabling and disabling the fastboot option.....	93
Using reload.....	93
Boot and reload command comparison.....	96
Operating notes about booting.....	96
Managing multiple configuration files.....	97
Viewing the status and content of startup-config files.....	97
Changing or overriding the reboot configuration policy.....	97
Managing startup-config files in the switch.....	98
Uploading a configuration file to a remote TFTP host.....	99
Downloading a configuration file from a remote TFTP host.....	100
Uploading a configuration file to a serially connected host.....	100
Downloading a configuration file from a serially connected host.....	101
Multiple configuration files.....	101
Operating notes for multiple configuration files.....	102
Viewing the configuration of interfaces.....	104
Viewing the running configuration of interfaces.....	104
Viewing the startup configuration of interfaces.....	108
Using automatic configuration update with DHCP Option 66.....	110
Enabling and disabling the configuration file update using Option 66.....	110
Possible scenarios for updating the configuration file.....	110
Operating notes about automatic configuration.....	111
Overview of switch configuration.....	112
Configuration file management.....	112

Chapter 8 Managing interface access and System Information..... 114

Managing interface access.....	114
Listing the current console/serial link configuration.....	114
Enabling and disabling inbound Telnet access.....	114
Initiating an outbound Telnet session to another device.....	115
Web-management interface configuration for idle timeout.....	116
Enabling and disabling inbound WebAgent access.....	117
Reconfiguring the console/serial link settings.....	117
Software version support of console/serial link settings.....	118
Interface-access parameters.....	119
Terminal line width and length settings.....	119
Window size negotiation for a telnet session.....	120
Denying interface access.....	120
Viewing and setting system information.....	121
Viewing system information.....	121
Setting system information.....	122
System parameters.....	123

Chapter 9 Configuring IP Addressing..... 125

Using the menu or WebAgent to configure IP addressing.....	125
Using the Switch Setup screen to quickly setup IP addressing.....	125
Using the menu to configure IP address, Gateway, and Time-To-Live (TTL).....	125

Using the WebAgent to configure IP addressing.....	126
Using the CLI to configure IP Addressing, Gateway, and Time-To-Live (TTL).....	126
Viewing the current IP configuration.....	126
Configuring an IP address and subnet mask on a VLAN.....	127
Removing an IP address that is configured on a VLAN.....	128
Multiple IP addresses configuration on a VLAN (multinetting).....	128
Removing IP addresses from a multinetted VLAN.....	129
Configuring the optional default gateway.....	129
Setting the Time-To-Live (TTL).....	130
Managing loopback interfaces.....	130
Adding a loopback interface.....	130
Removing a loopback interface.....	131
Displaying loopback interface configurations.....	131
Summary of loopback interface configuration.....	132
Overview of loopback interfaces.....	133
Retaining VLAN-1 IP addressing across configuration file downloads.....	133
Enabling IP preserve to retain VLAN-1 IP addressing.....	133
Operating rules for IP preserve.....	133
Overview of IP preserve.....	134
Configuring a single source IP address for software applications.....	136
Specifying the source IP address.....	136
Canceling the source IP address assignment.....	136
Viewing source IP address configurations.....	136
Viewing source IP selection policy status.....	137
Viewing full source IP details.....	138
Viewing protocol configuration and status information.....	139
Configuration error messages.....	140
Overview of single source IP addresses for software applications.....	140
The source IP selection policy.....	141
IP configuration features.....	142
Effects of IP addressing on switch operation.....	143
Network preparations for configuring DHCP/Bootp.....	144
Overview of IP Addressing.....	145
IP addressing with multiple VLANs.....	145
DHCP/Bootp operation.....	145

Chapter 10 Managing switch software..... 148

Viewing or downloading the software manual set.....	148
Updating the switch software to a new version.....	148
Updating the switch software.....	148
Backing up your current configuration and image.....	149
Downloading and installing software from a TFTP server.....	150
Downloading and installing software from a PC or Unix workstation.....	150
Downloading and installing software from a USB flash drive.....	151
Best practices, recommendations, and precautions.....	152
Validating switch software.....	153
Validating a software image.....	153
Software signing and verification.....	154
Rolling back switch software.....	154
Managing scheduled jobs.....	155
Schedule a job to run automatically.....	155
Deleting a scheduled job.....	157
Viewing scheduled jobs.....	157
Time adjustments and scheduling jobs.....	158
The Job Scheduler.....	159

Alternate configuration files.....	159
Chapter 11 Daylight Saving Time.....	161
Chapter 12 Managing power-saving features.....	163
Configuring the module power-saving option.....	163
Configuring the LED power-saving option.....	163
Configuring the slot low-power option.....	164
Disabling power-saving options.....	165
Enabling energy-efficient-ethernet (EEE).....	165
Enabling advertisement of EEE TLVs.....	166
Disabling EEE or advertisement of EEE TLV.....	167
Hibernate mode.....	167
hibernate.....	167
Viewing settings for power-saving and energy efficiency.....	168
Displayed values for Energy-efficient-ethernet (EEE).....	170
Power-saving features supported by modules.....	171
Overview of power-saving features.....	172
Chapter 13 Websites.....	174
Chapter 14 Support and other resources.....	175
Accessing Hewlett Packard Enterprise Support.....	175
Accessing updates.....	175
Customer self repair.....	175
Remote support.....	176
Warranty information.....	176
Regulatory information.....	176
Documentation feedback.....	177
Finding and Maintaining Networking Devices.....	178
Compliance.....	179
RFC 4292.....	179
RFC 4292 supported operations.....	179
RFC 4292 MIB operations.....	180
JITC authorization requirements.....	181
Local authentication and authorization.....	181
Security user log access.....	181
Authentication and Authorization through RADIUS.....	182
Authentication and Authorization through TACACS.....	182
Common access card (two-factor) authentication.....	182
Overview.....	182
Two-factor authentication.....	182
Restrictions.....	182
Expected behaviors.....	183
Secure Mode.....	184
Federal government certification.....	184

Managing the device link detection protocol (DLDP)	186
Enabling or disabling DLDP.....	186
Setting the DLDP advertisement interval.....	186
Enabling and disabling types of DLDP debugging.....	186
Clearing statistics on DLDP packets.....	187
Viewing DLDP configuration information and statistics.....	187
Setting the DLDP delaydown timer.....	189
Setting DLDP unidirectional-shutdown mode.....	189
Setting the DLDP authentication-mode.....	189
Setting or removing a DLDP authentication password.....	190
Include-credentials and encrypt-credentials considerations.....	190
Validation rules for DLDP.....	192
Restrictions for DLDP.....	193
Overview of device link detection protocol (DLDP).....	193
Mobile web interface	195
Viewing web management-to-server configurations.....	195
Validation rules.....	195

This guide provides information on how to use the switch interfaces and introduces basic operations.

Applicable products

This guide applies to these products:

Aruba 2530 Switch Series (J9772A, J9773A, J9774A, J9775A, J9776A, J9777A, J9778A, J9779A, J9780A, J9781A, J9782A, J9783A, J9853A, J9854A, J9855A, J9856A, JL070A)

Aruba 2540 Switch Series (JL354A, JL355A, JL356A, JL357A)

Aruba 2620 Switch Series (J9623A, J9624A, J9625A, J9626A, J9627A)

Aruba 2920 Switch Series (J9726A, J9727A, J9728A, J9729A, J9836A)

Aruba 2930F Switch Series (JL253A, JL254A, JL255A, JL256A, JL258A, JL259A, JL260A, JL261A, JL262A, JL263A, JL264A)

Aruba 2930M Switch Series (JL319A, JL320A, JL321A, JL322A, JL323A, JL324A)

Aruba 3800 Switch Series (J9573A, J9574A, J9575A, J9576A, J9584A)

Aruba 3810 Switch Series (JL071A, JL072A, JL073A, JL074A, JL075A, JL076A)

Aruba 5400R zl2 Switch Series (J9821A, J9822A, J9850A, J9851A, JL001A, JL002A, JL003A, JL095A)

Switch prompts used in this guide

Examples in this guide are representative and may not match your particular switch/environment. The following table explains the types of command prompts that may be used in examples, along with information on what each prompt indicates.

Prompt	Explanation
switch#	# indicates manager context (authority).
switch>	> indicates operator context (authority).
switch(config)#	(config) indicates the config context.
switch(vlan-x)#	(vlan-x) indicates the vlan context of config, where x represents the VLAN ID. For example: switch(vlan-128)#.
switch(eth-x)#	(eth-x) indicates the interface context of config, where x represents the interface. For example: switch(eth-48)#.
switch-Stack#	Stack indicates stacking is enabled.
switch-Stack(config)#	Stack(config) indicates the config context while stacking is enabled.

Table Continued

Prompt	Explanation
switch-Stack (stacking) #	Stack (stacking) indicates the stacking context of config while stacking is enabled.
switch-Stack (vlan-x) #	Stack (vlan-x) indicates the vlan context of config while stacking is enabled, where x represents the VLAN ID. For example: switch-Stack (vlan-128) #.
switch-Stack (eth-x/y) #	Stack (eth-x/y) indicates the interface context of config, in the form (eth-<member-in-stack>/<interface>). For example: switch (eth-1/48) #

Using the switch setup screen

The quickest and easiest way to minimally configure the switch for management and password protection is to use a direct console connection to the switch, start a console session and access the Switch Setup screen.

Procedure

1. Using the method described in the *Installation and Getting Started Guide* for your switch, connect a terminal device to the switch and display the switch console command (CLI) prompt (the default display).
2. The CLI prompt appears displaying the switch model number, for example: **HPE switch#**
3. Screen. The following illustration is an example of a Setup screen with default settings. Your screen may vary slightly.

Figure 1: Example Switch Setup screen

```
HP Switch
=====-- TELNET - MANAGER MODE -----
                        Switch Setup

System Name : HP Switch
System Contact :
Manager Password :
Confirm Password :
Logon Default : CLI                               Time Zone [0] : 0
Community Name : public                           Spanning Tree Enabled [No] : No
Default Gateway :
Time Sync Method [None] : TIMEP
TimeP Mode [Disabled] : Disabled

IP Config [Manual] : DHCP/Bootp

IP Address   : 127.0.0.1
Subnet Mask  : 255.255.255.255
Actions->   Cancel      Edit      Save      Help

Enter System Name - up to 32 characters.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

4. Use the **[Tab]** key to select the **Manager Password** field and enter a manager password of up to 16 characters and press **[Tab]**.
5. Tab to the **IP Config (DHCP/Bootp)** field and use the **Space** bar to select the **Manual** option and press **[Tab]**.
6. Tab to the **IP Address** field and enter the IP address that is compatible with your network and press **Enter**.
7. Tab to the **Subnet Mask** field and enter the subnet mask used for your network.
8. Press **S** (for Save).



After editing, pressing **Enter** and then selecting Save will also save the configuration.

Table 1: Setup screen field descriptions

Parameter	Default	
System Name	blank	Optional; up to 255 characters, including spaces
System Contact	blank	Optional; up to 255 characters, including spaces
Manager Password	blank	Recommended; up to 16 characters (no blank spaces)
Logon Default	CLI	The default setting selects the command-line interface for console access. The alternative is the Menu interface.
Time Zone	0 (none)	Optional: 1440 to -1440. The number of minutes your location is to the West (-) or East (+) of GMT.
Community Name	public	Default setting recommended.
Spanning Tree Enabled	No	Default setting recommended unless STP is already running on your network or the switch will be used in complex network topologies.
Default Gateway	blank	Recommended. Enter the IP address of the next-hop gateway node if network traffic has to reach off-subnet destinations.
Time Sync Method	TimeP	Optional: The protocol the switch uses to acquire a time signal. The options are SNTP and TimeP.
TimeP Mode	Disabled	Synchronizes the time kept on the switch to the TimeP server ¹ .
IP Config	DHCP/ Bootp	Set to Manual unless a DHCP/Bootp server is used on your network to configure IP addressing.
IP Address	xxx.xxx.xx x.xxx	Recommended. If you set IP Config to Manual, then enter an IP address compatible with your network ² .
Subnet Mask	xxx.xxx.xx x.xxx	Recommended. If you entered an IP address, then enter a subnet mask compatible with your network ² .

¹For more on this topic, see the "Time Protocols" chapter in the latest *Management and Configuration Guide* for your switch.

²The IP address and subnet mask assigned for the switch must be compatible with the IP addressing used in your network. For more on IPv4 addressing, see **Configuring IP Addressing** on page 125. For IPv6 addressing topics, see the latest IPv6 configuration guide for your switch.

Configuring and displaying a nondefault banner

You can enable or disable banner operation using either the switch's CLI or an SNMP application. The steps include:

Procedure

1. Enable nondefault banner operation and define the endpoint delimiter for the banner.
2. Type the desired banner text, including line breaks.
3. Type the endpoint delimiter.

Use `show banner motd` to display the current banner status.

Syntax

```
banner motd {<delimiter>}
```

```
no banner motd
```

This command defines the single character used to terminate the banner text and enables banner text input. You can use any character except a blank space as a delimiter. The `no` form of the command disables the login banner feature.

```
<banner-text-string>
```

The switch allows up to 3070 banner characters, including blank spaces and CR-LF (**[Enter]**). (The tilde “~” and the delimiter defined by `banner motd <delimiter>` are not allowed as part of the banner text.) While entering banner text, you can backspace to edit the current line (that is, a line that has not been terminated by a CR-LF.) However, terminating a line in a banner by entering a CR-LF prevents any further editing of that line. To edit a line in a banner entry after terminating the line with a CR-LF requires entering the delimiter described above and then reconfiguring new banner text.



In redundant management, the banner is not seen on the standby module, only the active module.

Example: Configuring and displaying a banner

Procedure

1. The following banner can be configured on your switch.

```
                This is a private system maintained by the  
  
                Allied Widget Corporation  
  
Unauthorized use of this system can result in  
  
                civil and criminal penalties!
```

2. Click **Enter**.

Use the **Enter** key to create line breaks, blank spaces for line centering, and the delimiter symbol to terminate the banner message.

```
switch(config)# banner motd %
```

Enter TEXT message. End with the character'

```
This is a private system maintained by the
  Allied Widget Corporation.
  Unauthorized use of this system can result in
    civil and criminal penalties!%
switch(config)# write memory
```

3. To view the current banner configuration, use either the `show banner motd` or `show running` command.

```
switch(config)# show banner motd
Banner Information
Configured Banner:

  This is a private system maintained by the
    Allied Widget Corporation.
  Unauthorized use of this system can result in
    civil and criminal penalties!
```

- 4.

```
switch (config)# show running
Running configuration:
; J8697A Configuration Editor; Created on release #K.15.12.0001
; Ver #01:01:00

hostname "switch"
module 1 type J8702A
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24
  ip address dhcp-bootp
  exit
banner motd "This is a private system maintained by the\n Allied Widget
Corporation.\nUnauthorized use of this system can result in\n civil and
criminal penalties!"
password manager

switch (config)#
```

The next time someone logs on to the management CLI, the login screen displays the configured banner. Entering a correct password clears the banner and displays the CLI prompt.

- 5.

```
  This is a private system maintained by the
    Allied Widget Corporation.
  Unauthorized use of this system can result in
    civil and criminal penalties!
```

Example: Setting the user-configurable banner message after authentication

Procedure

1. A text message that has been configured with the

`banner motd` command displays with the authentication prompt when a user opens a console, telnet, SSH, or WebAgent session.

2. The

`exec` option of the `banner` command displays a user-configurable message after the user has been authenticated. If there is no password on the switch, the `exec` banner message displays immediately.

3. Syntax

```
banner exec <ASCII-string>  
no banner exec <ASCII-string>
```

4. Sets the `exec` banner text. Text can be multiple lines up to 3070 characters, and can consist of any printable character except the tilde (~) and the delimiting character.

<ASCII-string>

5. The text must end with a delimiting character, which can be any single character except the tilde (~) character.
6. The `no` version of the command removes the `banner exec` text.

```
switch(config)# banner exec &
```

Enter TEXT message. End with the character &

```
This is Switch A in the language lab
```

Use the `show banner exec` command to display the status and text for the `exec` banner configuration.

7.

```
switch(config)# show banner exec
```

```
Banner Information
```

```
Banner Status: Enabled
```

```
Configured Banner:
```

```
This is Switch A in the language lab
```

Physical installation

Use the *Installation and Getting Started Guide*, available at <http://www.hpe.com/support>:

- Notes, cautions, and warnings related to installing and using the switch and its related modules.
- Instructions for physically installing the switch in your network.
- Quickly assigning an IP address and subnet mask, setting a Manager password, and (optionally) configuring other basic features.
- Interpreting LED behavior.

Initial switch set-up

Initial setup includes:

- Setting a Manager password
- Assigning an IP (Internet Protocol) address and subnet mask
- Configuring optional banners

Recommended minimal configuration

In the factory default configuration, the switch has no IP (Internet Protocol) address and subnet mask, and no passwords. In this state, it can be managed only through a direct console connection. To manage the switch through in-band (networked) access, you must configure the switch with an IP address and subnet mask compatible with your network. Also, you must configure a Manager password to control access privileges from the console and web browser interface. Other parameters in the Switch Setup screen can be left at their default settings or you can configure them with values you enter.

For more information on IP addressing, see [Configuring IP Addressing](#) on page 125.



By default, the switch is configured to acquire an IPv4 address configuration from a DHCP or Bootp server. To use DHCP/Bootp instead of the manual method described in this chapter, see DHCP/Bootp Operation in the *Management and Configuration Guide* for your switch.

For information on configuring IPv6 addressing, see to the latest *IPv6 Configuration Guide* for your switch.

Login banners

Custom log in banners

You can configure the switch to display a login banner of up to 3070 characters. An operator initiates a management session with the switch through any of the following methods:

- Telnet
- Serial connection
- SSHv2
- WebAgent

The default banner displays product registration information; the copyright splash is no longer displayed.

If a banner is configured, the banner page is displayed when you access the WebAgent. The default product registration information is not displayed as there is already a product registration prompt displayed in the WebAgent.

Banner operation with telnet, serial, or SSHv2 access

When a system operator begins a login session, the switch displays the banner above the prompts for local password and **Press any key to continue**. Entering a correct password or, if no password is configured, pressing any key clears the banner from the CLI and displays the CLI prompt.

Banner operation with the WebAgent

When a system operator uses the WebAgent to access the switch, the text of a nondefault banner configured on the switch appears in a dedicated banner window with a link to the next page. Click **Continue** to display either the Registration page or the switch's home page. If the banner feature is disabled or if the switch is using the factory-default banner, then the banner page does not appear in the WebAgent screen when an operator initiates a login session with the switch.

Banner operating notes

- The default banner appears only when the switch is in the factory default configuration. Using the command `no banner motd` deletes the currently configured banner text and blocks display of the default banner. The default banner is restored only if the switch is reset to its factory default configuration.
- The switch supports one banner at any time. Configuring a new banner replaces any former banner configured on the switch.

- If the switch is configured with `ssh version 1` or `ssh version 1-or-2`, configuring the banner sets the SSH configuration to `ssh version 2` and displays the message `Warning: SSH version has been set to v2.`
- If a banner is configured, the switch does not allow configuration with `ssh version 1` or `ssh version 1-or-2`. Attempting to do so produces the error message `Banner has to be disabled first..`
- If a banner is enabled on the switch, the WebAgent displays `Notice` to all users on the banner page.

banner motd command with non-interactive mode

The use of escape characters allows the `banner motd` command to be used in non-interactive mode for multiple message lines. In non-interactive mode, you can create a banner message enclosed in double quotes or other delimiter that uses escape characters within the delimiters. Other existing CLI commands do not support the escape characters. For more information on interactive and non-interactive mode, see [Enabling and disabling CLI interactive command mode](#) on page 59 in this guide.

Table 2: Supported escape characters

Character	
<code>\"</code>	double quote
<code>\'</code>	single quote
<code>\`</code>	forward quote
<code>\\</code>	backslash
<code>\f</code>	form feed
<code>\n</code>	newline
<code>\r</code>	carriage return
<code>\t</code>	horizontal tab
<code>\v</code>	vertical tab

Configuring the banner message using escape characters within double quote delimiters

```
switch(config)# banner motd
"You can use the \'banner motd\' CLI command in non-interactive mode.\n\n\tThe
banner
motd command will support escape characters."

switch(config)# show banner motd

Banner Information

Banner status: Enabled

Configured Banner:

You can use the 'banner motd' CLI command in non-interactive mode.
```

The banner motd command will support escape characters."

The running configuration file with banner motd configured in non-interactive mode

```
switch(config)# show running-config

Running configuration:

;J8693A Configuration Editor; Created on release #K.15.10.0002
;Ver #01:01:00

hostname "switch"
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-48, a1-a4
  ip address dhcp-bootp
  exit
banner motd "You can use the \'banner motd\' CLI command in
non-interactive mode.\n\n\tThe banner motd command will support
escape characters."
```

Configuring the banner message using an alternate delimiter of '#'

```
switch(config)# banner motd #
```

Enter TEXT message.

End with the character '#'.
#

You can use the `banner motd` CLI command in non-interactive mode. The `banner motd` command `\n\n\t` will support escape characters #.

Starting a menu interface session

Starting the session

In its factory default configuration, the switch console starts with the CLI prompt. To use the menu interface with Manager privileges, go to the Manager level prompt and enter the **menu** command.

Prerequisites

Before you start a menu interface session, you must complete the following tasks:

1. Configure and connect to the switch. See the *Installation and Getting Started Guide* for your switch.
2. Access the menu interface using any of the following methods.
 - A direct serial connection to the switch's console port, as described in the installation guide you received with the switch
 - A Telnet connection to the switch console from a networked PC or the switch's web browser interface. Telnet requires that an IP address and subnet mask compatible with your network have already been configured on the switch.

Procedure

1. Use one of these methods to connect to the switch:
 - a. A PC terminal emulator or terminal
 - b. Telnet
2. Do one of the following:
 - a. If you are using Telnet, go to step 3.
 - b. If you are using a PC terminal emulator or a terminal, press **[Enter]**
one or more times until a prompt appears.
3. When the switch screen appears, do one of the following:
 - a. If a password has been configured, the password prompt appears.

```
Password: _
```

Type the Manager password and press **[Enter]**. Entering the Manager password gives you manager-level access to the switch. (Entering the Operator password gives you operator-level access to the switch. See the *Access Security Guide* for your switch.)
 - b. If no password has been configured, the CLI prompt appears. Go to the next step.
4. When the CLI prompt appears, display the Menu interface by entering the **menu** command. For example:

```
switch# menu [Enter]
```

results in the following display:

Figure 2: Example of the Main Menu with Manager Privileges

```
----- CONSOLE - MANAGER MODE -----
                          Main Menu

1. Status and Counters...
2. Switch Configuration...
3. Console Passwords...
4. Event Log
5. Command Line (CLI)
6. Reboot Switch
7. Download OS
8. Run Setup
0. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

For a description of Main Menu features, see [Main Menu features](#) on page 23.



To configure the switch using the menu interface instead of the CLI, go to the Manager level prompt in the CLI, enter the **setup** command, and in the resulting display, change the **Logon Default** parameter to Menu. For more information, see the *Installation and Getting Started Guide* of your switch.

Ending a menu session and exiting the console

The method for ending a menu session and exiting the console depends on whether, during the session, any changes made to the switch configuration requires a switch reboot to activate. (Most changes via the menu interface need only a **Save**, and do not require a switch reboot.) Configuration changes that need a reboot are

marked with an asterisk (*) next to the configured item in the menu and also next to the **Switch Configuration** item in the Main Menu.

Figure 3: Example indication of a configuration change requiring a reboot

```
----- CONSOLE - MANAGER MODE -----
                          Main Menu

  1. Status and Counters...
 *2. Switch Configuration...
  3. Console Passwords...
  4. Event Log
  5. Command Line (CLI)
  6. Reboot Switch
  7. Download OS
  8. Run Setup
  0. Logout

Displays the menu for customizing the switch configuration.
To select menu item, press item number, or highlight item and press <Enter>.
(*Needs reboot to activate changes.)
```

Procedure

1. In the current session, if you have not made configuration changes that require a switch reboot to activate, return to the Main Menu and press **[0]** (zero) to logout. Then, exit the terminal program, turn off the terminal, or quit the Telnet session.
2. If you **have** made configuration changes that require a switch reboot— that is, if an asterisk (*) appears next to a configured item or next to **Switch Configuration** in the Main Menu:
 - a. Return to the Main Menu.
 - b. Press **[6]** to select **Reboot Switch** and follow the instructions on the reboot screen.
3. Rebooting the switch terminates the menu session, and if you are using Telnet, disconnects the Telnet session. (See **Rebooting the switch** on page 91).
4. Exit from the terminal program, turn off the terminal, or close the Telnet application program.

Rebooting the switch

Rebooting the switch from the menu interface:

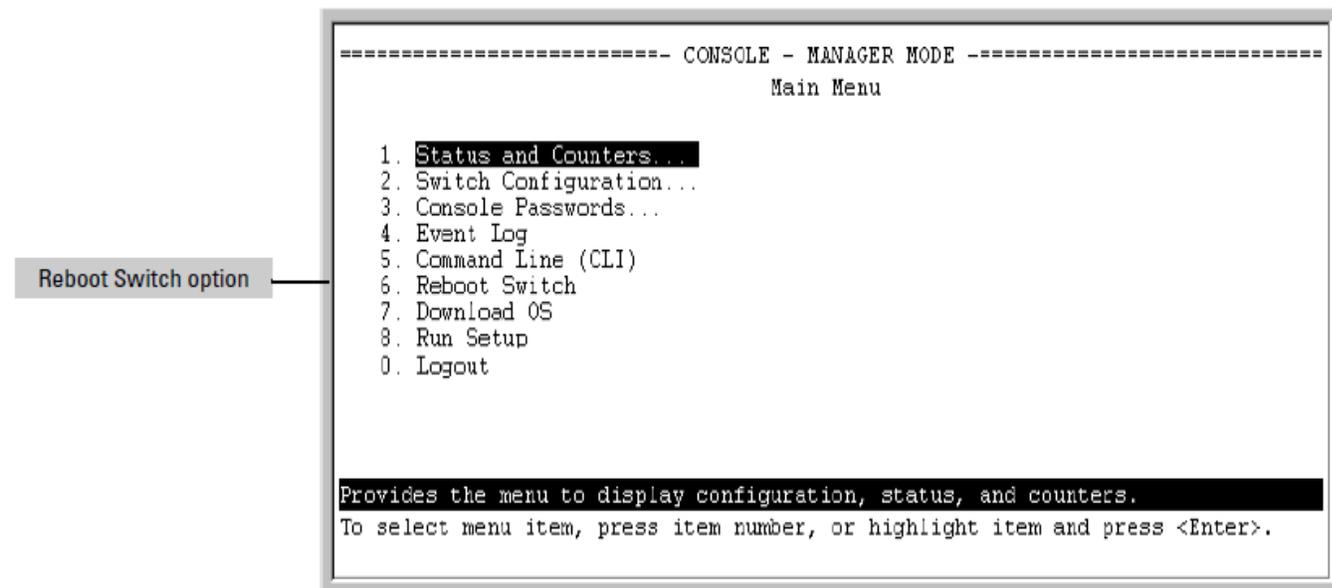
Procedure

1. Terminates all current sessions and performs a reset of the operating system
2. Activates any menu interface configuration changes that require a reboot
3. Resets statistical counters to zero

(Note that statistical counters can be reset to zero without rebooting the switch.)

To Reboot the switch, use the **Reboot Switch** option in the Main Menu. (Note that **Reboot Switch** is not available if you log on in Operator mode; that is, if you enter an Operator password instead of a manager password at the password prompt.)

Figure 4: *The Reboot Switch option in the Main Menu*



Rebooting to activate configuration changes. Configuration changes for most parameters in the menu interface become effective as soon as you save them. However, you must reboot the switch to implement a change in the **Maximum VLANs to support parameter**. To access this parameter, go to the Main Menu and select:

- 2. Switch Configuration
- 8. VLAN Menu
- 1. VLAN Support.

If you make configuration changes in the menu interface that require a reboot, the switch displays an asterisk (*) next to the menu item in which the change has been made. For example, if you change and save the value for the **Maximum VLANs to support parameter**, an asterisk appears next to the **VLAN Support** entry in the VLAN Menu screen, and also next to the **Switch Configuration** entry in the Main Menu.

To activate changes indicated by the asterisk, go to the Main Menu and select the **Reboot Switch** option.



Executing the **write memory** command in the CLI does not affect pending configuration changes indicated by an asterisk in the menu interface. That is, only a reboot from the menu interface or a **boot** or reload command from the CLI will activate a pending configuration change indicated by an asterisk.

Configuring ports on HPE 3800 switches with stacking enabled

When stacking is enabled on an HPE 3800 switch, the procedures for configuring specific switch ports are the same as for 3800 switches without stacking enabled. However, the port designations for the ports in the stack are modified. That is, each port is identified by its switch's stack member ID followed by a slash and then the port

number, as it is shown on the switch. For example, for a switch with stack member ID 3, port 10 on that switch is identified as port 3/10 for CLI command input and output. Entering a CLI command on a 3800 switch configured for stacking without using the modified port designation results in the message "Module not present for port or invalid port".

For more on this topic, see "Interaction with Other Switch Features" in the "Stack Management" chapter of the latest *Management and Configuration Guide* for 3800 switches.

Using individual features of the menu interface.

To use the individual features of the menu interface, see the references listed in the following table.

Option:	Turn to:
To use the Run Setup option	See the <i>Installation and Getting Started Guide</i> shipped with the switch.
To view and monitor switch status and counters	Appendix B, "Monitoring and Analyzing Switch Operation" in the <i>Management and Configuration Guide</i> for your switch.
To learn how to configure and use passwords and other security features	See the <i>Access Security Guide</i> for your switch.
To learn how to use the Event Log	Appendix C, "Using the Event Log for Troubleshooting Switch Problems" in the <i>Management and Configuration Guide</i> for your switch.
To learn how the CLI operates	Using the Command Line Interface (CLI) on page 56
To download switch software	Appendix A, "File Transfers" in the <i>Management and Configuration Guide</i> for your switch.
For a description of how switch memory handles configuration changes	Configuring the switch on page 74

Main Menu features

The Main Menu gives you access to these Menu interface features:

- **Status and Counters:**

Provides access to display screens showing switch information, port status and counters, and port and VLAN address tables. (See the *Management and Configuration Guide* for your switch.) All of the items that are included in **Status and Counters** are stated in the following list:

- Address Table
- General System Information
- Module Information
- Port Address Table
- Port Counters
- Port Status
- Spanning Tree Information
- Switch Management Address Information
- VLAN Address Table

- **Switch Configuration:**

Provides access to configuration screens for displaying and changing the current configuration settings. (See the contents listing at the front of this manual.) For an index of the features covered in the software manuals for your switch, see the *Software feature index-extended manual* for your switch. All of the items that are included in **Switch Configuration** are stated in the following list:

- System Information
- Port/Trunk Settings
- Network Monitoring Port
- IP Configuration
- SNMP Community Names
- IP authorized Managers
- VLAN Menu
- Spanning Tree Operation
- **Console Passwords:**

Provides access to the screen used to set or change Manager-level and Operator-level passwords, and to delete Manager and Operator password protection. (See the *Access Security Guide* for your switch.)
- **Event Log:**

Enables you to read progress and error messages that are useful for checking and troubleshooting switch operation. (See the *Management and Configuration Guide* for your switch.)
- **Command Line (CLI):**

Selects the Command Line Interface at the same level (Manager or Operator) that you are accessing in the Menu interface.
- **Reboot Switch:**

Performs a "warm" reboot of the switch, which clears most temporary error conditions, resets the network activity counters to zero, and resets the system up-time to zero. A reboot is required to activate a change in the VLAN Support parameter.
- **Download OS:**

Enables you to download a new software version to the switch. (See Appendix A, "File Transfers" in the *Management and Configuration Guide* for your switch.)
- **Run Setup:**

Displays the Switch Setup screen for quickly configuring basic switch parameters such as IP addressing, default gateway, logon default interface, and others. (See the *Installation and Getting Started Guide* for your switch.)
- **Logout:**

Closes the Menu interface and console session, and disconnects Telnet access to the switch.

Overview of the Menu Interface

The menu interface operates through the switch console to provide you with a subset of switch commands in an easy-to-use menu format.

- Performs a "quick configuration" of basic parameters, such as the IP addressing required to provide management access through your network
- Configures these features:
 - Manager and Operator passwords
 - System parameters
 - IP addressing
 - Time protocol
 - Ports
 - Trunk groups
 - A network monitoring port

- SNMP community names
- IP authorized managers
- VLANs (Virtual LANs) and GVRP
- View status, counters, and Event Log information
- Update switch software
- Reboot the switch

For a detailed list of menu features, see the **Main Menu features** on page 23.

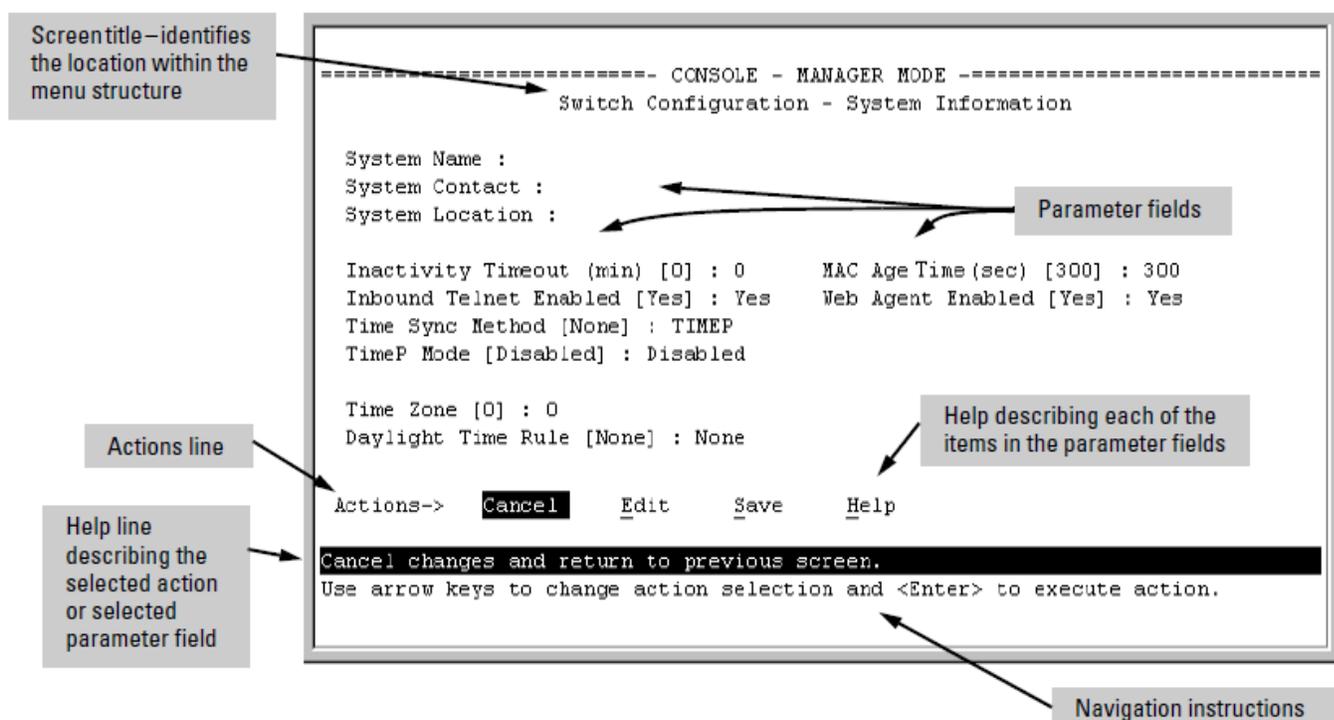
Screen structure and navigation

Menu interface screens include these three elements:

- Parameter fields and/or read-only information such as statistics
- Navigation and configuration actions, such as Save, Edit, and Cancel
- Help line to describe navigation options, individual parameters, and read-only data

For example, in the following System Information screen:

Figure 5: *Elements of the screen structure*



"Forms" design. The configuration screens, in particular, operate similarly to a number of PC applications that use forms for data entry. When you first enter these screens, you see the current configuration for the item you have selected. To change the configuration, the basic operation is to:

1. Press **[E]** to select the **Edit** action.
2. Navigate through the screen making all the necessary configuration changes.
3. Press **[Enter]** to return to the **Actions** line. From there, you can save the configuration changes or cancel the changes. Cancel returns the configuration to the values you saw when you first entered the screen.

Table 3: How to navigate the Menu interface

Task:	Actions:
Execute an action from the "Actions →" list at the bottom of the screen:	
Reconfigure (edit) a parameter setting or a field:	<ol style="list-style-type: none"> 1. Select a configuration item, such as System Name. 2. Press [E](for Edit on the Actions line). 3. Use [[Tab]] or the arrow keys ([←], [→], [↑], or [↓]) to highlight the item or field. 4. Do one of the following: <ul style="list-style-type: none"> • If the parameter has preconfigured values, either use the Space bar to select a new option or enter the first part of your selection and the rest of the selection appears automatically. (The help line instructs you to "Select" a value.) • If there are no preconfigured values, type in a value (the Help line instructs you to "Enter" a value). 5. If you want to change another parameter value, return to step 3. 6. If you are finished editing parameters in the displayed screen, press [Enter] to return to the Actions line and do one of the following: <ul style="list-style-type: none"> • To save and activate configuration changes, press [S] (for the Save action). This saves the changes in the startup configuration and also implements the change in the currently running configuration. (See, "Switch Memory and Configuration".) • To exit from the screen without saving any changes that you have made (or if no changes are done), press [C] (for the Cancel action). <p>Note: In the menu interface, executing Save activates most parameter changes and saves them in the startup configuration (or flash) memory, and it is therefore not necessary to reboot the switch after making these changes. But, if an asterisk appears next to any menu item you reconfigure, the switch will not activate or save the change for that item until you reboot the switch. In this case, rebooting must be done after you have made all desired changes and then returned to the Main Menu.</p> 7. When you finish editing parameters, return to the Main Menu. 8. If necessary, reboot the switch by highlighting Reboot Switch in the Main Menu and pressing [Enter]. (See the Note in Step 6.)
Exit from a read-only screen.	Press [B] (for the Back action).

To get Help on individual parameter descriptions. In most screens, there is a **Help** option in the **Actions** line. Whenever any of the items in the **Actions** line are highlighted, press **[H]**, and a separate help screen is displayed.

To get Help on the actions or data fields in each screen: Use the arrow keys ([←], [→], [↑], or [↓]) to select an action or data field. The help line under the **Actions** items describes the currently selected action or data field.

For guidance on how to navigate in a screen: See the instructions provided at the bottom of the screen, or See [Screen structure and navigation](#) on page 25.)

Privilege levels and password security

Hewlett Packard Enterprise strongly recommends that you configure a Manager password to help prevent unauthorized access to your network. A Manager password grants full read/write access to the switch. An Operator password grants access to status and counter, Event Log, and the Operator level in the CLI. After you configure passwords on the switch and log off of the interface, access to the menu interface (and the CLI and web browser interface) requires entries of either the Manager or Operator password.



- If the switch does not have Manager or an Operator password, anyone having access to the console interface can operate the console with full manager privileges.
- If you configure only an Operator password, entering the Operator password enables full manager privileges.
- If the switch only has a Manager password someone without a password can still gain read-only access.

For more information on passwords, see the *Access Security Guide* for your switch.

Menu interaction with other interfaces

The menu interface displays the current running-config parameter settings. From the running config, use the menu interface to save configuration changes made in the CLI. A configuration change made through any switch interface overwrites earlier changes made through any other interface.

The Menu Interface and the CLI both use the switch console. Use the `menu` command to enter the menu from the CLI and the **CLI** option from the menu interface to enter the CLI.

For more on how switch memory manages configuration changes, see the **Switch Memory and Configuration**.

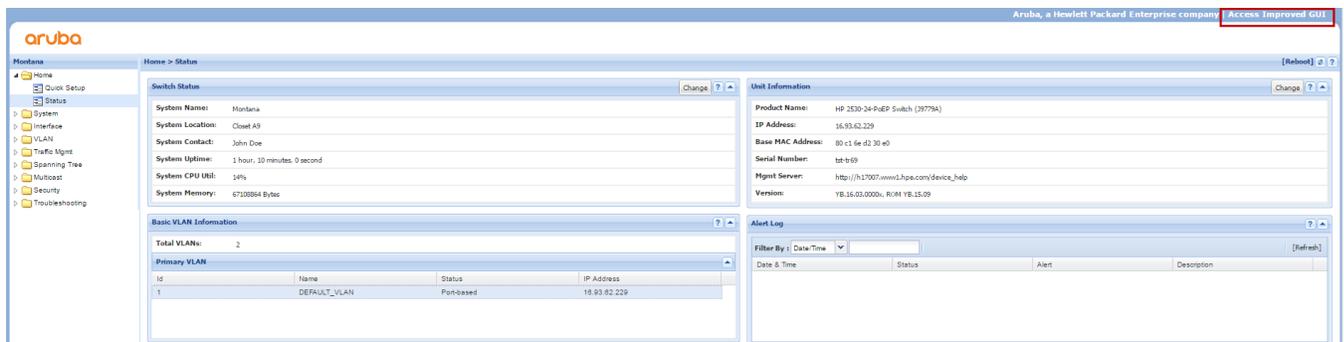
Management and configuration of ArubaOS-Switch can occur through its web interface. Two interfaces are available, the Legacy UI and the Next Generation UI.

- The **Legacy UI** provides full functionality for the monitoring and configuration of switches running ArubaOS.
- The **Next Generation UI** provides a subset of the Legacy UI functionality. Additional functionality will be added in future releases and it will eventually replace the Legacy UI.

Accessing the ArubaOS-Switch Next Generation UI

Access the ArubaOS-Switch Improved UI by clicking the **Access Improved GUI** link displayed in the upper right corner of the Traditional UI.

Figure 6: Traditional UI



Using HTTPS secure connection

ArubaOS-Switch devices can be configured and monitored using a web browser based HTTP interface, which is enabled by default. However, this connection method is unencrypted, thus making it vulnerable to credential interception by devices connected to the network in the path between the user and the switch being configured. To secure connections to the web management UI, it is recommended to enable HTTPS and disable HTTP access to the switch. HTTPS is HTTP traffic running on a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) connection, which requires a certificate to be present on the switch. To generate a certificate; enable HTTPS, and disable HTTP, the steps are as follows:

Procedure

1. Open a switch console session and enter the configuration context using the command:

```
switch# configure
```

2. Create a self-signed SSL/TLS certificate.

```
switch(config)# crypto pki enroll-self-signed certificate-name <name of certificate> subject common-name <common name of device>
```

- a. View the SSL/TLS certificate information.

```
switch(config)# show crypto pki local-certificate web-mgmt
Certificate Detail:
Version: 3 (0x2)
```

```

Serial Number:
 56:12:69:dd:3d:91:c1:8a:4e:2c:f4:62:a3:0a:96:76:b5:f0:b4:31
Signature Algorithm: sha256withRSAEncryption
Issuer: CN=5400R
Validity
  Not Before: Aug 14 13:33:32 2017 GMT
  Not After : Aug 14 23:59:59 2018 GMT
Subject: CN=5400R
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      30:0d:06:09:2a:86:48:86:f7:0d:01:01:01:05:00:
      03:81:8d:00:30:81:89:02:81:81:00:b0:90:f9:d8:
      88:f0:d5:eb:31:1e:aa:06:3b:30:5a:5b:d2:ed:eb:
      ff:12:ff:9d:52:55:98:cd:2a:c2:72:8e:94:69:47:
      a3:29:0f:f7:47:c3:c9:57:fa:11:d8:9a:8d:2f:e4:
      84:5e:3d:67:b2:fc:59:81:53:83:12:6a:68:6b:a5:
      4d:20:8f:b5:be:a2:23:b9:aa:e5:9a:55:ac:4a:fb:
      20:4b:71:6d:74:db:ab:89:4f:ed:27:c0:aa:31:fa:
      4b:64:76:be:f8:11:de:0e:5e:1e:17:b2:ba:a2:13:
      ce:2e:aa:31:d6:51:ad:e5:ed:23:93:42:27:d2:44:
      bd:2f:83:9d:02:03:01:00:01
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment, Key Agreement
  X509v3 Extended Key Usage:
    TLS Web Server Authentication

Signature Algorithm: sha256withRSAEncryption
 5c:00:9e:b2:8a:98:49:f3:e5:11:51:a8:2b:23:07:0c:f8:e8:
 26:bf:09:98:8a:9a:45:22:57:5b:af:ab:2f:ed:34:50:4d:ac:
 d9:59:18:e1:52:68:7f:20:ae:14:e7:d9:97:1b:91:5f:ae:ba:
 cd:b5:d3:7b:14:b6:da:99:fa:4f:2b:ed:65:96:59:fc:87:45:
 1c:49:93:2b:8c:47:3e:08:ae:7f:85:c3:31:58:17:32:d5:13:
 60:a3:c1:d2:4c:69:d5:54:7e:3d:e2:67:64:ba:38:6e:cb:c5:
 9e:17:9e:0b:30:52:8f:47:5d:59:2b:0e:c3:14:07:8f:f0:71:
 97:9d
MD5 Fingerprint: cbdc 5288 60e1 9576 4fd8 1f1d cae7 4edc
SHA1 Fingerprint: 6ea3 7708 a6dd cd6d 065b 1b34 1734 f385 42d6 0121

```

3. Enable HTTPS web management.

```
switch(config)# web-management ssl
```

4. (Recommended) Disable HTTP web management.

```
switch(config)# no web-management
```

5. Verify the web-management configuration.

```
switch(config)# show web-management
```

```
Web Management - Server Configuration
```

```

HTTP Access      : Disabled
HTTPS Access     : Enabled
SSL Port        : 443

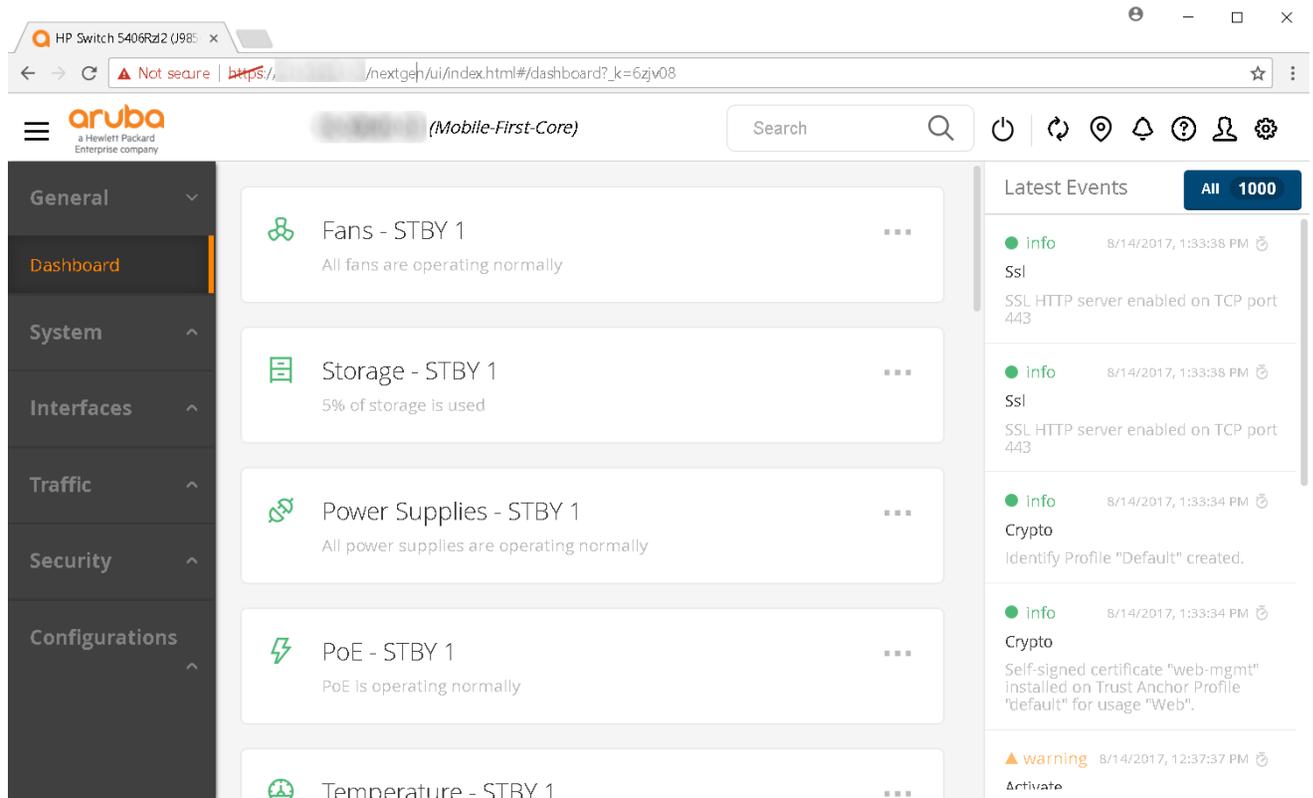
```

```
Idle Timeout      : 600 seconds
Management URL    : http://h17007.www1.hpe.com/device_help
Support URL       : http://www.arubanetworks.com/products/networking/
User Interface    : Improved
Listen Mode       : bot
```

- To log into the web management UI, open a browser and enter an IP address configured on the switch .

For example, `https://X.X.X.X`

IP addresses are configured on the switch by the VLAN. Use `show ip` command to view the configured IP addresses.



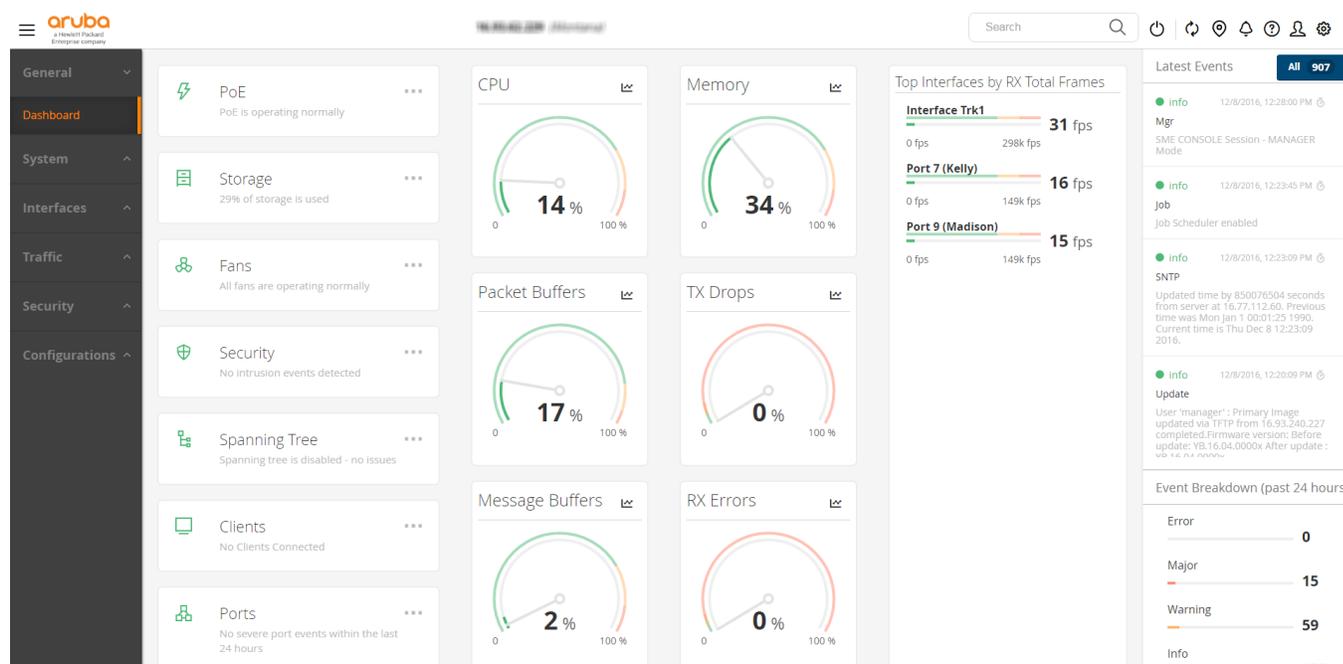
For more information about SSL/TLS configuration, see the *ArubaOS-Switch Access Security Guide* of your switch.

Improved UI functionality

Overview

The Improved UI includes four major elements that are common across all views within the UI. The dashboard view, which provides an at-a-glance overview of system performance, is displayed here as an example. All four elements are described below the dashboard image.

Figure 7: Improved UI dashboard



Header panel

This is the panel in the upper right corner of the screen. It includes the following icons and fields, from left to right:

- **Search:** Enter a search term in this field and press **Enter** to view results.
- **Reboot:** Click this icon to reboot the switch. You will be asked to confirm before the switch is rebooted.
- **Refresh:** Click this icon to reload the components and refresh the page.
- **Toggle locator LED:** Click this icon to identify a physical device.
- **Notifications:** Click this icon to see a list of recent events.
- **Help:** Click this icon to see the help text associated with the current screen.
- **User details:** Click this icon to see a list of user roles. You can also launch the Traditional user interface by clicking **Launch Traditional GUI**.
- **Settings:** Click this icon to modify the web interface settings for the current screen.

Navigation pane

This is the gray bar on the left side of the screen. It contains a series of drop-down menus, each representing an area of functionality, that allow you to navigate through the Improved UI. The drop-down menus include:

- **General:** Includes the Dashboard submenu.
- **System:** Includes the Status, Events, Monitor, SNMP, Firmware Update, and Stack (supported only for BPS/VSF) submenus.
- **Interfaces:** Includes the Ports, PoE, Monitor, VLANs, and Trunks submenus.
- **Traffic:** Includes the Spanning Tree submenu.

- **Security:** Includes the Clients, User Roles, Intrusion Log, Port Security, and IP Authorization submenus.
- **Configurations:** Includes the Config Report and Management submenus.

View pane

The view pane is a series of viewing options to the right of the navigation pane. It is broken into two sections:

Status panels - These panels display the status of the following elements.



Click on the ... icon in each status panel to navigate to the detailed view associated with the selected panel. For example, if you click on ... in the PoE view option, you will jump to the PoE page.

- **PoE:** Displays PoE port status.
 - Green: No PoE ports have a fault or have been denied power.
 - Yellow: One or more PoE ports have been denied power.
 - Red: One or more PoE ports have a fault.
- **Storage:** Displays system storage status.
 - Green: The current system storage use is within normal range.
 - Yellow: The current system storage use exceeds the warning threshold of 70%.
 - Red: The current system storage use exceeds the critical threshold of 90%.
- **Fans:** Displays system fan status.
 - Green: All fans are operating normally.
 - Yellow: One or more fans have failed but the number of failures does not exceed 50% of all system fans.
 - Red: At least 50% of the system fans have failed.
- **Security:** Displays security status based on the Intrusion Log flags.
 - Green: No intrusion events have occurred since acknowledgement.
 - Yellow: This status has no warning state.
 - Red: At least one new intrusion event has occurred.
- **Spanning Tree:** Displays spanning tree status.
 - Green: Spanning tree is disabled or no loop/root inconsistent ports were detected.
 - Yellow: Either loop or root inconsistent ports were detected.
 - Red: Both loop and root inconsistent ports were detected.
- **Clients:** Displays the summarized status of clients connected to the switch.
 - Green: All switch clients successfully authenticated/No Clients Connected.
 - Yellow: At least one client is not properly authenticated.
 - Red: Client authentication attempts were rejected.
- **Ports:** Displays ports with warning or critical events.
 - Green: Only info/debug events occurred on device ports.
 - Yellow: Warning events have occurred on one or more ports.
 - Red: Error/major events have occurred on one or more ports.
- **Power Supplies:** Displays system power supply status.
 - Green: All power supplies are operating normally.
 - Yellow: One or more power supplies have failed but the number of failures does not exceed 40% of all system power supplies.
 - Red: At least 40% of the system power supplies have failed.
- **Temperatures:** Displays system temperature status.

- Green: The current system temperature is within normal range.
- Yellow: The current system temperature exceeds the warning threshold of <variable>. The threshold is based on a user-controlled setting on the switch.
- Red: The current system temperature exceeds the critical threshold of <variable>. The threshold is based on a user-controlled setting on the switch.
- **Uptime:** Displays the device system uptime.

Gauges - These gauges display information about:

- **CPU:** Displays the current CPU usage of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest CPU usage reached for the device.
 - Green: CPU usage is within normal range.
 - Yellow: CPU usage exceeds the warning threshold of 75%.
 - Red: CPU usage exceeds the critical threshold of 90%.
- **Memory:** Displays the current memory usage of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest memory usage reached for the device.
 - Green: Memory usage is within normal range.
 - Yellow: Memory usage exceeds the warning threshold of 75%.
 - Red: Memory usage exceeds the critical threshold of 90%.
- **Packet Buffers:** Displays the current packet buffer usage of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest packet buffer usage reached for the device.
 - Green: Packet buffer usage is within normal range.
 - Yellow: Packet buffer usage exceeds the warning threshold of 85%.
 - Red: Packet buffer usage exceeds the critical threshold of 95%.
- **Tx Drops:** Displays the current transmit drop rate of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest transmit drop rate reached for the device.
 - Green: Transmit drop rate is within normal range.
 - Yellow: Transmit drop rate exceeds the warning threshold of 3% of transmit attempts.
 - Red: Transmit drop rate exceeds the critical threshold of 5% of transmit attempts.
- **Message Buffers:** Displays the current message buffer usage of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest message buffer usage reached for the device.
 - Green: Message buffer usage is within normal range.
 - Yellow: Message buffer usage exceeds the warning threshold of 75%.
 - Red: Message buffer usage exceeds the critical threshold of 90%.
- **Rx Errors:** Displays the current receive error rate of the device.
 - The outer ring of the gauge indicates regions of normal, warning, and critical values.
 - The peak value shown on the inner ring indicates the highest receive error rate reached for the device.
 - Green: Receive error rate is within normal range.
 - Yellow: Receive error rate exceeds the warning threshold of 2% of received frames.
 - Red: Receive error rate exceeds the critical threshold of 5% of received frames.
- **Top Interfaces:** Displays the top ten ports with any one of 25 user-selected metrics (RX Total Frames in this example). Only ports that are enabled and up will be shown.

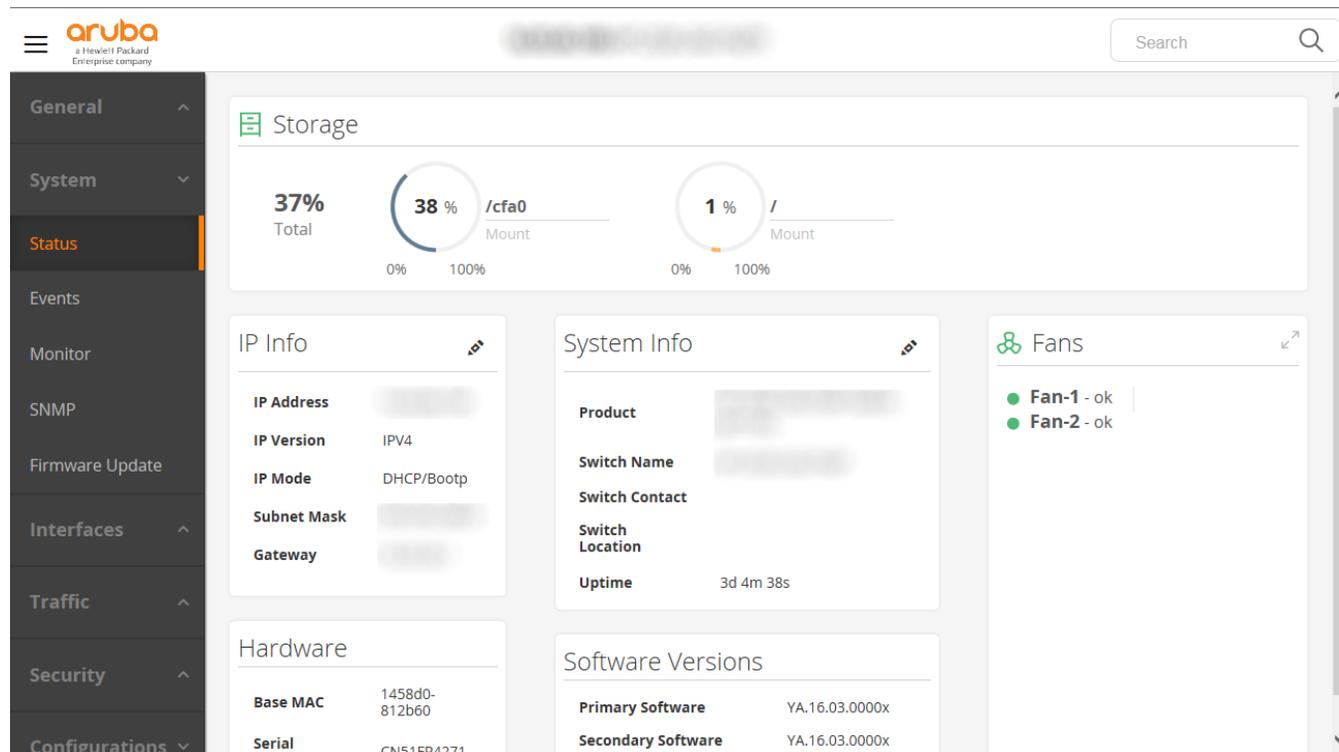
Right pane

Also called the events pane, this section displays:

- The latest events on the system
- User settings per page
- User roles across the system
- Help information

System — Status

Figure 8: System–Status



IP Info: Displays the basic IP configuration of the default VLAN. It is also possible to specify an IP configuration mode and associated settings.

Hardware: Displays basic hardware information for the device or stack commander. The MAC address and serial number of the device or stack commander are shown.

System Info: Displays general system information including:

- Product name
- Configured values for the device name
- Contact
- Location
- Uptime since the device was last rebooted

For a stack, this information pertains to the stack commander. It is also possible to edit the values for device name, contact, and location.

Software Versions: Displays the primary software, secondary software, and ROM versions for the device or, for a stack, the stack commander. In a stack, the commander's active software version is propagated to all stack members.

Storage: Displays system storage details for the device or, for a stack, summary data for each stack member.

- For a standalone device, a breakout of storage use per volume is shown.
- For a stack member, clicking the icon in its summary will navigate to the Stack page for the member where its breakout data can be viewed.
- This panel can be swapped to the top of the page by clicking the icon in the top right corner.

Fans: Displays system fan details for the device or, for a stack, summary data for each stack member.

- For a standalone device, a breakout of fan details is shown.
- For a stack member, clicking the icon in its summary will navigate to the stack page where its breakout data may be viewed.
- This panel can be swapped to the top of the page by clicking the icon in the top right corner.

Power Supplies: Displays system power supply status regarding the presence of removable supplies and their status in a device. For a stack, summary data is displayed for each stack member.

- For a standalone device, a breakout of power supply details is shown.
- For a stack member, clicking the icon in its summary will navigate to the stack page where its breakout data may be viewed.
- This panel can be swapped to the top of the page by clicking the icon in the top right corner.

Temperature: Displays system thermal status for the device or, for a stack, summary data for each stack member.

- For a standalone device, a breakout of temperature details is shown.
- For a stack member, clicking the icon in its summary will navigate to the stack page where its breakout data may be viewed.
- This panel can be swapped to the top of the page by clicking the icon in the top right corner.

System — Events

Figure 9: System–Events

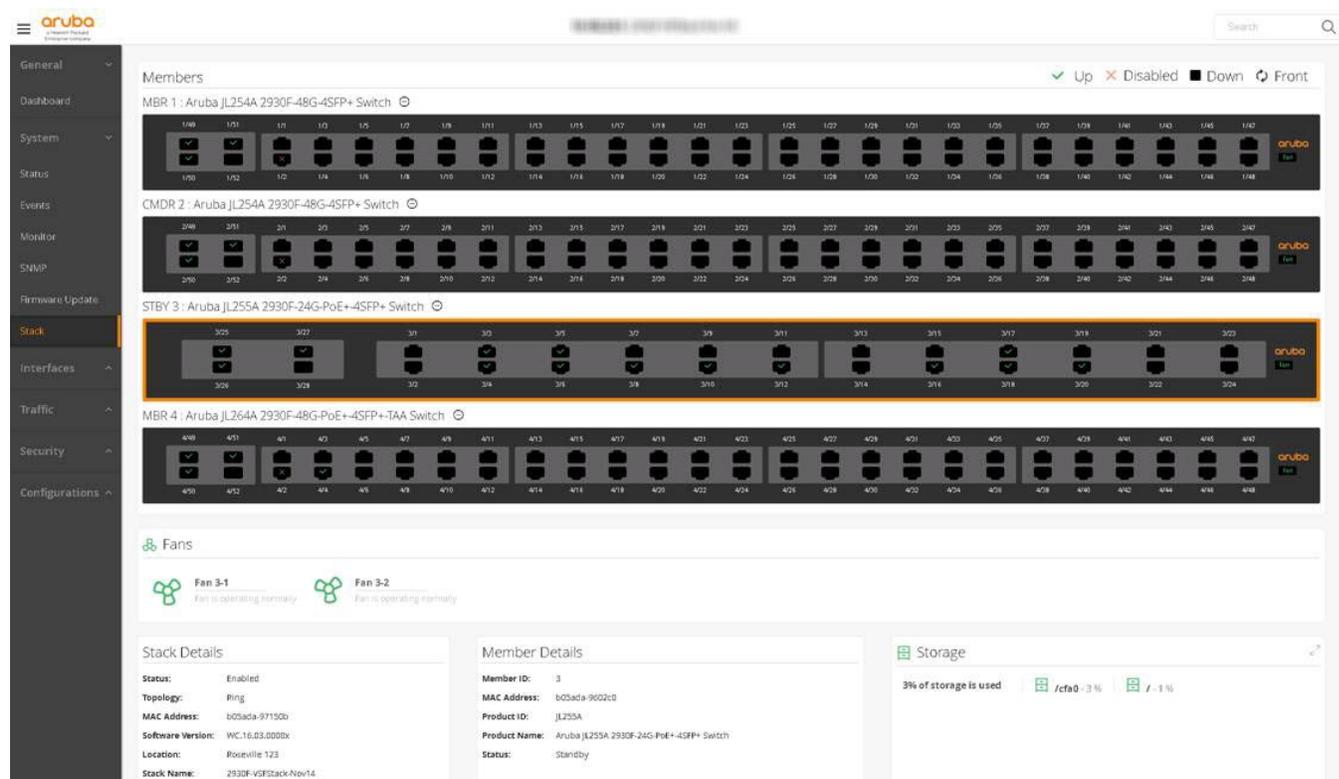
Severity	Time	Sub-System	Description
info	10/17/2016 09:29:47 ...	dhcp	DHCP server did not offer all the DNS parameters on Pri...
info	10/17/2016 09:29:47 ...	dhcp	updating IP address and subnet mask
info	10/17/2016 04:06:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:06:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:05:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:05:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:04:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:04:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:03:54 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:03:54 ...	mgr	SME TELNET from [redacted] - MANAGER Mode
info	10/17/2016 04:03:39 ...	mgr	SME TELNET from [redacted] - MANAGER Mode

Events List: Displays a list of the current system events. Available information includes event severity, time of occurrence, member information, and description.

Filter Events: The display dropdown and filter icon can be used to show/hide table columns and filter the results based on the user-specified options. Select either tool to begin filtering.

System — Stack

Figure 10: System–Stack



This view is only present on switch stacks.

Box Graphic: Displays each stack member physically.

- Used to view member information.
- The switch outlined in orange is the currently selected member.
- Data on the page reflects the selected member.
- The Box Graphic can be flipped to show either the front or back of the switch.

Fans: Displays member fan status.

Status:

- Green: The current system storage use is within normal range.
- Yellow: The current system storage use exceeds the warning threshold of 70%.
- Red: The current system storage use exceeds the critical threshold of 90%.

Storage: Displays system storage status.

Status:

- Green: All fans are operating normally.
- Yellow: One or more fans have failed but the number of failures does not exceed 50% of all system fans.
- Red: At least 50% of the system fans have failed.

Temperature: Displays system temperature status.

Status:

- Green: The current system temperature is within normal range.
- Yellow: The current system temperature exceeds the warning threshold of <variable>. The threshold is based on a user-controlled setting on the switch.
- Red: The current system temperature exceeds the critical threshold of <variable>. The threshold is based on a user-controlled setting on the switch.

Power Supplies: Displays system power supply status.

Status:

- Green: All power supplies are operating normally.
- Yellow: One or more power supplies have failed but the number of failures does not exceed 40% of all system power supplies.
- Red: At least 40% of the system power supplies have failed.

Stack Details: Displays system information regarding the stack including stack topology/configuration and software version on all members.

Member Details: Displays status, MAC address, location and stack name.

CPU: Displays the current CPU usage of the selected stack member.

- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest CPU usage reached for the device.

Status:

- Green: CPU usage is within normal range.
- Yellow: CPU usage exceeds the warning threshold of 75%.
- Red: CPU usage exceeds the critical threshold of 90%.

Memory: Displays current memory usage of the selected stack member.

- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest memory usage reached for the device.

Status:

- Green: Memory usage is within normal range.
- Yellow: Memory usage exceeds the warning threshold of 75%.
- Red: Memory usage exceeds the critical threshold of 90%.

Packet Buffers: Displays current packet buffer usage.

- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest packet buffer usage reached for the device.

Status:

- Green: Packet buffer usage is within normal range.
- Yellow: Packet buffer usage exceeds the warning threshold of 85%.
- Red: Packet buffer usage exceeds the critical threshold of 95%.

Tx Drops: Displays current transmit drop rate.

- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest transmit drop rate reached for the device.

Status:

- Green: Transmit drop rate is within normal range.
- Yellow: Transmit drop rate exceeds the warning threshold of 3% of transmit attempts.
- Red: Transmit drop rate exceeds the critical threshold of 5% of transmit attempts.

Message Buffers: Displays current message buffer usage.

- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest message buffer usage reached for the device.

Status:

- Green: Message buffer usage is within normal range.
- Yellow: Message buffer usage exceeds the warning threshold of 75%.
- Red: Message buffer usage exceeds the critical threshold of 90%.

Rx Errors: Displays the current receive error rate.

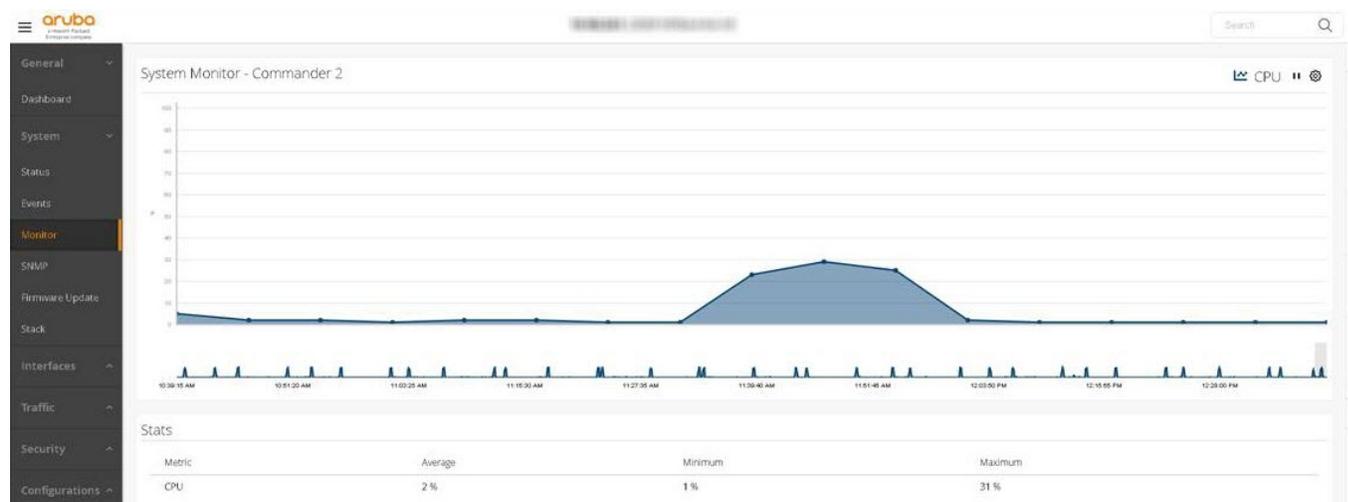
- The outer ring of the gauge indicates regions of normal, warning, and critical values.
- The peak value shown on the inner ring indicates the highest receive error rate reached for the device.

Status:

- Green: Receive error rate is within normal range.
- Yellow: Receive error rate exceeds the warning threshold of 2% of received frames.
- Red: Receive error rate exceeds the critical threshold of 5% of received frames.

System — Monitor

Figure 11: System–Monitor



Monitors up to six system metrics at a given time.

- Metrics include:
 - CPU usage
 - Memory usage
 - Packet buffer usage
 - Transmit drop rate
 - Message buffer usage
 - Receive error rate
- Metrics can be hidden from the graph by selecting the corresponding graph icon in the toolbar at the top of the graph.
- Select and slide the minimap (the gray box at the bottom of the graph) to zoom in and out of the graph. You can also focus in on a specific portion of the graph.
- Zooming in will provide a finer granularity of displayed data points, while zooming out will display fewer data points.

Pause and Play Graph: Use the pause and play icons in the toolbar in the upper right corner of the graph to start and stop the display of data points on the current graph.

- Pausing the graph will not pause the collection of system monitor data.
- Upon restarting the graph, the data points collected while the graph was paused will be filled in.

Graph options: Select the Graph Settings icon in the upper right corner of the graph to:

- View system monitor graph options
- Select metrics to graph
- Show/hide system alerts
- Show/hide summary lines (maximum, minimum, and average)

The **Metrics Statistics:** Displays statistics for each of the currently graphed metrics. Statistics include average, maximum, and minimum values for the metric.

System – SNMP

Figure 12: System–SNMP

Trap receivers: Displays all the trap receivers configured.

- Each card represents a trap receiver configured.
- To add a trap receiver, click the Add Trap Receiver (+) icon on the left side of the black panel.
- To edit a trap receiver, select the Edit Trap Receiver icon on the receiver card.
- To delete a trap receiver, select the Delete Trap Receiver icon on the receiver card.
- The interface offers different sorting options, which can be viewed by hovering over the sort icons. Select one to apply the sort. Select the arrow next to the sort icons to switch between ascending and descending sorting.
- Different sorting options are available, which can be viewed by hovering over the sort icons. Select one to apply the sort.
- Select the arrow next to the sort icons to switch between ascending and descending sort order.

IP Configuration: Displays the IP Configuration for the Trap Source and Trap Response. To edit either the Trap Source or Trap Response, select the Edit Configuration icon in the upper right corner of the IP Configuration panel.

Community Names: Displays a list of all community names. To add a community name, select the Add Community Name icon (+) in the upper right corner of the Community Names panel.

Community Info: Select a community name in the table to display it in the Community Info tile.

- To edit the community name, select the Edit Community Name icon in the upper right corner of the Community Info tile.
- To delete a community name, select the Delete Community Name icon in the upper right corner of the Community Info tile.

General Traps: Displays the traps supported and indicates whether each is enabled or disabled. To enable or disable a trap:

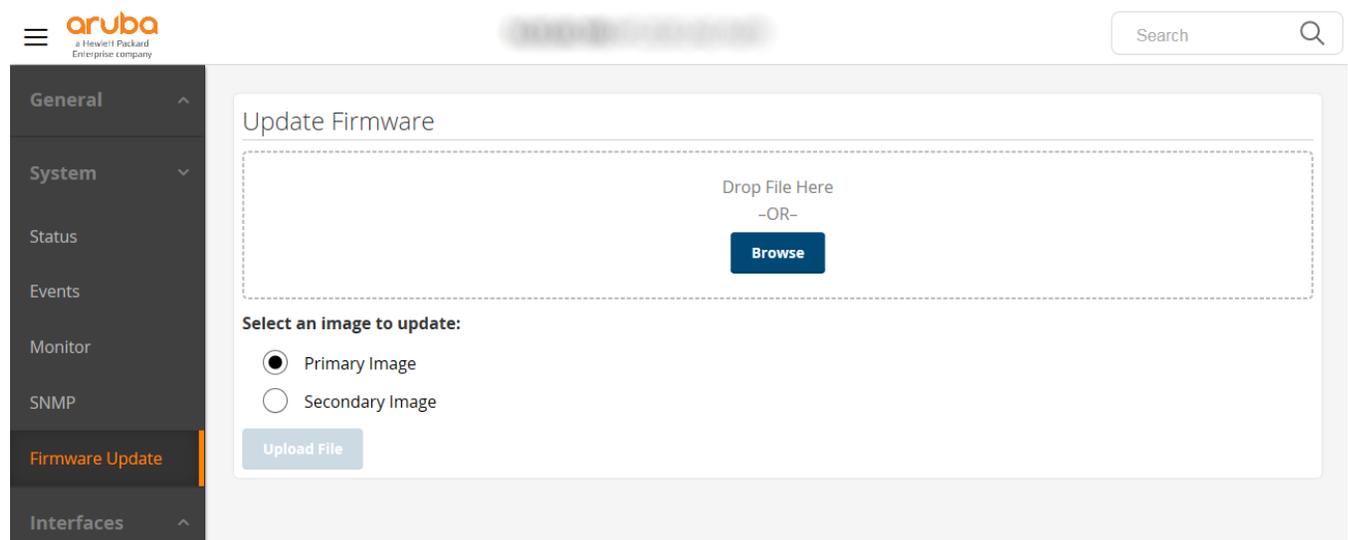
1. Select the Edit General Traps icon in the upper right corner of the General Traps tile.
2. Check or clear the box to the right of the trap to enable or disable that trap.
3. Click Save or Cancel.

Link Status Change Trap: Select the Expand icon on the left of the panel to view a table of ports and their link status change trap configurations.

- Use the page controls at the bottom of the table to navigate all the ports.
- If the Expand icon was previously selected, select the Collapse icon at the upper left of the panel to hide the table.
- To edit the link status change trap configuration for a port, select the Edit Link Status Change Trap icon in the upper right corner of the panel.

System – Firmware Update

Figure 13: System–Firmware Update



This functionality updates the device firmware with a file from the local system where the browser is being used.

1. Select which image to update: primary or secondary.
2. Drag and drop a file onto the indicated area or click **Choose File** to browse for a file.
3. Click **Upload File** to initiate the upload.

Interfaces — Ports

Figure 14: Interfaces–Ports

The screenshot displays the ArubaOS-Switch web interface. On the left is a dark sidebar with navigation menus: General, System, Interfaces, Ports (highlighted), PoE, Monitor, VLANs, Trunks, Traffic, Security, and Configurations. The main content area is titled 'Ports' and features a search bar at the top right. Below the search bar is a 'Status' section with a legend: a green checkmark for 'Up', a red 'X' for 'Disabled', and a black square for 'Down'. This is followed by a 'Box View' showing a grid of 28 port icons arranged in two rows of 14. Port 5 in the first row has a green checkmark, while others are black. Below this is the 'Port 1 Stats' section, which displays various performance metrics for port 1. At the bottom is the 'Ports' table, which lists port details.

Name	Custom...	Enabled	Status	Type	Config M...	Mode	Flow Con...	Trunk	Neighbor...
1		Yes	Down	100/1000T	Auto	1000FDx	Disabled		
2		Yes	Down	100/1000T	Auto	1000FDx	Disabled		

Port List: Displays a list of all physical ports on the device. Use the pagination control at the bottom of the table to page through the port list.

Box View: Visual representation of the physical view of the device including hardware status and ports.

- Active and disabled ports display the corresponding status indicator inside the port image.
- If a back of the box view is available, the option to view the back of the box displays in the toolbar at the top of the page.

Filter Port Table: The display dropdown and filter icon can be used to show/hide table columns and filter the table results based on the user-specified options. Select either tool to begin filtering.

Port Configuration: Configure a port by selecting the Edit Ports icon in the upper right corner of the toolbar at the top of the table. The configuration panel opens to allow for port selection and option configuration.

Interfaces — PoE

Figure 15: Interfaces–PoE

The screenshot displays the ArubaOS-Switch web interface for PoE management. The left sidebar contains navigation menus for General, System, Status, Events, Monitor, SNMP, Firmware Update, Stack, Interfaces, Ports, PoE, VLANs, Trunks, Traffic, Spanning Tree, Security, and Configurations. The main content area shows PoE Status for four switches in a stack: MBR 1 (Aruba JL254A 2930F-48G-4SFP+ Switch), CMDR 2 (Aruba JL254A 2930F-48G-4SFP+ Switch), STBY 3 (Aruba JL255A 2930F-24G-PoE+-4SFP+ Switch), and MBR 4 (Aruba JL264A 2930F-48G-PoE+-4SFP+TAA Switch). Each switch view includes a grid of port status indicators and a table of power usage. The bottom panel shows detailed configuration for Port 3/1, including PoE Power, PLC Class/Type, Allocate By Config, Allocate By Actual, LLDP Information, and PoE Slot Information.

This view displays the PoE information for the switch. In a stack, the power information will not be displayed for non-PoE switches.

- The box view and port table data is updated every 30 seconds.
- The detail view is updated every 3 seconds.

PoE Port List: Displays a list of all PoE physical ports on the device. Non-PoE ports are not shown. Use the pagination control at the bottom of the table to page through the port list.

PoE Box View: Visual representation of the physical view of the device including hardware status and ports. Active and disabled ports display the corresponding status indicator inside the port image.

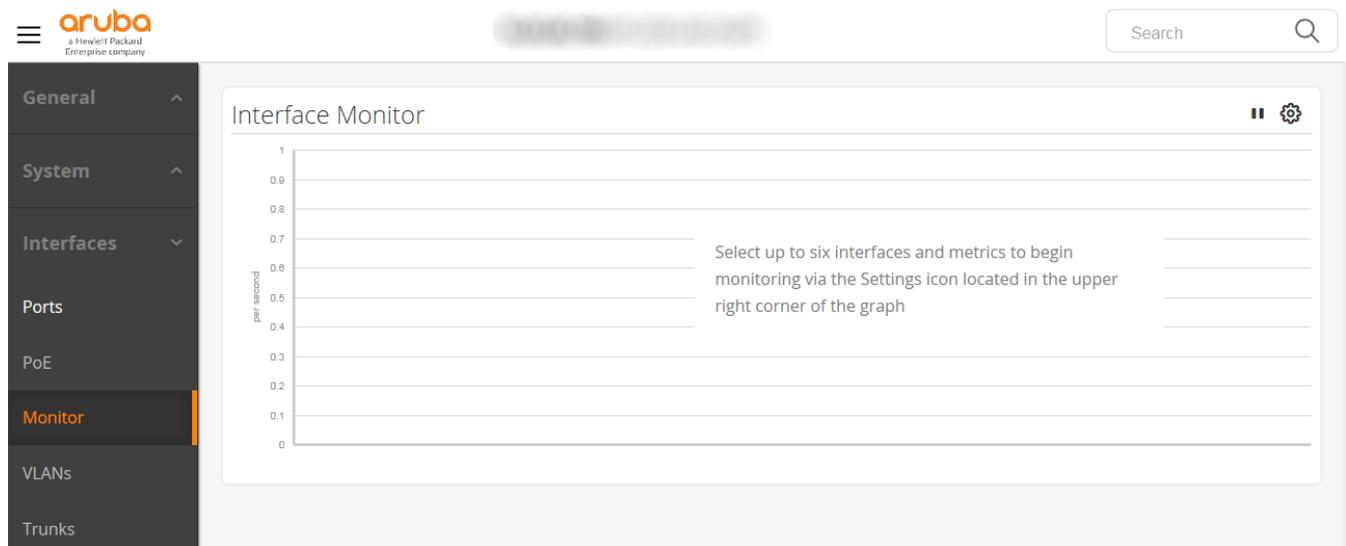
PoE Port Details: The PoE Port Details panel provides detailed information on the configuration, power usage, and statistics of a selected port. A port can be selected using the Box View or the port table.

Filter PoE Port Table: The display dropdown and filter icon can be used to show/hide table columns and filter the table results based on the user-specified options. Select either tool to begin filtering.

PoE Port Configuration: Configure a port by selecting the Edit Ports icon in the upper right corner of the toolbar at the top of the table. The configuration panel opens to allow for port selection and option configuration. By default, the selected port will be edited.

Interfaces — Monitor

Figure 16: Interfaces–Monitor



Interface Monitor Graph: Monitors up to six interface metrics at a given time.

- There are approximately two dozen metrics to choose from on any interface; all except utilization are expressed as per-second rates (for example, frames/second).
- Metrics may be monitored on a single interface or across multiple interfaces. The total number monitored at any juncture is limited to six or fewer.
- Only interfaces that are enabled and up may be selected.
- Metrics can be hidden from the graph by selecting the corresponding graph icon in the toolbar at the top of the graph.
- Metric collection is started anew each time this view is entered.

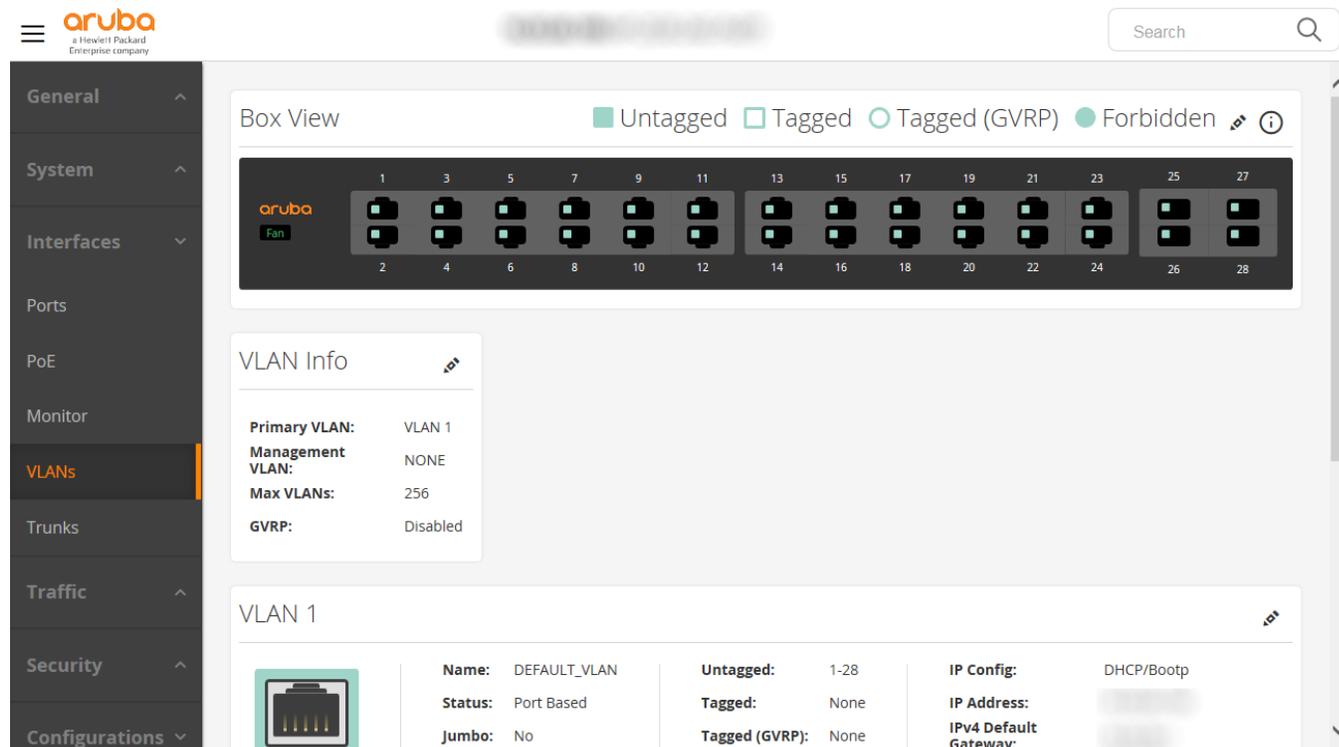
Pause and Play Graph: Use the pause and play icons in the upper right corner of the graph to start and stop the display of data points on the graph.

- Pausing the graph will not pause the collection of interface monitor data.
- Upon restarting the graph, the data points collected while the graph was paused will be filled in.

Graph Options: Select the Graph Settings icon in the upper right corner of the graph to select interfaces and metrics to graph data for.

Interfaces — VLANs

Figure 17: Interfaces–VLANs



VLAN Box View: Indicates which ports are members of the selected VLAN. Color and shape indicators are used to differentiate between port types and membership. Editing port membership can also be done through the box view.

Device VLAN Info: Displays the general VLAN information pertaining to the device.

VLAN Details: Displays a range of details regarding the selected VLAN. Select a VLAN by clicking it in the table.

All VLANs: Displays all configured VLANs on the device including information regarding each of the configured VLANs. This information includes:

- Status
- IP information
- Port membership

Select a VLAN in the table to view more information.

Edit General VLAN Info: Configure VLAN properties on the device. Configuration options include:

- Setting the primary and management VLAN
- Enabling or disabling GVRP
- Setting the maximum number of VLANs

Edit VLAN: Edit the properties and port membership of an existing VLAN.

Create VLAN: Create a VLAN.

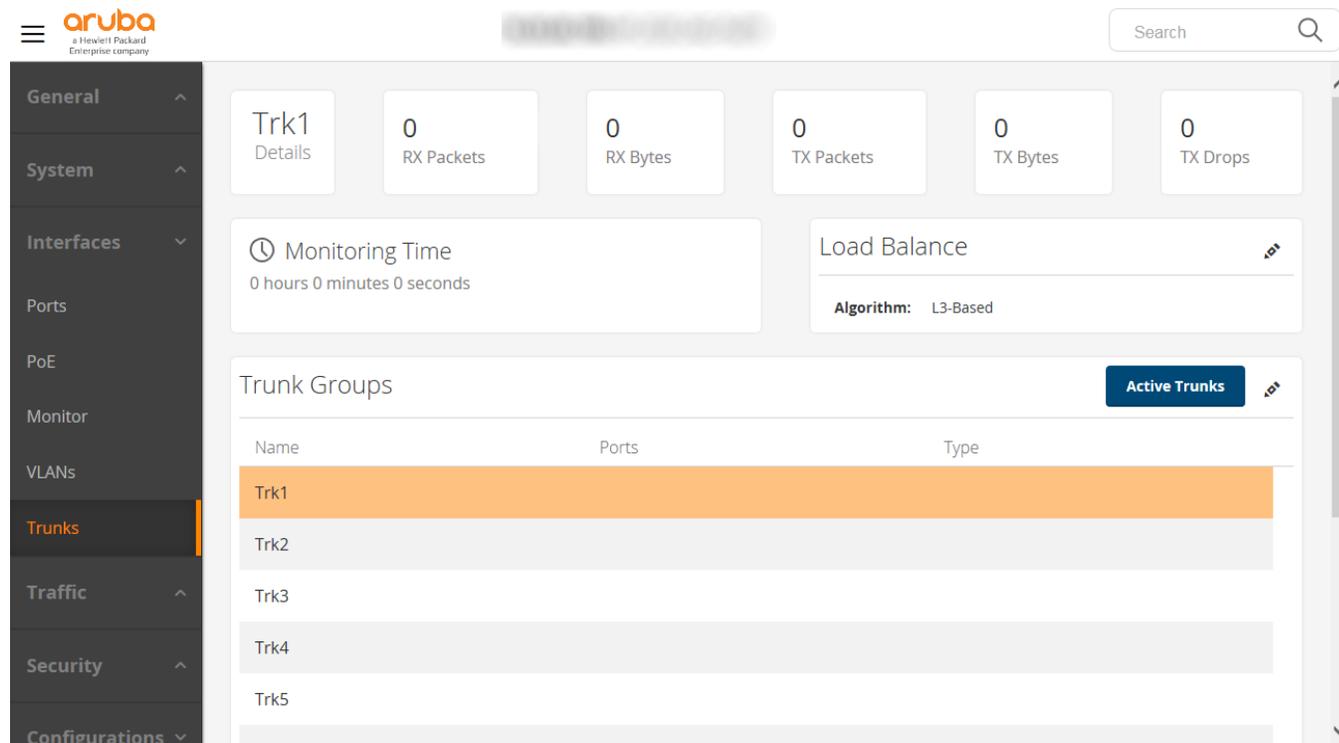
Delete VLAN: Delete an existing VLAN.

Edit VLAN via Box View: Select Ports in the box view to add or remove that port from the currently selected VLAN. Use the dropdown option in the header to change the port type.

Magnify Box View: Magnify the box view to display up to six VLANs in a single port to view VLAN membership. Double-click in the magnifier to cycle to the next VLAN if more than six are present. Press the Esc key to exit the magnifier.

Interfaces — Trunks

Figure 18: Interfaces–Trunks



Trunk Table: Displays a list of active trunks on the device or the configured trunk groups.

- Active trunks are trunk groups that have ports assigned to them.
- Toggle between the active trunks and trunk groups by using the labeled button in the upper right corner of the table.

Trunk Details: Displays details about a selected trunk. Select a trunk in the table to see its details.

Load Balancing: Displays the current load balancing algorithm configured on the switch.

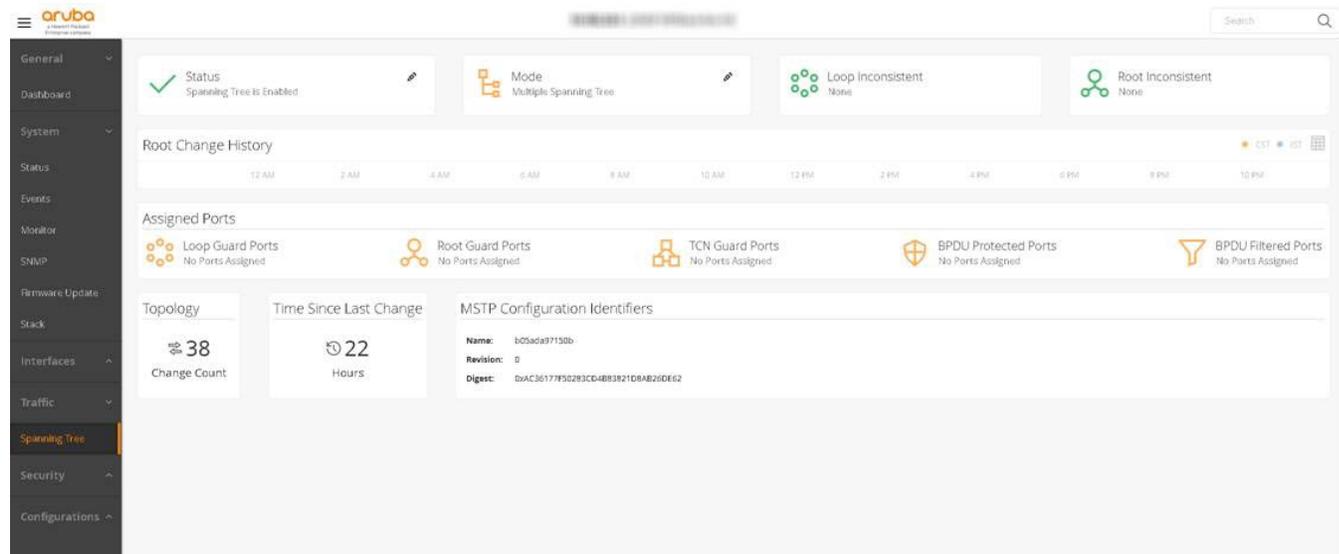
- L2 - Uses the best MAC Source Address (MAC-SA) and MAC Destination Address (MAC-DA) information to load balance traffic.
- L3 - Uses the best IP Source Address (IPSA) and IP Destination Address (IPDA) method to load balance IP traffic, and MAC Source Address (MAC-SA) and MAC Destination Address (MAC-DA) to load balance non-IP traffic.
- L4 - Uses the best L4 information (if present) or L3 information for IP traffic, or MAC Source Address (MAC-SA) and MAC Destination Address (MAC-DA) for non-IP traffic.

Edit Load Balancing: Edit the configured load balancing algorithm on the device.

Edit Trunks: Configure trunks on this device.

Traffic — Spanning Tree

Figure 19: Traffic–Spanning Tree



Spanning Tree Status: Displays whether spanning tree is enabled or disabled on the device.

Spanning Tree Mode: Displays the current spanning tree mode on the device:

- MSTP (Multiple Spanning Tree)
- RPVST (Rapid Per-VLAN Spanning Tree)

Loop Inconsistent Ports: Displays the list of loop inconsistent ports on the device detected by Loop Guard.

Root Inconsistent Ports: Displays the list of root inconsistent ports on the device detected by Root Guard.

Root Change History: Displays the last 10 root change events on the device.

- By default, a scatter plot chart will be shown representing the data on an hourly basis broken out per day.
- Use the icon in the upper right corner of this component to view the data in a standard table format.

Assigned Ports: Displays the ports assigned to a variety of spanning tree port types that are configurable through the CLI. Types include:

- Loop Guard
- Root Guard
- TCN Guard
- BPDU Protected Ports
- BPDU Filtered ports

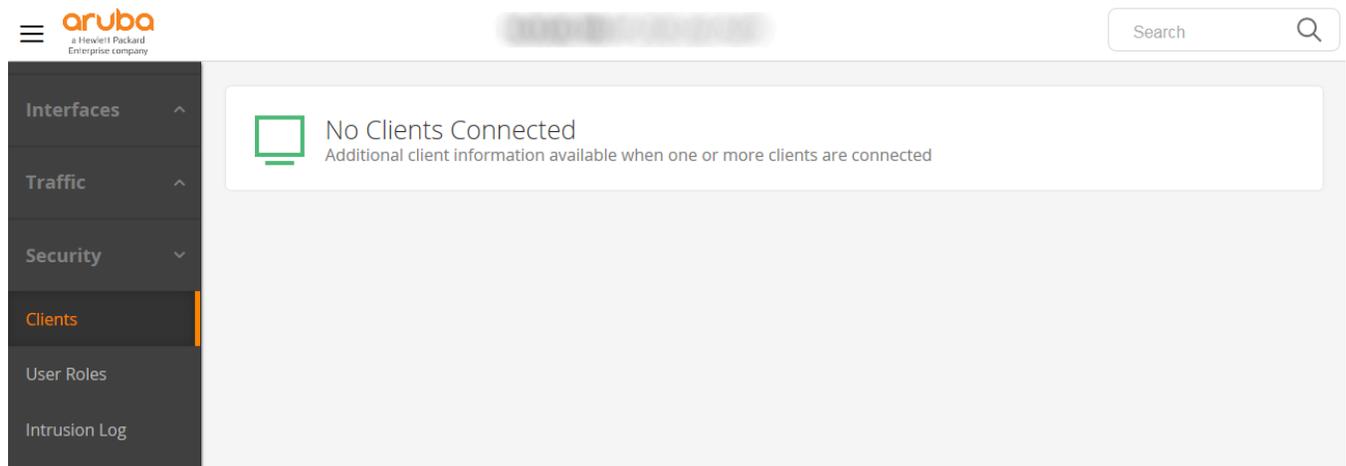
Topology Change Count: Displays the current topology change count on the device.

Time Since Last Change: Displays the time since that last topology change detected on the device.

MSTP Details: Displays the MSTP configuration identifiers on the device including the name, revision, and digest.

Security — Clients

Figure 20: Security–Clients



Authentication Type Graph: Displays a graph that summarizes the use of authentication types used for client authorization. Displays statistics like most used and least used authentication types.

User Role Graph: Displays a graph that summarizes the use of user roles associated with the connected clients.

Client Status Summary: Displays the total number of clients connected to the switch. Also displays client status summary.

Client Details: Displays client-specific information such as:

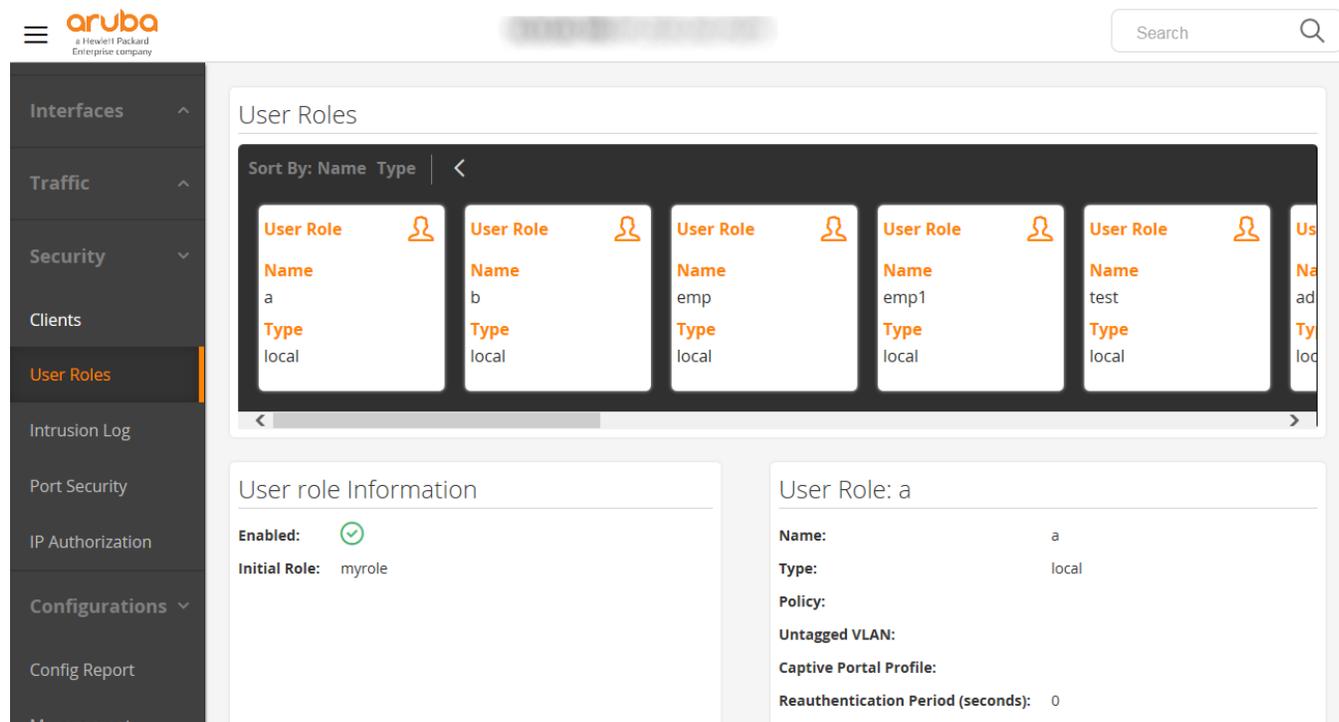
- Physical port ID
- MAC address
- IP address
- Untagged and tagged VLANs
- User role session time

Connected Clients: Displays a list of all clients connected to the switch. Use the pagination controls at the bottom of the page to move through the client list.

Filter Clients Table: The display dropdown and filter icon can be used to show/hide table columns and filter the table results based on user-specified options. Select either tool to begin filtering.

Security — User Roles

Figure 21: Security–User Roles



User Roles: Displays all user roles configured on the switch.

- Each card represents a user role configured.
- User role cards are clickable.
- You can sort the role cards by name or type.
- Click **Apply** the sort.
- Click the arrow to switch between ascending and descending sort orders.

User Role Information: Indicates whether the user role is enabled or disabled. Also displays the initial user role configured on the switch.

User Role Card: Displays user role details such as:

- Name
- Type
- Policy
- VLAN
- Captive portal profile
- Reauthentication period

Security — Intrusion Log

Figure 22: Security–Intrusion Log

Intrusion Log: Displays a list of the 20 most recent violation attempts detected on the device regardless of whether the alert flags for these attempts have been reset.

Ports With Intrusion Flag: Displays a list of ports that have the intrusion flag set. The flag gets set when the device detects a violation attempt on the listed port.

Reset Intrusion Flags: Reset all intrusion flags using the **Reset Intrusion Flag** button located in the upper right corner of the log table.

Security — Port Security

Figure 23: Security–Port Security

ID	Name	Custom Name	Learn Mode	Address Limit	Violation Action
1	1		Continuous	1	None
2	2		Continuous	1	None
3	3		Continuous	1	Send Trap
4	4		Continuous	1	None

Port Security Table: Displays security properties for all ports on the device.

Properties include:

- Learn mode
- Address limit
- Violation action

Select a row in the table to see additional details about the port.

Learn Mode: Displays the selected ports learn mode.

Mode options include:

- Continuous
- Static
- Configured
- Port Access
- Limited

Additional information about what the assigned mode means can be seen following the mode type.

Authorized Address Limit: Displays the number of authorized addresses allowed on the port.

Authorized MAC Addresses: Displays the authorized MAC addresses allowed on the port.

Filter Port Table: Filter the port table by any of the available table columns.

Edit Port: Configure the port security properties on the selected port.

Security — IP Authorization

Figure 24: Security–IP Authorization

The screenshot shows the ArubaOS-Switch IP Authorization configuration page. The sidebar on the left contains navigation options: Interfaces, Traffic, Security, Clients, User Roles, Intrusion Log, Port Security, IP Authorization (selected), Configurations, and Config Report. The main content area displays 'IP Authorization Info' with fields for IP Address, Subnet Mask / Prefix Length, Access Method, and Access Level. Below this are three summary cards: 'Total Single Station Entries with Manager Access' (0), 'Total Multiple Station Entries with Manager Access' (0), and 'Total Single Station Entries with Operator Access' (0). A larger card shows 'Total Multiple Station Entries with Operator Access' (0). At the bottom, there is an 'IP Authorized Management' table with columns for IP Authorized Address, Subnet Mask / Prefix Length, Access Method, and Access Level. The table currently shows 'No records'.

IP Authorization Info: Displays the IP Authorization Info from the row selected in the IP Authorization Table. You can edit the entry by selecting the drawing icon in the top right corner. You can also delete the entry by selecting the garbage icon in the top right corner.

Total Single Station Entries with Manager Access: Displays the total number of entries in the IP Authorization Table that have Manager Access Level and only apply to one computer. This is essentially all entries with a subnet mask of 255.255.255.255 or 32 prefix length and have Manager Access Level.

Total Multiple Station Entries with Manager Access: Displays the total number of entries in the IP Authorization Table that have Manager Access Level and apply to multiple computers. This is essentially all entries with a subnet mask different from 255.255.255.255 or 32 prefix length and have Manager Access Level.

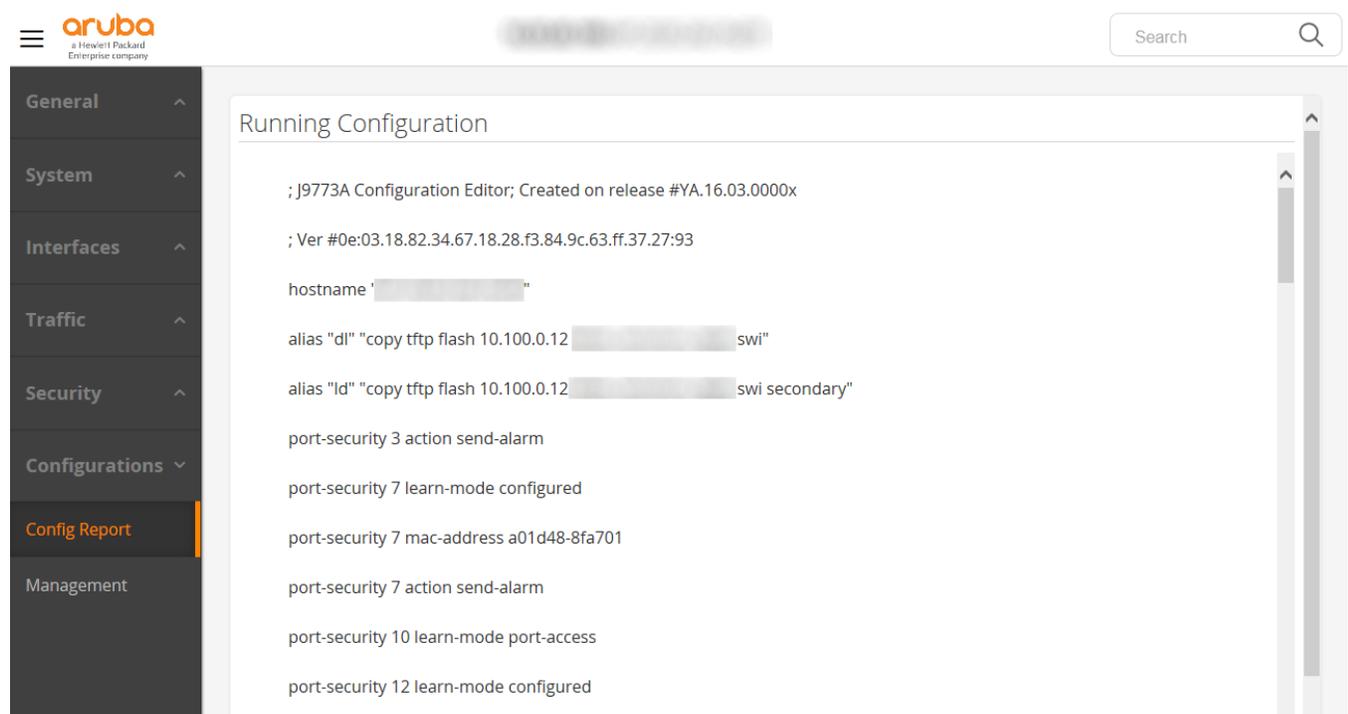
Total Single Station Entries with Operator Access: Displays the total number of entries in the IP Authorization Table that have Operator Access Level and only apply to one computer. This is essentially all entries with a subnet mask of 255.255.255.255 or 32 prefix length and have Operator Access Level.

Total Multiple Station Entries with Operator Access: Displays the total number of entries in the IP Authorization Table that have Operator Access Level and apply to multiple computers. This is essentially all entries with a subnet mask different from 255.255.255.255 or 32 prefix length and have Operator Access Level.

IP Authorized Management: Displays a table of all IP Authorized entries. You can add an entry by selecting the add icon in the top right corner. To edit or delete an entry, use the icons in the IP Authorization Info tile.

Configurations — Config Report

Figure 25: Configurations—Config Report



The screenshot shows the ArubaOS-Switch UI. On the left is a navigation menu with categories: General, System, Interfaces, Traffic, Security, Configurations (expanded), Config Report (selected), and Management. The main content area is titled "Running Configuration" and displays the output of the `show running-config` command. The configuration includes:

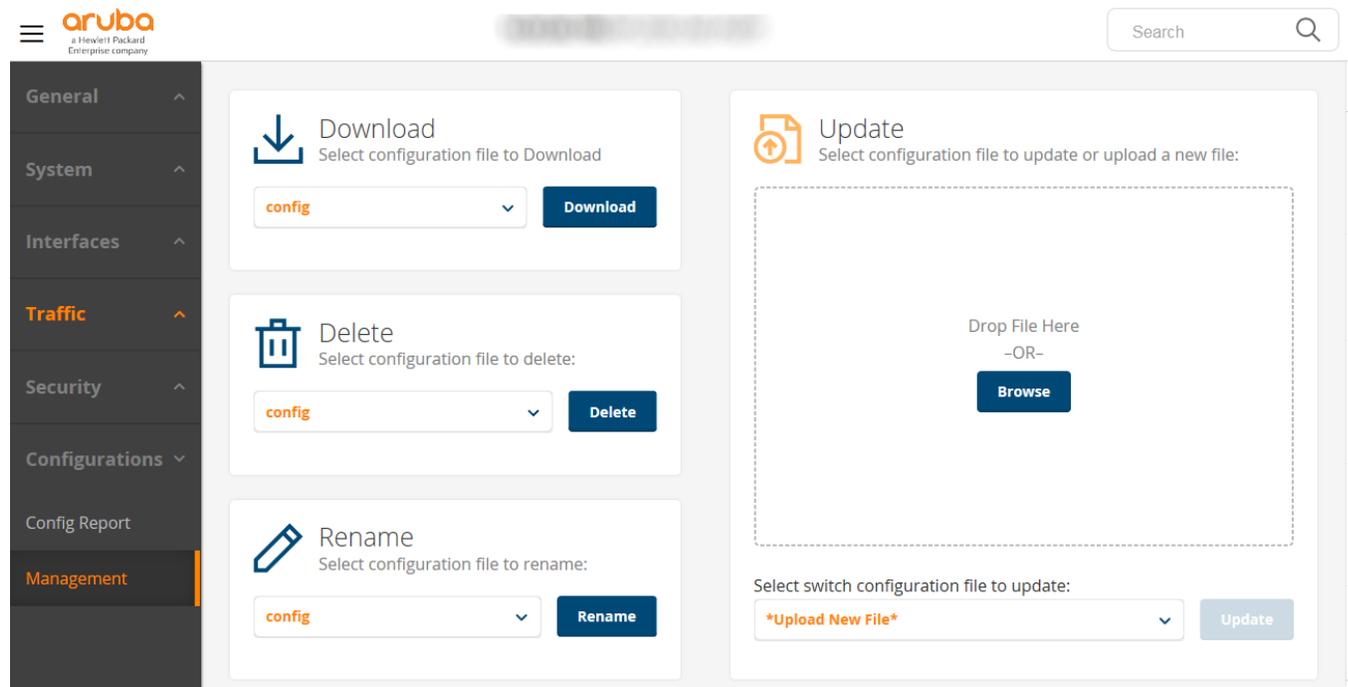
```
; J9773A Configuration Editor; Created on release #YA.16.03.0000x
; Ver #0e:03.18.82.34.67.18.28.f3.84.9c.63.ff.37.27:93
hostname ' '
alias "dl" "copy tftp flash 10.100.0.12 swi"
alias "ld" "copy tftp flash 10.100.0.12 swi secondary"
port-security 3 action send-alarm
port-security 7 learn-mode configured
port-security 7 mac-address a01d48-8fa701
port-security 7 action send-alarm
port-security 10 learn-mode port-access
port-security 12 learn-mode configured
```

Running Configuration: Displays the current running configuration as shown in the `show running-config` CLI command.

Expand and collapse nodes in the running configuration by selecting the + and - icons next to a node that has content underneath it.

Configurations — Management

Figure 26: Configurations–Management



Download: Downloads the selected configuration file from the device to the local system where the browser is being used.

Delete: Deletes the selected configuration file from the device. A confirmation window is displayed because after a file is deleted it cannot be recovered.

Rename: Renames the selected configuration file to a new name. A field is displayed in which the new name may be entered. When done, Click **Save** or **Cancel**.

Update: Updates an existing device configuration file or uploads a new configuration file from the local system where the browser is being used. A confirmation window is displayed because after the upload begins it cannot be aborted.

Procedure

1. Drag and drop a file onto the indicated area or click the button to browse for a file to be uploaded.
2. Specify which configuration file is to be updated (existing or new). If using a new file, the name of the file on the local system will be used.
3. Click **Update** to initiate the upload.
4. A confirmation window displays because after the upload begins, it cannot be aborted.

Overview of Preview Mode

Preview mode feature is available only when preview mode is enabled on a switch. The intent of having features in preview mode is to allow users to experiment the features and solicit early feedback from them.

Use the features in a preview mode at your own risk. When you enable preview mode on a switch, you are prompted before entering the preview mode. On confirmation, the `prev-mode` is prefixed with the switch configuration prompt.

For example:

```
(Prev-mode) switch(config)#
```



The existing configuration for a switch continues even after you enable preview mode.

When you exit the preview mode, you are prompted to reboot the switch. Rebooting the switch reverts the switch to a configuration that existed prior to enabling preview mode.

Supported Platforms

- Aruba 2930F
- Aruba 5400R
- Aruba 3810M

Enabling Preview Mode

Procedure

1. Use the CLI command to enable the preview mode on the switch.

Syntax

```
preview-mode
```

Description

Enter preview mode on the switch. You can now configure the features in preview mode. Exiting the preview mode reboots the switch to a configuration, that existed prior to enabling the preview mode.

Example output

```
switch(config)# preview-mode
ATTENTION: You are entering preview mode on this product. This mode, the
commands, features and functionality specific to this mode, and all output
from this mode are Hewlett Packard Enterprise Confidential and Proprietary.
You may use this mode at your own risk. Any defects or issues encountered
in this mode will be addressed per Hewlett Packard Enterprise's discretion.
```

```
Continue (y/n)? y
Prev-mode) switch(config) #
```

Viewing features in Preview Mode

Procedure

1. Use the CLI command to view the features in a preview mode.

Syntax

```
show preview-mode
```

Description

Displays the list of features in preview mode.

Parameters

```
features
```

Displays the features in a preview mode.

Example output

```
(Prev-mode) switch(config) # show preview-mode
features                               Show the features under preview mode.
(Prev-mode) switch(config) # show preview-mode features
Features in Preview Mode:
Multicast Offload Engine  Enable/Disable multicast offload engine for routed
                           multicast IPv4 traffic.
                           Usage:
                           fabric-offload multicast ipv4 route
```

Multicast Offload Engine

In the current release, enabling Multicast Offload Engine (MOE) to route multicast IPv4 traffic is the only feature supported on the switch in a preview mode.

Procurve switches without MOE enabled, use ingress replication to send multicast traffic to multiple destinations. The processes such as request, reply, or forward are repeated for every destination node chip. Thus, it results in sending the packet over the ingress node's fabric interface once for each destination node. To overcome this problem, MOE is enabled.

There is a significant improvement in the performance, as enabling MOE prevents sending multiple copies of the packet across the ingress node chip's fabric interface. When you enable MOE, the request or reply process to each destination node chip still occurs, but the packet is forwarded once to the fabric chip, and the fabric chip replicates the packet to all other destination nodes that has to receive the packet.



In the current release, MOE is enabled only to route multicast IPv4 packets.

As the feature is available for experiment purpose, it has the following limitations:

- You cannot use MOE with VSF.
- You cannot enable MOE on jumbo-enabled VLANs.

Supported Platform

Aruba 5400R v3 standalone

Enabling MOE

Procedure

1. Use the CLI command to enable MOE for IPv4 multicast traffic. The `running-config` file displays the MOE enabled for IPv4 traffic.

Syntax

```
fabric-offload multicast ipv4 route {enable|disable}
```

Description

Enable or disable multicast offload engine for routed multicast IPv4 traffic.

Usage

```
fabric-offload multicast ipv4 route {enable|disable}
```

Example output

```
(Prev-mode)switch# show running-config
```

Running configuration:

```
; J9851A Configuration Editor; Created on release #KB.16.01.0000x
; Ver #0a:19.f4.7b.ff.ff.fc.ff.ff.3f.ef:b0
hostname "HP-5412Rz12"
module A type j9992a
module L type j9987a
fabric-offload multicast ipv4 route enable
ip routing
ip multicast-routing
snmp-server community "public" unrestricted
oobm
ip address dhcp-bootp
exit
vlan 1
name "DEFAULT_VLAN"
untagged A1-A21,L1-L24
ip address dhcp-bootp
exit
no allow-v2-modules
preview-mode
```

Listing available commands

Procedure

1. Type `?` to list available commands. Typing the `?` symbol lists the commands you can execute at the current privilege level.
2. The commands that are available to a user depend on the user's privilege level. At a given privilege level, you can list and execute the commands that the privilege level offers, plus all commands available at preceding levels.
3. When `-- MORE --` appears, there are more commands in the listing. Do one of the following:
 - a. To list the next screen of commands, press the Space bar.
 - b. To list the remaining commands one-by-one, repeatedly press **[Enter]**.

The following example shows the result of typing `?` at the Operator level. You can list and execute only the Operator-level commands at the Operator level.

Figure 27: *The Operator-level command listing*

```
switch> ?
chassislocate      Control the chassis locate led.
dir                Display a list of the files and subdirectories in a
                  directory on a USB device.
display            Display current system information.
enable             Enter the Manager Exec context.
exit               Return to the previous context or terminate current
                  console/telnet session if you are in the Operator
                  context level.

link-test          Test the connection to a MAC address on the LAN.
logout             Terminate this console/telnet session.
menu               Change console user interface to menu system.
page              Toggle paging mode.
ping               Send IPv4 ping request(s) to a device on the network.
ping6              Send IPv6 ping request(s) to a device on the network.
quit               Exit from current command view
services           Display parameters for the services module.
show               Display switch operation information.
traceroute         Trace the IPv4 route to a device on the network.
traceroute6        Trace the IPv6 route to a device on the network.
verify             Verify the signature of a switch firmware image.
wireless-services  Display parameters for the wireless-services module.
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

The following example shows the result of typing `?` at the Manager level. At this level, you can list and execute commands that are available at both the Operator and Manager levels. Typing `?` at the Global Configuration level or the Context Configuration level produces similar results.

Figure 28: *The Manager-level command listing*

```
switch# ?
backup          Backup next startup-configuration file to TFTP server
boot           Reboot the device.
clear          Clear table/statistics.
clock          Display/set current time, date, and local time
               parameters.
command-alias  Specify command alias
configure      Enter the Configuration context.
copy           Copy datafiles to/from the switch.
debug          Enable/disable debug logging.
delete         Delete a file
diagnostic-level Set the diagnostic level.
end            Return to the Manager Exec context.
erase          Erase stored data files.
getMIB         Retrieve and display the value of the MIB objects
               specified.
getNextMIB     Retrieve and display the value of the next MIB object
               for each OID specified
kill           Kill other active console, Telnet, or SSH sessions.
licenses       Manage premium features.
log            Display log events.
print          Execute a command and redirect its output to the device
               channel for current session.
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

Listing command options

Procedure

1. Enter command keywords followed by `?` to display command options.

For example, suppose you want to see the command options for configuring the console settings:

```
switch(config)# console ?
baud-rate      Set the data transmission speed for the device connect
               sessions initiated through the Console port.
events         Set level of the events displayed in the device's Events
               Log.
flow-control   Set the Flow Control Method; default is xon-xoff.
idle-timeout   The number of seconds of no activity detected before the
               switch terminates a session.
inactivity-timer [Deprecated] Set the number of minutes of no activity
               detected before the switch terminates a communication
               session.
local-terminal Set type of terminal being used for the current console
               or Telnet session (default is vt100).
screen-refresh Set refresh time for menu status and counters in
               seconds.
```

```
terminal          Set type of terminal being used for all console and
                  Telnet sessions (default is vt100).
```

Displaying CLI “Help”

Do one of the following:

Procedure

1. Type “help” to display a list of commands that includes a brief summary of each command’s purpose. The list includes all commands available at the current privilege level. That is, at the Operator level, executing **help** displays the Help summaries only for Operator-Level commands. At the Manager level, executing **help** displays the Help summaries for both the Operator and Manager levels, and so on.
2. Type a command string followed by “help” to display detailed information about how to use an individual command. Use the following syntax:

```
<command-string> help
```

Help is displayed for any command that is available at the current privilege level. An “Invalid input” message is displayed if you try to list the help for an individual command from a privilege level that does not include that command.

The following example shows the result of typing “help” at the Operator privilege level. The Operator-Level commands are listed with their purposes.

Figure 29: *Help for Operator-Level commands*

```
switch> help

chassislocate      Control the chassis locate led.
dir                Display a list of the files and subdirectories in a
                  directory on a USB device.
display           Display current system information.
enable            Enter the Manager Exec context.
exit              Return to the previous context or terminate current
                  console/telnet session if you are in the Operator
                  context level.
link-test          Test the connection to a MAC address on the LAN.
logout            Terminate this console/telnet session.
```

The following example shows Help for the **interface** command at the Global Configuration privilege level:

Figure 30: *Detailed Help for a specific command*

```
switch(config)# interface help
Usage: no interface < [ethernet] PORT-LIST [...] | loopback <num> >

Description: Enter the Interface Configuration Level, or execute one
             command for that level. Without optional parameters
             specified, the 'interface' command changes the context to
             the Interface Configuration Context Level for execution of
             configuration changes to the port or ports in the PORT-LIST
             or with loopback keyword it will change context to loopback
             mode. Use 'interface ?' to get a list of all valid commands.
```

Note that trying to list the help for an individual command from a privilege level that does not include that command results in an error message. For example, trying to list the help for the **interface** command while at the global configuration level produces this result:

```
switch# speed-duplex help
Invalid input: speed-duplex
```

Enabling and disabling CLI message prefixes

When message prefixes are enabled, a CLI command returns a message that is prefixed with “Error”, “Warning”, or “Information” to indicate the type of message.

Procedure

1. Type “session show-message-type enable” to enable the display of prefixes with the returned message.
2. Type “session show-message-type disable” to disable the display of prefixes with the returned message.

The syntax is as follows:

```
session show-message-type [enable|disable]
```

The message prefixes setting is not saved when the switch is rebooted. The message prefixes are disabled on all CLI sessions by default.

The following example shows returned messages of each of the three message types.

Figure 31: Message prefixes

```
switch(config)# router rip
Error: IP Routing support must be enabled first.

switch(config)# qinq mixed vlan
Warning: This command will reboot the device. Any prior configuration
on this config file will be erased and the device will boot up with a
default configuration
for the new qinq mode.
Do you want to continue [y/n]? n

switch(config)# snmp-server mib hpSwitchAuthMIB included
Information: For security reasons, network administrators are
encouraged to disable SNMPv2 before using the MIB.
```

To determine if message labeling is enabled, enter the **show session** command.

Figure 32: The label cli-return-message command enabled

```
switch(config)# show session
show message type    : Enabled
cli interactive mode: Enabled
```

Enabling and disabling CLI interactive command mode

When the CLI interactive command mode is enabled, you must explicitly enter the choice of yes (‘y’) or no (‘n’) for interactive commands. When interactive command mode is disabled, you are not prompted to explicitly enter the choice of yes (‘y’) or no (‘n’) unless you are saving a configuration.

Procedure

1. Type “session interactive-mode enable” to enable the CLI interactive command mode.
2. Type “session interactive-mode disable” to disable the CLI interactive command mode.

The syntax is as follows:

```
session interactive-mode [enable|disable]
```

The interactive-mode setting is not saved when the switch is rebooted. The interactive mode is enabled on all CLI sessions by default.

The following example shows some commands used with the CLI interactive command mode disabled.

Figure 33: CLI interactive mode when disabled

```
switch(config)# no password all
Password protection for all will be deleted, continue [y/n]? y

switch(config)# boot system flash secondary
System will be rebooted from secondary image.
Do you want to continue [y/n]? y
Do you want to save current configuration [y/n]? n
```

To determine if the CLI interactive mode is enabled or disabled, enter the **show session** command.

Figure 34: CLI interactive mode enabled

```
switch(config)# show session
show message type      : Enabled
cli interactive mode: Enabled
```

Interactive commands requiring additional options

Interactive commands that require input other than yes or no are not affected when CLI interactive mode is disabled. A warning message is displayed when these commands are executed, for example:

```
Interactive mode is disabled; This command will be ignored.
Enable cli-interactive-mode to use this command.
```

The following commands will issue this warning when interactive mode is disabled. An alternate way to enter the command (when one is available) is shown.

Command	Non-Interactive Alternate Command
setup mgmt-interfaces	No equivalent non-interactive command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
password manager	password manager plaintext <password-string>
password operator	password operator plaintext <password-string>
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
crypto host-cert generate self-signed	crypto host-cert generate self-signed <start- date> <end-date> <CNAME-STR> <ORG-UNIT-STR> <ORGANIZATION-STR> <CITY-STR> <STATE-STR> <CODE>

Menu commands

When CLI interactive mode is disabled, all CLI commands that launch the menu interface are not affected by the interactive mode. A warning message is displayed, for example:

```
switch(config)# menu
Interactive mode is disabled; This command will be ignored.
Enable cli-interactive-mode to use this command.
```

Other menu-based commands that will not be affected are:

- setup
- show interfaces display

SNMPv3 special cases

The following are special cases when using SNMPv3 with interactive mode.

- **snmpv3 user:**

In interactive mode, the command **snmpv3 user** will create snmpv3 users, even if snmpv3 has not been enabled.

- **snmpv3 user:**

When interactive mode is disabled, this command only enables snmpv3. It does not prompt for an authentication password. When the command is first executed, a default initial user is created. A message displays:

```
User 'initial' has been created.
```

Simplifying entry of commands at the command line

Do one or more of the following to simplify entry of commands:

Procedure

1. To find or complete a command, use the **[TAB]** key.
See **Finding or completing a command** on page 61
2. To re-execute a command, use the `redo` command.
See **redo** on page 62
3. To repeatedly re-execute one or more commands, use the `repeat` command.
See **repeat** on page 63
4. To create a shortcut name for a command to simplify keystrokes, use the `alias` command.
See **alias** on page 64
5. To simplify movement or placement of your cursor at the command line, use the shortcut keystrokes. See **CLI shortcut keystrokes** on page 65

Finding or completing a command

Procedure

1. Type one or more consecutive characters of a command and then press **[Tab]** (with no spaces allowed) to find a CLI command or to quickly complete a CLI command name. The CLI completes the current command name, including hyphenated extensions, if you have typed enough characters for the CLI to distinguish it from other possibilities.
2. The following example shows the result when you press

[Tab] immediately after typing “t” at the Global Configuration level. The CLI displays the available command options that begin with “t”.

```
switch(config)# t
tacacs-server
telnet-server
tftp
time
timesync
trunk
trunk-load-balance
task-monitor
telnet
terminal
test
traceroute
traceroute6
```

3. The following example shows the result when you press

[Tab] immediately after typing “port-”.

```
switch (config)# port-
switch (config)# port-security
```

4. The following example shows the result of pressing

[Tab] after a completed command word lists the further options for that command. In this example, entering

```
switch(config)# qos [Tab]
```

displays the following:

```
switch (config)# qos
udp-port          Set UDP port-based priority.
tcp-port          Set TCP port-based priority.
device-priority   Configure device-based priority for a particular IP
                  address.
dscp-map          Define mapping between a DSCP (Differentiated-Services
                  Codepoint) value and an 802.1p priority.
protocol          Configure protocol-based priority.
queue-config      Configure the number of egress priority queues for each
                  port.
type-of-service   Configure the Type-of-Service method the device uses to
                  prioritize IP traffic.
watch-queue       Enables monitoring of per-queue dropped packets due to
                  outbound congestion on the given port.
```

redo

Syntax

```
redo [ <number> | <command-str> ]
```

Description

Parameters/Options/Flags/Strings/...

The `redo` command re-executes a command. The last command that was used is executed by default.

Specifiers

<number>

Specifies the position of the command in the history list. When the position is specified, the **nth** command starting from the most recent command in the history is executed.

<command-str>

Specifies the name of a previously executed command. The most recently executed command whose name matches the specified string is executed.

Example

This example shows the use of the `redo` command.

```
switch(config)# show history
2      show arp
1      show flash
```

```
switch(config)# redo 2
```

```
IP ARP table
```

IP Address	MAC Address	Type	Port
-----	-----	-----	----
15.255.128.1	00000c-07ac00	dynamic	A11

repeat

Syntax

```
repeat [cmdlist] [count] [delay]
```

Description

The `repeat` command repeatedly re-executes one or more commands. By default, the most recent command in the history is executed until a key is pressed.

Options

[cmdlist]

Specifies the position of a command, or range of positions of multiple commands, in the history list. The **nth** most recent commands in the history, where "n" is the position in the history list, are re-executed.

[count]

Specifies number of times to execute the command or commands.

[delay]

Specifies a delay. The execution of the command is delayed for the number of seconds specified.

Usage

```
switch(config)# repeat 1-4,7-8,10 count 2 delay 3
```

Example

This demonstrates the use of the `repeat` command to re-execute commands that are at positions 1 through 2 in the command history.

```
switch(config)# show history
3      show ver
2      show ip
1      show arp
```

```
switch(config)# repeat 1-2
```

IP ARP table

IP Address	MAC Address	Type	Port
15.255.128.1	000000-000000	dynamic	

Internet (IP) Service

IP Routing : Disabled

Default Gateway :
Default TTL : 64
Arp Age : 20
Domain Suffix :
DNS server :

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP
DEFAULT_VLAN	DHCP/Bootp	15.255.131.90	255.255.248.0	No No

alias

Syntax

```
alias <name> <command>  
no alias <name> <command>
```

Description

The `alias` command creates a shortcut alias name that can be used in place of a CLI command to simplify keystrokes and aid memory. The `alias` command is executed from the current configuration context.

Options

no

Specifies that the alias for the command is to be removed.

Specifiers

<name>

Specifies the alias for the CLI command. The alias name must not be an existing CLI command.

<command>

Specifies an existing CLI command for which to create the alias. The command must be enclosed in quotes.

It is recommended that you use an alias that does not have an existing tab completion in the CLI. For example, using an alias that starts with "show" or "int" would complete to "show" and "interface" respectively when you use the tab completion function.

Privilege

The `alias` command is executed from the current configuration context (operator, manager, or global). If the command that is aliased has to be executed in the global configuration context, you must execute the alias for that command in the global configuration context. This prevents bypassing the security for a particular context.

Restrictions

- The alias name must not be an existing CLI command. Existing CLI commands are searched before looking for an alias command; an alias that is identical to an existing command will not be executed.
- Hewlett Packard Enterprise recommends that you configure no more than 128 aliases.

Example

This example shows the creation and use of an alias for the `show int custom` command to demonstrate how a command alias can simplify keystrokes when entering a command. The actual `show int custom` command is used first and then an alias is created for it and then used.

```
switch(config)# show int custom 1-4 port name:4 type vlan intrusion speed
enabled mdi
```

Status and Counters - Custom Port Status

Port	Name	Type	VLAN	Intrusion			MDI-mode
				Alert	Speed	Enabled	
1	Acco	100/1000T	1	No	1000FDx	Yes	Auto
2	Huma	100/1000T	1	No	1000FDx	Yes	Auto
3	Deve	100/1000T	1	No	1000FDx	Yes	Auto
4	Lab1	100/1000T	1	No	1000FDx	Yes	Auto

```
switch(config)# alias sic "show int custom 1-4 port name:4 type vlan intrusion
speed enabled mdi"
switch(config)#
```

```
switch(config)# sic
```

Status and Counters - Custom Port Status

Port	Name	Type	VLAN	Intrusion			MDI-mode
				Alert	Speed	Enabled	
1	Acco	100/1000T	1	No	1000FDx	Yes	Auto
2	Huma	100/1000T	1	No	1000FDx	Yes	Auto
3	Deve	100/1000T	1	No	1000FDx	Yes	Auto
4	Lab1	100/1000T	1	No	1000FDx	Yes	Auto

CLI shortcut keystrokes

Keystrokes	Functions
[Ctrl] [A]	Jumps to the first character of the command line.
[Ctrl] [B] or '←'	Moves the cursor back one character.
[Ctrl] [C]	Terminates a task and displays the command prompt.
[Ctrl] [D]	Deletes the character at the cursor.
[Ctrl] [E]	Jumps to the end of the current command line.
[Ctrl] [F] or '→'	Moves the cursor forward one character.

Table Continued

Keystrokes	Functions
[Ctrl] [K]	Deletes from the cursor to the end of the command line.
[Ctrl] [L] or [Ctrl] [R]	Repeats current command line on a new line.
[Ctrl] [N] or '↓'	Enters the next command line in the history buffer.
[Ctrl] [P] or '↑'	Enters the previous command line in the history buffer.
[Ctrl] [U] or [Ctrl] [X]	Deletes from the cursor to the beginning of the command line.
[Ctrl] [W]	Deletes the last word typed.
[Esc] [B]	Moves the cursor backward one word.
[Esc] [D]	Deletes from the cursor to the end of the word.
[Esc] [F]	Moves the cursor forward one word.
[Backspace]	Deletes the first character to the left of the cursor in the command line.
[Spacebar]	Moves the cursor forward one character.

Overview of the CLI

The CLI is a text-based command interface for configuring and monitoring the switch. The CLI gives you access to the switch's full set of commands while providing the same password protection that is used in the web browser interface (WebAgent) and the menu interface.

Access

Like the menu interface, the CLI is accessed through the switch console, and in the switch's factory default state, is the default interface when you start a console session. You can access the console out-of-band by directly connecting a terminal device to the switch, or in-band by using Telnet either from a terminal device or through the WebAgent.

Also, if you are using the menu interface, you can access the CLI by selecting the **Command Line (CLI)** option in the Main Menu.

Privilege levels

The CLI offers these privilege levels to help protect the switch from unauthorized access:

1. Operator
2. Manager
3. Global Configuration
4. Context Configuration



CLI commands are not case-sensitive.

When you use the CLI to make a configuration change, the switch writes the change to the Running-Config file in volatile memory. This allows you to test your configuration changes before making them permanent. To make changes permanent, you must use the **write memory** command to save them to the Startup-Config file in non-volatile memory. If you reboot the switch without first using **write memory**, all changes made since the last reboot or **write memory** (whichever is later) will be lost.

More information

Configuring the switch on page 74.

Privilege levels for CLI access

Privilege levels at log on

Privilege levels control the type of access to the CLI. To implement this control, you must set at least a Manager password. **Without a Manager password configured, anyone having serial port, Telnet, or web browser access to the switch can reach all CLI levels.** (For more on setting passwords, See the usernames and passwords in the *Access Security Guide* for your switch.)

When you use the CLI to log on to the switch, and passwords are set, you will be prompted to enter a password. For example:

CLI log-on screen with password(s) set

```
switch
Software revision K.15.12.0001
```

```
Copyright (C) 1991-2013 Hewlett-Packard Development Company, L.P.
```

RESTRICTED RIGHTS LEGEND

```
Confidential computer software. Valid license from HP 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.
```

```
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.
20555 State Highway 249, Houston, TX 77070
```

```
We'd like to keep you up to date about:
```

- * Software feature updates
- * New product announcements
- * Special events

```
Please register your products now at: www.hp.com/networking/register
```

```
Username:
```

In the above case, you will enter the CLI at the level corresponding to the password you provide (operator or manager).

If no passwords are set when you log on to the CLI, you will enter at the Manager level. For example:

```
switch# _
```



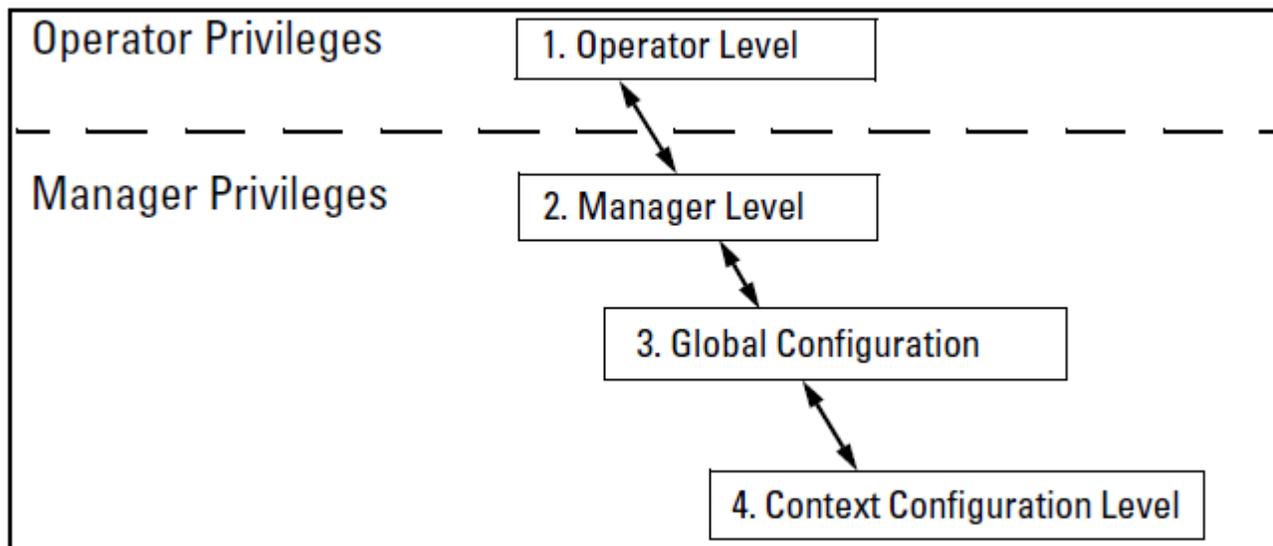
Hewlett Packard Enterprise strongly recommends that you configure a Manager password. If a Manager password is not configured, then the Manager level is not password-protected, and anyone having in-band or out-of-band access to the switch may be able to reach the Manager level and compromise switch and network security. Note that configuring only an Operator password **does not** prevent access to the Manager level by intruders who have the Operator password.

Pressing the Clear button on the front of the switch removes password protection. **For this reason, it is recommended that you protect the switch from physical access by unauthorized persons.** If you are concerned about switch security and operation, you must install the switch in a secure location, such as a locked wiring closet.

Privilege level operation

The access sequence for the various privilege levels is shown in **Figure 35: Access sequence for privilege levels** on page 68.

Figure 35: Access sequence for privilege levels



You can move between the privilege levels. The following table lists examples and results of movement between the privilege levels.

Change in Levels	Example of Prompt, Command, and Result	
Operator level to Manager level	<pre>switch> enable Password:_ switch#_</pre>	After you enter enable , the Password prompt appears. After you enter the Manager password, the system prompt appears with the # symbol:
Manager level to Global configuration level	<pre>switch# config switch(config)#</pre>	
Global configuration level to a Context configuration level	<pre>switch(config)# vlan 10 switch(vlan-10)#</pre>	
Context configuration level to another Context configuration level	<pre>switch(vlan-10)# interface e 3 switch(int-3)#</pre>	The CLI accepts "e" as the abbreviated form of "ethernet".

Table Continued

Change in Levels	Example of Prompt, Command, and Result	
Move from any level to the preceding level	<pre>switch(int-3)# exit switch(config)# exit switch# exit switch></pre>	
Move from any level to the Manager level	<pre>switch(int-3)# end switch# -or- switch(config)# end switch#</pre>	

Moving between the CLI and the Menu interface. When moving between interfaces, the switch retains the current privilege level (Manager or Operator). That is, if you are at the Operator level in the menu and select the **Command Line Interface (CLI)** option from the Main Menu, the CLI prompt appears at the Operator level.

Changing parameter settings. Regardless of which interface is used (CLI, menu interface, or WebAgent), the most recently configured version of a parameter setting overrides any earlier settings for that parameter. For example, if you use the menu interface to configure an IP address of "X" for VLAN 1 and later use the CLI to configure a different IP address of "Y" for VLAN 1, then "Y" replaces "X" as the IP address for VLAN 1 in the running-config file. If you subsequently execute `write memory` in the CLI, then the switch also stores "Y" as the IP address for VLAN 1 in the startup-config file. (For more on the startup-config and running config files, see "Switch Memory and Configuration".)

Operator privileges

At the Operator level, you can examine the current configuration and move between interfaces without being able to change the configuration. A ">" character delimits the Operator-level prompt. For example:

```
switch>_
```

(Example of the Operator prompt.)

When using `enable` to move to the Manager level, the switch prompts you for the Manager password if one has already been configured.

Manager privileges

Manager privileges give you three additional levels of access: Manager, Global Configuration, and Context Configuration. A "#" character delimits any Manager prompt. For example:

```
switch#_
```

(Example of the Manager prompt.)

- **Manager level:**

Provides all Operator level privileges plus the ability to perform system-level actions that do not require saving changes to the system configuration file. The prompt for the Manager level contains only the system name and the "#" delimiter, as shown above. To select this level, enter the **enable** command at the Operator prompt and enter the Manager password, when prompted. For example:

```
switch> enable
Password:
switch# _
```

Enter enable at the Operator prompt. CLI prompt for the Manager password. The Manager prompt appears after the correct Manager password is entered.

- **Global configuration level:**

Provides all Operator and Manager level privileges, and enables you to make configuration changes to any of the switch's software features. The prompt for the Global Configuration level includes the system name and "(config)". To select this level, enter the **config** command at the Manager prompt. For example:

```
switch# config
switch(config)# _
```

Enter config at the Manager prompt. The Global Config prompt.

- **Context configuration level:**

Provides all Operator and Manager privileges, and enables you to make configuration changes in a specific context, such as one or more ports or a VLAN. The prompt for the Context Configuration level includes the system name and the selected context. For example:

```
switch(eth-1)#
switch(vlan-10)#
```

The Context level is useful, for example, for executing several commands directed at the same port or VLAN, or if you want to shorten the command strings for a specific context area. To select this level, enter the specific context at the Global Configuration level prompt. For example, to select the context level for an existing VLAN with the VLAN ID of 10, you would enter the following command and see the indicated result:

```
switch(config)# vlan 10
switch(vlan-10)#
```

Table 4: Privilege level hierarchy — Operator Privilege

Privilege Level	Example of Prompt and Permitted Operations		
Operator Level	switch>	show <command> setup	View status and configuration information.
		ping <argument> link-test <argument>	Perform connectivity tests.
		enable	Move from the CLI interface to the menu interface.  NOTE Use enable at the Operator level to move to the Manager level.
		menu	Move from the CLI interface to the menu interface.

Table Continued

Privilege Level	Example of Prompt and Permitted Operations	
	logout	Exit from the CLI interface and terminate the console session.
	exit	Terminate the current session (same as logout).

Table 5: Privilege level hierarchy — Manager Privilege

Privilege Level	Example of Prompt and Permitted Operations	
Manager Level	switch#	Perform system-level actions such as system control, monitoring, and diagnostic commands, plus any of the Operator-level commands. For a list of available commands, enter ? at the prompt.
Global Configuration Level	switch(config)#	Execute configuration commands, plus all Operator and manager commands. For a list of available commands, enter ? at the prompt.
Context Configuration Level	switch(eth-5)# switch(vlan-100)#	Execute context-specific configuration commands, such as a particular VLAN or switch port. This is useful for shortening the command strings you type, and for entering a series of commands for the same context. For a list of available commands, enter ? at the prompt.

Configuration commands and context configuration modes

You can execute any configuration command in the global configuration mode or in selected context modes. However, using a context mode enables you to execute context-specific commands faster, with shorter command strings.

The switch offers interface (port or trunk group) and VLAN context configuration modes:

Port or trunk-group context. Includes port-or trunk-specific commands that apply only to the selected port(s) or trunk group, plus the global configuration, Manager, and Operator commands. The prompt for this mode includes the identity of the selected port(s):

```
switch(config)# interface c3-c6
switch(eth-C5-C8)#
switch(config)# interface trk1
switch(eth-Trk1)#
```

Commands executed at configuration level for entering port and trk1static trunk-group contexts, and resulting prompts showing port or static trunk contexts.

```
switch(eth-C5-C8)#
switch(eth-Trk1)#
switch(eth-C5-C8)# ?
switch(eth-C5-C8)# ?
```

Lists the commands you can use in the port or static trunk context, plus the Manager, Operator, and context commands you can execute at this level.

Figure 36: Context-specific commands affecting port context

```
Switch(eth-C3-C6) # ?
| arp-protect          Configure the port as trusted or untrusted.
| bandwidth-min       Enable/disable and configure guaranteed minimum
|                    bandwidth settings for outgoing traffic on the port(s).
| broadcast-limit     Set a broadcast traffic percentage limit.
| dhcp-snooping       Configure the port as trusted or untrusted.
| disable             Disable port(s).
| enable              Enable port(s).
| energy-efficient-e... Enables or disables EEE on each port in the port list.
| flow-control        Enable/disable flow control negotiation on the port(s)
|                    during link establishment.
| gvrp                Set the GVRP timers on the port (hundredths of a
|                    second).
| ip                  Apply the specified access control list to inbound
|                    packets on this INTERFACE list.
| ipv6                Configure various IPV6 parameters for the VLAN.
| lACP                Define whether LACP is enabled on the port, and whether
|                    it is in active or passive mode when enabled.
| ...
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| class               Create a classifier class and enter the class context.
| interface           Enter the Interface Configuration Level, or execute one
|                    command for that level.
| policy              Create a classifier policy and enter the policy
|                    context.
| ...
```

In the port context, the first block of commands in the "?" listing show the context-specific commands that will affect only ports C3-C6.

The remaining commands in the listing are Manager, Operator, and context commands.

VLAN context. Includes VLAN-specific commands that apply only to the selected VLAN, plus Manager and Operator commands. The prompt for this mode includes the VLAN ID of the selected VLAN. For example, if you had already configured a VLAN with an ID of 100 in the switch:

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

Command executed at configuration level to enter VLAN 100 context.

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

Resulting prompt showing VLAN 100 context.

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

Lists commands you can use in the VLAN context, plus Manager, Operator, and context commands you can execute at this level.

Figure 37: Context-specific commands affecting VLAN context

In the VLAN context, the first block of commands in the "?" listing show the commands that will affect only vlan-100.

```
Switch(vlan-100) #
connection-rate-11... Re-enables access to a host or set of hosts that has
been previously blocked by the connection rate filter.

dhcp-snooping
disable Enable/Disable various features on the switch.
forbid Prevent ports from becoming a member of the current
VLAN.

igmp-proxy Associate an IGMP proxy domain with a VLAN.
ip Configure various IP parameters for the VLAN.
ip-recv-mac-address Associates a L3-mac-address with a VLAN.
ipv6 Configure various IPv6 parameters for the VLAN.
jumbo Labels this VLAN as a Jumbo VLAN, allowing you to pass
packets up to 9216 bytes in size.

monitor Define either the VLAN is to be monitored or not.
name Set the VLAN's name.
protocol Set a predefined protocol for the current VLAN.
qos Set VLAN-based priority.
service-policy Apply the QoS/Mirror policy on the vlan.
tagged Assign ports to current VLAN as tagged.
untagged Assign ports to current VLAN as untagged.
voice Labels this VLAN as a Voice VLAN, allowing you to
separate, prioritize, and authenticate voice traffic
moving through your network.

vrrp Enable/disable/configure VRRP operation on the VLAN.
```

class Create a classifier class and enter the class context.
interface Enter the Interface Configuration Level, or execute one
command for that level.
policy Create a classifier policy and enter the policy
context.
...

The remaining commands in the listing are Manager, Operator, and context commands.

Using the CLI to implement configuration changes

The CLI offers these capabilities for implementing configuration changes:

Procedure

1. Access to the full set of switch configuration features
2. The option of testing configuration changes before making them permanent

How to use the CLI to view the current configuration files. Use **show** commands to view the configuration for individual features, such as port status or Spanning Tree Protocol. However, to view either the entire startup-config file or the entire running-config file, use the following commands:

- **show config**

Displays a listing of the current startup-config file.

- **show running-config**

Displays a listing of the current running-config file.

- **write terminal**

Displays a listing of the current running-config file.

- **show default-config**

Displays a listing of a custom default config file.

- **show config status**

Compares the startup-config file to the running-config file and lists one of the following results:

- If the two configurations are the same, you will see:
 - Running configuration is the same as the startup configuration.
- If the two configurations are different, you will see:
 - Running configuration has been changed and saved.



show config, **show running-config**, and **write terminal** commands display the configuration settings that differ from the switch's factory default configuration.

How to use the CLI to reconfigure switch features. Use this procedure to permanently change the switch configuration (that is, to enter a change in the startup-config file).

1. Use the appropriate CLI commands to reconfigure the desired switch parameters. This updates the selected parameters in the running-config file.
2. Use the appropriate **show** commands to verify that you have correctly made the desired changes.
3. Observe the switch's performance with the new parameter settings to verify the effect of your changes.
4. When you are satisfied that you have the correct parameter settings, use the **write memory** command to copy the changes to the startup-config file.

The **write memory** command saves the running configuration file to the startup-config. The saved configuration becomes the boot-up configuration of the switch on the next boot.

When using redundant management, saves the running configuration of the switch to flash on the active management module. The saved configuration becomes the boot-up configuration of the switch the next time it is booted. The saved configuration file is synchronised to the standby management module.

Note: If the active management module and the standby management module are running on different operating systems because the **boot set-default** command was executed and then the standby module was rebooted, the **write memory** command displays this warning: "Warning: The next reboot or failover is set to boot from a different software image. These config changes may be incompatible or not used after a reboot or failover."

For example, the default port mode setting is **auto**. Suppose that your network uses Cat 3 wiring and you want to connect the switch to another autosensing device capable of 100 Mbps operation. Because 100 Mbps over Cat 3 wiring can introduce transmission problems, the recommended port mode is **auto-10**, which allows the port to negotiate full- or half-duplex, but restricts speed to 10 Mbps. The following command configures port A5 to auto-10 mode in the running-config file, allowing you to observe performance on the link without making the mode change permanent.

```
switch(config)# interface e a5 speed-duplex auto-10
```

After you are satisfied that the link is operating properly, you can save the change to the switch's permanent configuration (the startup-config file) by executing the following command:

```
switch(config)# write memory
```

The new mode (**auto-10**) on port A5 is now saved in the startup-config file, and the startup-config and running-config files are identical. If you subsequently reboot the switch, the **auto-10** mode configuration on port A5 will remain because it is included in the startup-config file.



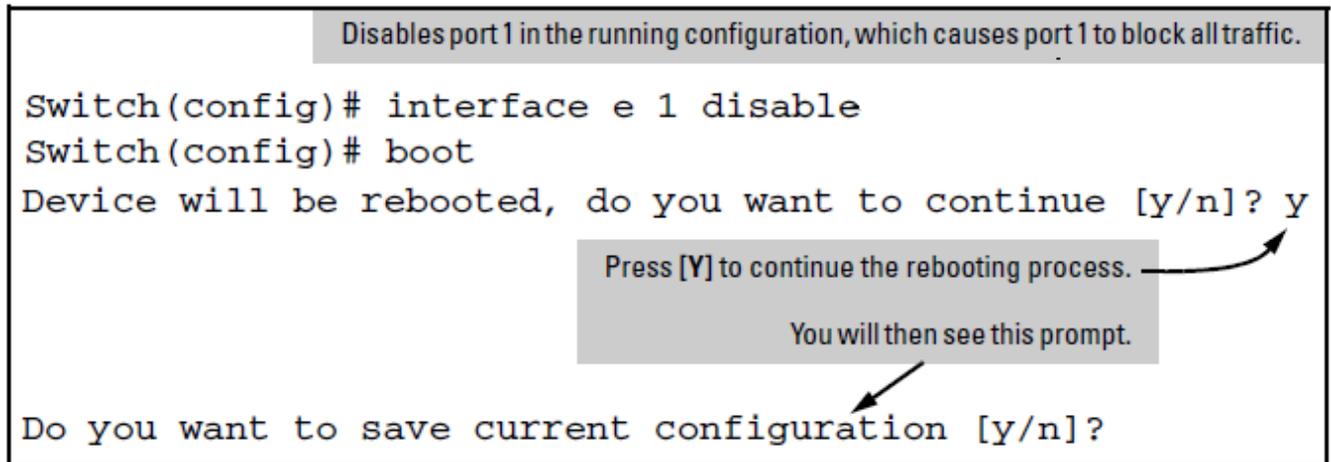
Beginning with K.15.01.0031, configuration changes to ports may require up to 10 seconds to take effect, especially on switches with high CPU utilization. After a configuration command, perform an appropriate **show** or **show running-config** command to confirm the configuration change. If configuration scripts are used, the script must be modified either to check for successful completion of the previous command before executing the next command, or to sleep for 10 seconds after the configuration command is executed.

How to cancel changes you have made to the running-config file. If you use the CLI to change parameter settings in the running-config file, and then decide that you do not want those changes to remain, you can use either of the following methods to remove them:

- Manually enter the earlier values you had for the changed settings. (This is recommended if you want to restore a small number of parameter settings to their previous boot-up values.)
- Update the running-config file to match the startup-config file by rebooting the switch. (This is recommended if you want to restore a larger number of parameter settings to their previous boot-up values.)

If you use the CLI to change a parameter setting, and then execute the **boot** command without first executing the **write memory** command to save the change, the switch prompts you to specify whether to save the changes in the current running-config file. For example:

Figure 38: Boot prompt for an unsaved configuration



The above prompt means that one or more parameter settings in the running-config file differ from their counterparts in the startup-config file and you can choose which config file to retain and which to discard.

- If you want to update the startup-config file to match the running-config file, press [Y] for “yes”. (This means that the changes you entered in the running-config file will be saved in the startup-config file.)
- If you want to discard the changes you made to the running-config file so that it will match the startup-config file, then select [N] for “no”. (This means that the switch will discard the changes you entered in the running-config file and will update the running-config file to match the startup-config file.)



If you use the CLI to make a change to the running-config file, you can either use the **write memory** command or select the save option allowed during a reboot (see **Figure 38: Boot prompt for an unsaved configuration** on page 76) to save the change to the startup-config file. That is, if you use the CLI to change a parameter setting, but then reboot the switch from either the CLI or the menu interface without first executing the **write memory** command in the CLI, the current startup-config file will replace the running-config file, and any changes in the running-config file will be lost.



Using the **Save** command in the menu interface does not save a change made to the running config by the CLI unless you have also made a configuration change in the menu interface. Also, the menu interface displays the current running-config values. Thus, where a parameter setting is accessible from both the CLI and the menu interface, if you change the setting in the CLI, the new value will appear in the menu interface display for that parameter. **However, as indicated above, unless you also make a configuration change in the menu interface, only the write memory command in the CLI will actually save the change to the startup-config file**

How to reset the startup-config and running-config files to the factory default configuration. Use the **erase startup-config** command to reboot the switch, which replaces the contents of the current startup-config and running-config files with the factory-default startup configuration.

Figure 39: The erase startup-config command

```
switch(config)# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?
```

Press [y] to replace the current configuration with the factory default configuration and reboot the switch. Press [n] to retain the current configuration and prevent a reboot.

In a redundant management system, this command erases the startup config file on both the active and the standby management modules as long as redundancy has not been disabled. If the standby management module is not in standby mode or has failed selftest, the startup config file is not erased.

Creating a custom default configuration



This feature is not supported on the 3800 switches.

The custom default configuration feature provides the ability to initialize a switch to a different state from the factory default state when you delete the active configuration file. The factory default configuration is not changed. If a custom configuration file has been created and the active configuration file is deleted, the switch will boot up using the custom configuration file.

The feature provides the ability to:

Procedure

1. Use a customized configuration file as a default configuration file
2. Enable the switch to start up with the specified default configuration

The existence of a custom default configuration file does not affect the results of loading a remotely stored configuration file onto the switch.

Using a custom default configuration, you can configure the features you want to be in the default configuration. When the active configuration is deleted using the **erase startup** command, the active configuration is removed and the custom default configuration file will be used upon bootup. The standard default configuration file remains and is used if there is no custom default configuration.



This feature does **not** change the system defaults. The custom default configuration file is automatically used when the startup configuration file is erased. It has no effect on what is loaded onto the switch when a remotely stored configuration file is restored.

The default configuration file can be customized using commands at the CLI prompt or by copying a configuration file with the desired configuration using TFTP, USB, or XMODEM copy commands. The existing default configuration file also can be transferred from the switch using these commands.

To start creating the configuration file to be used as the custom default configuration file, enter the commands that configure the features desired and then save the configuration file using the **write memory** command. The following example is as shown.

Figure 40: Creating a config file with the desired features

```
switch(config)# spanning-tree
switch(config)# interface 4 flow-control

switch(config)# write memory
```

This configuration, which enables flow control on interface 4, and also spanning tree on the switch, is stored in the startup configuration file.

To save this configuration as the custom default configuration, the startup configuration file is copied to the default configuration file, as shown following.

Figure 41: Copying the startup configuration file to the custom default configuration file

```
switch(config)# copy startup-config default-config
```

Copying an existing configuration file to the custom default configuration file

Use the following command to copy a configuration file that exists in flash memory to the custom default configuration file:

```
copy config <source-filename> default-config
```

The switch can have up to three different configuration files stored in flash memory. (For more information about multiple configuration files, see "Multiple Configuration Files" in the *Management and Configuration Guide* for your switch.)

```
switch(config)# copy abc.cfg default-config
```



HPE does not support issues that arise from a configuration file that was manually edited and downloaded to the switch.

Copying the custom default config file onto the switch

The custom default config file can be copied onto the switch using TFTP, XMODEM, or USB.

- TFTP

Use the **copy tftp default-config** command to copy a configuration file stored on a TFTP server to the custom default configuration file:

```
copy tftp default-config <ip-addr> <stored config file name>
```

Copying a stored config file to the default config file using TFTP

```
switch(config)# copy tftp default-config 10.10.10.1 stored_config.cfg
```

- XMODEM

Use the **copy xmodem default-config** command to copy a configuration file to the custom default configuration file using XMODEM:

```
copy xmodem default-config
```

Copying a stored config file to the custom default config file using XMODEM

```
switch(config)# copy xmodem default-config
```

- USB

Use the **copy usb default-config** command to copy a configuration file to the custom default configuration file using USB:

```
copy usb default-config <stored config file name>
```

Copying a stored config file to the custom default config file using USB

```
switch# copy usb default-config stored_config.cfg
```

Copying the custom default config file off the switch

The following sections explain how to copy the custom default config file off the switch using TFTP, XMODEM, or USB.

Procedure

1. TFTP—Enter the following command to copy the custom default configuration file to the stored_config.cfg file on the TFTP server.

```
copy default-config tftp <server ip-address> stored_config.cfg
```

2. XMODEM—Enter the following command to copy the custom default configuration file to the configuration file specified by the XMODEM server device.

```
copy default-config xmodem
```

3. USB—Enter the following command to copy a custom default configuration file from the switch to the stored_config.cfg file on the USB device.

```
copy default-config usb stored_config.cfg
```

Using SFTP and SCP to transfer the custom configuration

To transfer the default custom configuration file to or from the switch, you must connect to the switch's SSH server using any SCP or SFTP client. Instead of the actual name of the custom default configuration file, an alias name of "default-config" is displayed in the file listings and for get/store functions.



When you use an SCP client to connect to the switch, you must know the name of the file you wish to get or store. When you use SFTP client to connect to the switch, you are provided with a list of filenames which are accessed by the switch.

While the switch supports an SSH server with SCP and/or SFTP running on it, the switch is not an SCP or SFTP client. You must have an SCP/SFTP client implemented in order to execute **copy scp** or **copy sftp** commands on the switch.

The following example shows the output from running **puTTY psftp** on a remote PC.

```
C:\PuTTY> psftp 10.1.243.209

We'd like to keep you up to date about:
* Software feature updates
* New product announcements
* Special events

Please register your product at: www.register.hp.com

Remote working directory is /
psftp> ls
Listing directory /
drwxr-xr-x   2 J9145A   J9145A   0 Jan 01 00:01 cfg
drwxr-xr-x   2 J9145A   J9145A   0 Jan 01 00:01 core
drwxr-xr-x   2 J9145A   J9145A   0 Jan 01 00:01 log
drwxrwxrwx   2 J9145A   J9145A   0 Jan 01 00:01 os
drwxrwxrwx   3 J9145A   J9145A   0 Jan 01 00:01 ssh

psftp> ls /cfg
Listing directory /cfg
-rwxrw-r--   1 J9145A   J9145A   1749 Jan 01 00:01 default-config
-rw-r--r--   1 J9145A   J9145A    745 Jan 01 01:19 running-config
-rwxrw-r--   1 J9145A   J9145A    360 Jan 01 01:19 startup-config

psftp>
```

Erasing a configuration file

To erase a configuration file:

Procedure

1. To erase the startup configuration file, use the **erase startup-config** command.

If a custom default configuration file exists and the **erase startup-config** command is executed, the current active configuration is erased and the switch is booted with the custom default configuration. If a custom default configuration file does not exist and the **erase startup-config** command is executed, the current active configuration is erased and the switch is booted with the system default configuration.

2. To erase the custom default configuration file, use the **erase default-config** command.

The following example shows how to erase the startup config file when a default custom config file exists

```
switch(config)# erase startup-config
Configuration will be deleted, and existing login passwords
removed, and device rebooted (using the custom default
configuration), continue [y/n]?
```

The following example shows how to erase the startup config file when a default custom config file does not exist

```
switch(config)# erase startup-config
Configuration will be deleted, and existing login passwords removed,
and device rebooted, continue [y/n]?
```

The following example shows how to erase the custom default config file.

```
switch(config)# erase default-config
The custom default configuration will be erased. The "erase
startup-config" command will now use system generated default
configuration. Continue [y/n]?
```

Displaying the configuration files

To display configuration files:

- Use the **show config files** command to display the existing configuration files. This command also indicates whether a custom default configuration file exists.
- Use either the command **show default config** or the command **show running-config** to display the custom default configuration.

If a custom default configuration file exists and you erase the current active config file (using the `erase startup-config` command), use the **show running-config** command to display the custom default configuration, which is loaded upon bootup.



For the 3800 switches, when the **show default config** command is executed in enhanced secure mode the following prompt displays:

Do you want to show sensitive information (y/n)?

If "Y/y" is entered, the normal command output is displayed on the console. If "N/n" is entered, all the sensitive information is hidden and will be displayed as asterisks ("*****"). The default option is "N/n"

when interactive mode is disabled. For more information, see the "Secure Mode" in the *Access Security Guide* for your switch.

Figure 42: *Output displaying three configuration files*

```
switch(config)# show config files

Configuration files:

id | act pri sec | name
---+-----+-----
 1  *   *       | config
 2                   | secondaryconfig
 3                   * | Kconfig
=====
A Custom default configuration file exists.
```

Figure 43: *Output for custom default configuration file*

```
switch(config)# show default-config

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.14.0001

; Ver #02:0b:ef:e6
hostname "switch"
module 1 type J93x7
module 2 type J93x7
vlan 1
  name "DEFAULT-VLAN"
  untagged 1-24
  ip address dhcp-bootp
  exit
interface 4
  flow-control
  exit snmp-server community "public" unrestricted
spanning-tree
```

Figure 44: *Output of custom default config file when current active config file erased*

```
switch(config)# show running-config

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.12.0001
; Ver #02:0b:ef:e6
hostname "switch"
module 1 type J93x7
module 2 type J93x7
vlan 1
  name "DEFAULT-VLAN"
  untagged 1-24
  ip address dhcp-bootp
  exit
interface 4
  flow-control
  exit
snmp-server community "public" unrestricted
spanning-tree
```

Troubleshooting custom default configuration files

Symptom

Switch cannot boot due to custom default configuration files.

Cause

Problem with the custom configuration file.

Action

1. Remove the custom configuration file from the ROM mode interface.
2. Use the **erase default-config** command to remove the custom default configuration file.

The custom default configuration files cannot be erased using the front panel buttons on the switch.

Using the menu and WebAgent to implement configuration changes configuration file

The menu and WebAgent offer these advantages:

Procedure

1. Quick, easy menu or window access to a subset of switch configuration features
2. Viewing several related configuration parameters in the same screen, with their default and current settings
3. Immediately changing both the running-config file and the startup-config file with a single command

Menu: implementing configuration changes

You can use the menu interface to simultaneously save and implement a subset of switch configuration changes without having to reboot the switch. That is, when you save a configuration change in the menu interface, you simultaneously change both the running-config file and the startup-config file.



NOTE

The only exception to this operation is two VLAN-related parameter changes that require a reboot as described in this section.

Using Save and Cancel in the menu interface

For any configuration screen in the menu interface, the **save** command:

1. Implements the changes in the running-config file
2. Saves your changes to the startup-config file

If you decide not to save and implement the changes in the screen, select **Cancel** to discard them and continue switch operation with the current operation. For example, suppose that you have made the changes as shown in the following System Information screen:

Figure 45: Example of pending configuration changes you can save or cancel

```
----- CONSOLE - MANAGER MODE -----
                Switch Configuration - System Information

System Name :      ProCurve Switch
System Contact :
System Location :

Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
Time Sync Method [None] : TIMEP
TimeP Mode [Disabled] : Disabled

Time Zone [0] : 0
Daylight Time Rule [None] : Continental-US-and-Canada

Actions->   Cancel      Edit      Save      Help

Select Daylight Time Rule for your location.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```



If you reconfigure a parameter in the CLI and then go to the menu interface without executing a write memory command, those changes are stored only in the running configuration (even if you execute a Save operation in the menu interface). If you then execute a switch **boot** command in the menu interface, the switch discards the configuration changes made while using the CLI. To ensure that changes made while using the CLI are saved, execute **write memory** in the CLI before rebooting the switch.

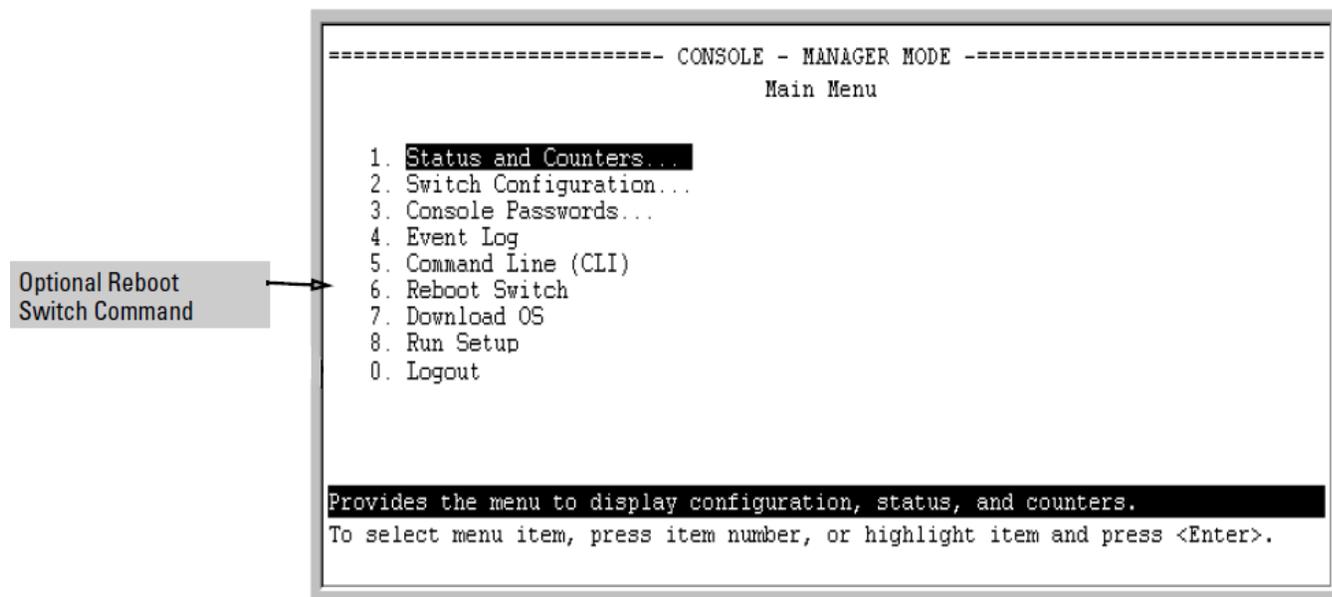
Rebooting from the menu interface

Rebooting from the menu interface does the following:

- Terminates the current session and performs a reset of the operating system
- Activates any configuration changes that require a reboot
- Resets statistical counters to zero

To Reboot the switch, use the **Reboot Switch** option in the Main Menu. (Note that the Reboot Switch option is not available if you log on in Operator mode; that is, if you enter an Operator password instead of a manager password at the password prompt.)

Figure 46: *The Reboot Switch option in the Main Menu*



Rebooting To Activate Configuration Changes. Configuration changes for most parameters become effective as soon as you save them. However, you must reboot the switch in order to implement a change in the **Maximum VLANs to support** parameter.

(To access these parameters, go to the Main menu and select **2. Switch Configuration**, then **8. VLAN Menu**, then **1. VLAN Support**.)

If configuration changes requiring a reboot have been made, the switch displays an asterisk (*) next to the menu item in which the change has been made. For example, if you change and save parameter values for the

Maximum VLANs to support parameter, an asterisk appears next to the **VLAN Support** entry in the VLAN Menu screen, and also next to the **Switch Configuration ...** entry in the Main menu:

Figure 47: Indication of a configuration change requiring a reboot

```
----- CONSOLE - MANAGER MODE -----
                          Switch Configuration Menu

1. System Information
2. Port/Trunk Settings
3. Network Monitoring Port
4. Spanning Tree Operation
5. IP Configuration
6. SNMP Community Names
7. IP Authorized Managers
*8. VLAN Menu...
0. Return to Main Menu...

Displays the menu to activate and configure, or deactivate VLAN support.
To select menu item, press item number, or highlight item and press <Enter>.
(*Needs reboot to activate changes.)
```

WebAgent: implementing configuration changes

You can use the WebAgent to simultaneously save and implement a subset of switch configuration changes without having to reboot the switch. That is, when you save a configuration change, you simultaneously change both the running-config file and the startup-config file. For online help with configuring changes in the WebAgent, click the "?" in the WebAgent screen.



If you reconfigure a parameter in the CLI and then go to the WebAgent without executing a **write memory** command, those changes will be saved to the startupconfig file if you click **Save** in the WebAgent.

Zeroizing the file storage of the management module

Zeroizing the management module files

Procedure

1. Use the **erase all** to erase all management module files, including configuration files, core dumps, password files, crypto-key files, and so on .

Software images are not erased.

```
erase all zeroize
```



When executed without the `zeroize` option, files are removed, but the flash storage is not zeroized. The data is still physically present in the flash. The flash can be removed from the switch and the data recovered with file recovery tools.

It is recommended that zeroization be performed from the serial console so that the status information can be viewed during the zeroization process.

```
switch(config)# erase all zeroize
```

```
The system will be rebooted and all management module files  
except software images will be erased and zeroized. This will  
take up to 60 minutes and the switch will not be usable during  
that time. Continue (y/n)? y
```

Zeroizing from the ROM console

Use the **erase-all zeroize** command at the prompt to zeroize the file storage from the ROM console of the switch. This is typically done during a switch recovery process. The warning messages are the same as for the CLI command.

Zeroizing the management module files from the ROM console

```
=> erase-all zeroize
```

```
The system will be rebooted and all management module files  
except software images will be erased and zeroized. This will  
take up to 60 minutes and the switch will not be usable during  
that time. Continue (y/n)? y
```

Zeroization

Sometimes it is desirable to completely remove the information stored in user files from flash storage. The zeroization feature will remove and "zeroize" all the files from flash storage except software images. Information removed includes the following:

- switch configurations
- system generated private keys
- user installed private keys
- legacy manager/operator password files
- crypto-key files
- fdr logs
- core dumps

Zeroization can be initiated in these ways:

- CLI command **erase all**
- ROM console command
- During Secure Mode transition, initiated through the **secure-mode** CLI command executed in a serial session

The zeroization process takes some time, so it is performed during the initial process of a switch reboot. After zeroization, the configuration file is rebuilt from the default config file, which is similar to the config rebuilding process performed by the **erase startup-config** command.

When zeroization is triggered by a secure mode transition, HA handles zeroization on the AMM and SMM automatically.

When the CLI command (**erase all zeroize**) is used to start zeroization, the AMM syncs with the SMM and ensures that the SMM performs the same level of zeroization before the AMM starts the zeroization process on itself. The AMM before the zeroization process occurs remains the AMM, unless it takes over a minute for the AMM to boot up, in which case the prior SMM becomes the AMM.

When zeroization is started from the ROM console, there is no synchronization performed between the AMM and SMM, as zeroization from the ROM console is treated as a recovery facility. Each MM has to be zeroized individually.

For information about Secure Mode and zeroization, see the "Secure Mode (5400zl and 3800)" in the *Access Security Guide* for your switch.

Using Primary and Secondary flash image options

The switches covered in this guide feature two flash memory locations for storing switch software image files:

Procedure

1. Primary Flash:

The default storage for a switch software image.

2. Secondary Flash:

The additional storage for either a redundant or an alternate switch software image.

With the Primary/Secondary flash option, you can test a new image in your system without having to replace a previously existing image. You can also use the image options for troubleshooting. For example, you can copy a problem image into Secondary flash for later analysis and place another, proven image in Primary flash to run your system. The switch can use only one image at a time.

The following tasks involve primary/secondary flash options:

- Displaying the current flash image data and determining which switch software versions are available
- Switch software downloads
- Replacing and removing (erasing) a local switch software version
- System booting

Displaying the current flash image data

Use the commands in this section to:

- Determine whether there are flash images in both primary and secondary flash
- Determine whether the images in primary and secondary flash are the same
- Identify which switch software version is currently running

Viewing the currently active flash image version. Use the `show version` command to identify the software version on which the switch is currently running, and whether the active version was booted from the primary or secondary flash image.

For example, if the switch is using a software version of X.X.XX stored in Primary flash, `show version` produces the following:

Figure 48: *The identity of the current flash image*

```
switch(config)# show version

Image stamp:  /su/code/build/info(s01)
              Dec 01 2006 10:50:26
              X.X.XX
              1223
Boot Image:   Primary
```

Determining whether the flash images are different versions. If the flash image sizes in primary and secondary are the same, then in almost every case, the primary and secondary images are identical. This command provides a comparison of flash image sizes, plus the boot ROM version and from which flash image the switch booted. For example, in the following case, the images are different versions of the switch software, and the switch is running on the version stored in the secondary flash image:

```
switch(config)# show flash
```

```

Image                Size(Bytes)   Date   Version
-----
Primary Image       : 7493854    03/21/10 K.15.01.0001
Secondary Image     : 7463821    03/23/10 K.15.01.0001

```

```

Boot Rom Version: K.15.08
Default Boot     : Primary

```

Determining which flash image versions are installed. The `show version` command displays which software version the switch is currently running and whether that version booted from primary or secondary flash. Thus, if the switch booted from primary flash, you will see the version number of the software version stored in primary flash, and if the switch booted from secondary flash, you will see the version number of the software version stored in secondary flash. Thus, by using `show version`, then rebooting the switch from the opposite flash image and using `show version` again, you can determine the version(s) of switch software in both flash sources. For example: Determining the software version in Primary and Secondary flash

```

switch(config)# show version
Management Module 1: Active
Image stamp:      /sw/code/build/btm(ec_K_15)
                  Aug 2 2012 09:06:58
                  K.15.12.001
                  152
Boot Image:      Primary
switch(config)# boot system flash secondary
Device will be rebooted, do you want to continue [y/n]? y
.
.
.

```

```

switch(config)# show version
Management Module 1: Active
Image stamp:      /sw/code/build/btm(ec_K_15)
                  Aug 2 2012 09:06:58
                  K.15.12.001
                  1753
Boot Image:      Secondary

```

Switch software downloads

The following table shows the switch's options for downloading a software version to flash and booting the switch from flash.

Table 6: *Primary/Secondary memory access*

Action	Menu	CLI	Web Agent	SNMP
Download to Primary	Yes	Yes	Yes	Yes
Download to Secondary	No	Yes	No	Yes
Boot from Primary	Yes	Yes	Yes	Yes
Boot from Secondary	No	Yes	No	Yes

The different software download options involve different `copy` commands, plus `xmodem`, `usb`, and `tftp`.

Download interruptions. In most cases, if a power failure or other cause interrupts a flash image download, the switch reboots with the image previously stored in primary flash. In the unlikely event that the primary image is corrupted, as a result of an interruption, the switch will reboot from secondary flash and you can either copy the secondary image into primary or download another image to primary from an external source.

Replacing or removing local switch software

This section describes commands for erasing a software version and copying an existing software version between primary and secondary flash.



It is not necessary to erase the content of a flash location before downloading another software file. The process automatically overwrites the previous file with the new file. If you want to remove an unwanted software version from flash, Hewlett Packard Enterprise recommends that you do so by overwriting it with the same software version that you are using to operate the switch, or with another acceptable software version. To copy a software file between the primary and secondary flash locations, See "Copying a switch software image from one flash location to another", below.

The local commands described here are for flash image management within the switch. To download a software image file from an external source, see "File Transfers" in the *Management and Configuration Guide* for your switch.

Copying a switch software image from one flash location to another. When you copy the flash image from primary to secondary or the reverse, the switch overwrites the file in the destination location with a copy of the file from the source location. This means you **do not** have to erase the current image at the destination location before copying in a new image.



Verify that there is an acceptable software version in the source flash location from which you are going to copy. Use the **show flash** command or, if necessary, the procedure under **Displaying the current flash image data** to verify an acceptable software version. Attempting to copy from a source image location that has a corrupted flash image overwrites the image in the destination flash location. In this case, the switch will not have a valid flash image in either flash location, but will continue running on a temporary flash image in RAM. **Do not reboot the switch.** Instead, immediately download another valid flash image to primary or secondary flash. Otherwise, if the switch is rebooted without a software image in either primary or secondary flash, the temporary flash image in RAM will be cleared and the switch will go down. To recover, see "Restoring a Flash Image" in the *Management and Configuration Guide* for your switch.

Syntax

```
copy flash flash <destination flash>
```

where: **destination flash = primary or secondary:**

For example, to copy the image in secondary flash to primary flash:

- Verify that there is a valid flash image in the secondary flash location. The following figure indicates that a software image is present in secondary flash. (If you are unsure whether the image in secondary flash is valid, try booting from it before you proceed by using `boot system flash secondary`)

The following example indicates two different software versions in Primary and Secondary flash:

```
switch(config)# show flash
Image              Size (bytes) Date      Version
-----
Primary Image      : 10167529   10/14/11 K.14.89
Secondary Image    : 15085139   08/17/12 K.15.10.0001

Boot ROM Version   : K.15.28
Default Boot       : Primary
```

Syntax

Execute the copy command as follows:

```
switch(config)# copy flash flash primary
```

Erasing the contents of Primary or Secondary flash. This command deletes the software image file from the



No undo! Before using this command in one flash image location (primary or secondary), ensure that you have a valid software file in the other flash image location (secondary or primary). If the switch has only one flash image loaded (in either primary or secondary flash) and you erase that image, then the switch does not have a software image stored in flash. In this case, if you do not reboot or power cycle the switch, you can recover by using xmodem or tftp to download another software image.

```
erase flash [primary | secondary]
```

For example, to erase the software image in primary flash, do the following:

1. First verify that a usable flash image exists in secondary flash. The most reliable way to ensure this is to reboot the switch from the flash image you want to retain. For example, if you are planning to erase the primary image, then first reboot from the secondary image to verify that the secondary image is present and acceptable for your system:

```
switch# boot system flash secondary
```

2. Then erase the software image in the selected flash (in this case, primary):

```
switch# erase flash primary
The Primary OS Image will be deleted, continue [y/n]?
```

3. Type 'y' at the prompt to complete the flash erase.

4. Use show flash to verify erasure of the selected software flash image. The "0" shows that the primary flash has been erased.

The following example shows flash listing after erasing Primary flash

```
switch# show flash
Compressed Primary Code size = 0
Compressed Secondary code size = 2555802
Boot ROM Version : K.15.19
Default Boot : Secondary
```

In redundant management systems, this command will erase the selected flash in both the active and the standby management modules. If redundancy has been disabled or the standby module has failed self-test, this command only affects the active management module.

Rebooting the switch

Setting the default flash for bootup

To specify the default flash (primary or secondary) to boot from on the next boot, use the **boot set-default flash** command. The syntax is as follows:

```
boot set-default flash [ primary|secondary ]
```

```
switch(config)# boot set-default flash secondary
switch(config)# show flash
Image                Size(Bytes)    Date      Version
-----
Primary Image       : 7476770      03/15/10  K.15.01.0001
Secondary Image     : 7476770      03/15/10  K.15.01.0001
```

```
Boot Rom Version: K.15.08
Default Boot      : Secondary
```

```
switch(config)# boot
This management module will now reboot from secondary
and will become the standby module! You will need to
use the other management module's console interface.
Do you want to continue [y/n]?
```

Booting from the default flash or configuration file

Procedure

1. To boot the switch from the default flash (primary or secondary) image, use the **boot** command.

This command allows a boot sequence that includes the complete set of self-tests.

The switch is booted either from the flash (primary or secondary) that you are currently booted on or from the flash image that was set by the **boot set-default** command or by the last executed **boot system flash <primary | secondary>** command. You can select which image to boot from during the boot process itself (you are prompted with a message which will indicate the flash being booted from). When using redundant management, the switch will fail over to the standby management module.

2. To boot from a configuration file, use the **boot config <filename>** command.

This command allows a boot sequence that includes the complete set of self-tests.

The following example shows the Boot command (default Primary flash) with redundant management

```
switch(config)# boot
This management module will now reboot from primary image
and will become the standby module! You will need to use
the other management module's console interface.
Do you want to continue [y/n]? y
```

```
Do you want to save current configuration [y/n]? n
```

In the above example, typing either a 'y' or 'n' at the second prompt initiates the reboot operation. (Entering 'y' saves any configuration changes from the running-config file to the startup-config file; entering 'n' discards them.)

The following example shows the Boot command booting from a different flash than the current flash (with redundant management module present)

```
switch(config)# show flash
Image Size(Bytes) Date Version
Primary Image : 7497114 03/29/10 K.15.01.0001
Secondary Image : 7497114 03/29/10 K.15.01.0001
Boot Rom Version: K.15.08
Default Boot : Primary
```

```
switch(config)# boot set-default flash secondary
This command changes the location of the default boot.
This command will change the default flash image to boot from
secondary. Hereafter, 'reload' 'boot' commands will boot from
secondary. Do you want to continue [y/n]? y
```

```
switch(config)# boot
This management module will now reboot from secondary image
and will become the standby module! You will need to use the
other management module's console interface.
Do you want to continue [y/n]? n
```

Booting from a specified flash

Procedure

1. To reboot from primary flash, use the **boot system flash primary** command . This command allows a boot sequence that includes the complete set of self-tests.
2. To reboot from secondary flash, use the **boot system flash secondary** command.
This command allows a boot sequence that includes the complete set of self-tests.

The following example shows use of the command to reboot the switch from secondary flash when there are no pending configuration changes in the running-config file. Typing either a [y] or [n] at the second prompt initiates the reboot operation.

Boot command with secondary flash option

```
switch(config)# boot system flash secondary
System will be rebooted from secondary image. Do you want to continue [y/n]?
```

Enabling and disabling the fastboot option

Procedure

1. To enable the fastboot option, use the **fastboot** command.
When this option is enabled, the bootup sequence does not include the internal power-on self-tests, resulting in a faster boot time.
2. To disable the fastboot option, use the **no fastboot** command.
When this option is disabled, the bootup sequence includes the complete set of self-tests.
3. To display the status of the fastboot feature, either enabled or disabled, use the **show fastboot** command.

When using redundant management and fastboot is enabled, it is saved to the standby management module when the config files are synchronized. Fastboot is used during the next bootup on either management module.

Enabling the fastboot option

```
switch(config)# fastboot
```

Using reload

The **reload** command reboots the switch from the flash image that you are currently booted on (primary or secondary) or the flash image that was set either by the **boot set-default** command or by the last executed **boot system flash <primary | secondary>** command. Because **reload** bypasses some subsystem self-tests, the switch reboots faster than if you use either of the **boot** command options. If you are using redundant management and redundancy is enabled, the switch will failover to the other management module.

Syntax

```
reload
```

For example, if you change the number of VLANs the switch supports, you must reboot the switch in order to implement the change. The **reload** command prompts you to save or discard the configuration changes.

The following example shows how to use reload with redundant management and pending configuration changes:

```
switch(config)# max-vlans 12
Command will take effect after saving configuration and reboot.

switch(config)# reload
This command will cause a switchover to the other management
```

module which may not be running the same software image and configurations. Do you want to continue [y/n]? y

Scheduled reload. Beginning with software release K.11.34, additional parameters have been added to the **reload** command to allow for a scheduled reboot of the switch via the CLI.

Syntax

```
reload [after <[dd:]hh:] [mm>] | [at <hh:mm[:ss]>] [<mm/dd[/[yy]yy]>]
no reload [after <[dd:]hh:] [mm>] | [at <hh:mm[:ss]>] [<mm/dd[/[yy]yy]>]
```

Enables a scheduled warm reboot of the switch. The switch boots up with the same startup config file and using the same flash image as before the reload.



When using redundant management, the reload at/after command causes a switch over at the scheduled time to the other management module, which may not be running the same software image or have the same configurations.

Parameters include:

- **after**
Schedules a warm reboot of the switch after a given amount of time has passed.
- **at**
Schedules a warm reboot of the switch at a given time.

The `no` form of the command removes a pending reboot request.

For more details and examples, see the following.

The scheduled reload feature removes the requirement to physically reboot the switch at inconvenient times (for example, at 1:00 in the morning). Instead, a **reload at 1:00 mm/dd** command can be executed (where **mm/dd** is the date the switch is scheduled to reboot).



Configuration changes are not saved with **reload at** or **reload after** commands. No prompt to save configuration file changes is displayed. See [Boot and reload command comparison](#).

Examples of scheduled **reload** commands:

- To schedule a reload in 15 minutes:

```
switch# reload after 15
```
- To schedule a reload in 3 hours:

```
switch# reload after 03:00
```
- To schedule a reload for the same time the following day:

```
switch# reload after 01:00:00
```
- To schedule a reload for the same day at 12:05:

```
switch# reload at 12:05
```
- To schedule a reload for some future date:

```
switch# reload at 12:05 01/01/2008
```

The following example shows the reload command with a redundant management system

```
switch(config)# reload after 04:14:00
Reload scheduled in 4 days, 14 hours, 0 minutes
This command will cause a switchover at the scheduled
time to the other management module which may not be
running the same software image and configurations.
Do you want to continue [y/n]?
```

Module reload. The module reload feature allows you to reset a module by initiating a warm reboot of a specified module or modules. This saves time over rebooting the entire switch, which can take several minutes to complete and disrupts all users on the switch. The specified module has its power turned off, and then turned on again. This causes the module to reset to a known good state and reload its software.

Syntax

```
reload [[after <[[DD:]HH:]MM>] | [[at HH:MM[:SS] [MM/DD[/[YY]YY]]]]]
| [[module <slot-id-range>]]]
no reload [[after <[[DD:]HH:]MM>] | [[at HH:MM[:SS] [MM/DD[/[YY]YY]]]]]
| [[module <slot-id-range>]]]
```

When specified with the module parameter, initiates a reload of the module in the specified slot or slots by turning the slot power off, then on again. A valid slot or range of slots must be specified. The at and after parameters are not allowed with the module option. The no version of the command is not valid with the module option.

When the reload command is executed without any parameters, an immediate switch reload occurs.



This feature is not supported for HPE One modules.

module: Powers the module on or off, forcing a software reload of the specified module or modules.

The following example shows reloading a specified module:

```
switch(config)# reload module C
The 'reload module' command will shutdown the specified
modules. Ports on specified modules will no longer pass
traffic. Any management traffic to the switch which
passes through the affected modules will be interrupted
(e.g. ssh, telnet, snmp). This command may take up to 2
minutes to power down all specified modules. Please check
the event log for current status of module power down,
power up cycle. Continue [y/n]?
```

Displaying reload information. Use the **show reload** command to display the reload information. This can include:

- A scheduled, pending reload of the entire switch
- A statement that no reload is scheduled
- The time of the last reload of each module on the system

The following example shows the scheduled reload at information:

```
switch(config)# reload at 23:45
Reload scheduled at 23:45:47 6/16/2012
(in 0 days, 1 hours, 41 minutes)

switch(config)# show reload at
Reload scheduled for 23:45:47 06/16/2012
(in 0 days, 1 hours, 40 minutes)

switch(config)# show reload after
Reload scheduled for 23:45:47 6/16/2012
(in 0 days, 1 hours, 40 minutes)
```

The following example shows the scheduled reload after information:

```
switch(config)# reload after 35
Reload scheduled in 0 days, 0 hours, 35 minutes
```

```
switch(config)# show reload at
Reload scheduled in 0 days, 0 hours, 34 minutes
```

```
switch(config)# show reload after
Reload scheduled in 0 days, 0 hours, 34 minutes
```

The following example shows the module reload information:

```
switch(config)# show reload module
```

Module Reload information:

```
Module | Last reload date
-----+-----
C      10:50:51 01/13/2012
```

Boot and reload command comparison

The switch offers reboot options through the **boot** and **reload** commands, plus the options inherent in a dual-flash image system. Generally, using **boot** provides more comprehensive self-testing; using **reload** gives you a faster reboot time.

Table 7: Comparing the boot and reload commands

Actions	Included in Boot?	Included in Reload	Note
Save all configuration changes since the last boot or reload	Optional, with prompt	Optional with reload <cr>, when prompt displays. Not saved with reload at/after commands; No prompt is displayed.	Config changes saved to the startup-config file if "y" is selected (reload command).
Perform all system self-tests	Yes	No	The reload command provides a faster system reboot.
Choice of primary or secondary flash image	Yes	No—Uses the current flash image.	
Perform a scheduled reboot	No	Yes	Use the reload command with after/at parameters (see for Using reload details).

Operating notes about booting

Default boot source. The switch reboots from primary flash by default unless you specify the secondary flash by entering either the **boot system flash [primary | secondary]** or **boot set-default flash [primary | secondary]** command. Both the **boot** command and the **reload** command will reboot based on how these options have been selected.

Boot attempts from an empty flash location. In this case, the switch aborts the attempt and displays:

```
Image does not exist
Operation aborted.
```

Interaction of Primary and Secondary flash images with the current configuration. The switch has one startup-config file (see [Configuration file management](#) on page 112), which it always uses for reboots, regardless of whether the reboot is from primary or secondary flash. Also, for rebooting purposes, it is not

necessary for the software image and the startup-config file to support identical software features. For example, suppose that you have just downloaded a software upgrade that includes new features that are not supported in the software you used to create the current startup-config file. In this case, the software simply assigns factory-default values to the parameters controlling the new features. Similarly, if you create a startup-config file while using a version "Y" of the switch software, and then reboot the switch with an earlier software version "X" that does not include all the features found in "Y", the software simply ignores the parameters for any features that it does not support.

Scheduled reload. If no parameters are entered after the **reload** command, an immediate reboot is executed. The **reload at** and **reload after** command information is not saved across reboots. If the switch is rebooted before a scheduled reload command is executed, the command is effectively canceled. When entering a **reload at** or **reload after** command, a prompt will appear to confirm the command before it can be processed by the switch. For the **reload at** command, if mm/dd/yy are left blank, the current day is assumed.

The scheduled reload feature removes the requirement to physically reboot the switch at inconvenient times (for example, at 1:00 in the morning). Instead, a **reload at 1:00 mm/dd** command can be executed (where **mm/dd** is the date the switch is scheduled to reboot).

Managing multiple configuration files

Viewing the status and content of startup-config files

Procedure

1. To view a list of the available startup-config files on the switch and the current use of each file, use the **show config files** command.
2. To view the content of the default startup-config file, use the **show config** command.

The default startup-config file is the startup-config file that is currently active on the switch.

3. To view the content of a specific startup-config file, use the **show config <filename>** command.

The **filename** argument specifies the file. With Multiple Configuration enabled, the switch can have up to three startup-config files. This command can display the content of any of the startup-config files stored in the switch, whereas the **show config** command always displays the content of the default startup-config file.

Changing or overriding the reboot configuration policy

To change the reboot configuration policy, do one of the following:

- Use the **startup-default primary config <filename>** command to change the current policy so that the switch automatically reboots from the primary flash using the specified startup-config file. The **filename** argument specifies the startup-config file to use.
- Use the **startup-default secondary config <filename>** command to change the current policy so that the switch automatically reboots from the secondary flash using the specified startup-config file. The **filename** argument specifies the startup-config file to use.

To override the default reboot configuration policy for a single reboot instance, do one of the following:

- Use the **boot system flash primary config <filename>** command to override the current policy so that the switch automatically reboots from the primary flash using the specified startup-config file. The **filename** argument specifies the startup-config file to use.
- Use the **boot system flash secondary config <filename>** command to override the current policy so that the switch automatically reboots from the secondary flash using the specified startup-config file. The **filename** argument specifies the startup-config file to use.

Reboot configuration policy that uses different startup-config files for different software versions

Suppose that you have the following situation:

- Software release “A” is stored in primary flash and a later software release is stored in secondary flash.
- Memory slot 1 stores a reliable, minimal configuration (named `minconfig`) to be used with the software version in the primary flash.
- Memory slot 2 stores a modified startup-config file (named `newconfig`) to be used with the software version in secondary flash. This startup-config file includes untested changes for improved network operation.

The operator wants to ensure that in case of a need to reboot by pressing the Reset button, or if a power failure occurs, the switch will automatically reboot with the minimal startup-config file in memory slot 1. Since a reboot due to pressing the Reset button or to a power cycle always uses the software version in primary flash, the operator has to configure the switch to always boot from primary flash with the startup-config file named `minconfig` (in memory slot 1). Also, whenever the switch boots from secondary flash, the operator also wants the startup-config named `newconfig` to be used. The following two commands configure the desired behavior.

```
switch(config)# startup-default primary config minconfig
switch(config) # startup-default secondary config newconfig
```

Managing startup-config files in the switch

Managing the startup-config files involves renaming, copying, and erasing startup-config files.

- Use the **rename config <current-filename> <new-filename>** command to change the name of an existing startup-config file. The **current-filename** argument specifies the existing startup-config file and the **new-filename** argument specifies the new name for the file.

A file name can include up to 63, alphanumeric characters. Blanks are allowed in a file name enclosed in quotes (" " or ' '). File names are not case-sensitive.

A file name can include up to 63, alphanumeric characters. Blanks are allowed in a file name enclosed in quotes (" " or ' '). File names are not case-sensitive.

For redundant management systems, renaming a config file affects both the active management module and the standby management module, unless redundancy is disabled or the standby module failed selftest.

- Use the **copy config <source-filename> config <target-filename>** command to create a new startup-config file or to replace an existing startup-config file with a new one.

This command copies the contents of an existing startup-config file in one memory slot to a new startup-config file in another, empty memory slot.

If the target startup-config file already exists, it is overwritten by the content of the source startup-config file otherwise, it will be created in the first empty configuration memory slot on the switch. If the destination startup-config file does not already exist and there are no empty configuration memory slots on the switch, then a new startup-config file is not created.

- Do one of the following to erase any of the startup-config files in the switches memory slots:
 - Use the **erase config <filename>** command to erase the specified startup-config file. `filename` argument specifies the file to be erased.
 - Use the **erase startup-config** command to erase the currently active startup-config file.

In some cases, erasing a file causes the switch to generate a new, default-configuration file for the affected memory slot. Where a file is assigned to either the primary or the secondary flash, but is not the currently active startup config file, erasing the file does not remove the flash assignment from the memory slot for that file. Thus, if the switch boots using a flash location that does not have an assigned startup-config, then the switch creates a new, default startup-config file and uses this file in the reboot. (This new startup-config file contains only the default configuration for the software version used in the reboot.) Executing `write memory` after the reboot causes a switch-generated filename of `config x` to appear in the `show config files` display for the new file, where `x` corresponds to the memory slot number.

In a redundant management system, these commands erase the startup config file on both the active and the standby management modules as long as redundancy has not been disabled. If the standby management module is not in standby mode or has failed selftest, the startup config file is not erased.

The following example shows how to create and assign a new startup config file

If you wanted to experiment with configuration changes to the software version in secondary flash, you could create and assign a separate startup-config file for this purpose, as shown in the following command sequence.

```
switch(config)# copy config config1 config config2
switch(config)# startup-default secondary config config2
switch(config)# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		Config1
2			*	Config2
3				

The following example shows how to erase a non-active startup-config file. The memory configuration has a non-active configuration file named “config3”, which you want to erase.

```
switch(config)# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		minconfig
2			*	config2
3				config3

```
switch(config)# erase config config3
switch(config)# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		minconfig
2			*	config2
3				

Uploading a configuration file to a remote TFTP host

Uploading a configuration file from a remote TFTP host

To upload a configuration file to a remote TFTP host through the out-of-band management interface, do one of the following:

Prerequisites

Before you upload a configuration file to a remote TFTP host, you must insure that the switch has a separate out-of-band management port if the traffic is being transmitted through the out-of-band management interface.

Procedure

1. Use the `copy config <src-file> tftp <ip-addr> <remote-file> pc oobm` command to upload a configuration file to a remote TFTP PC host.

2. Use the `copy config <src-file> tftp <ip-addr> <remote-file> unix oobm` command to upload a configuration file to a remote TFTP UNIX host.

To upload a configuration file to a remote TFTP host through the data interface, do one of the following:

- Use the `copy config <src-file> tftp <ip-addr> <remote-file> pc` command to upload a configuration file to a remote TFTP PC host.
- Use the `copy config <src-file> tftp <ip-addr> <remote-file> unix` command to upload a configuration file to a remote TFTP UNIX host.

For more information on using TFTP to upload a file to a remote server, see "TFTP: Copying a Configuration File to a Remote Host" in Appendix A of the *Management and Configuration Guide* for your switch.

Example

The following command uploads a startup-config file named **test01** from the switch to a (UNIX) TFTP server at IP address 10.10.28.14:

```
switch(config)# copy config test-01 tftp 10.10.28.14 test-01.txt unix
```

Downloading a configuration file from a remote TFTP host

Downloading a configuration file from a remote TFTP host

To download a configuration file from a remote TFTP host through the out-of-band management interface, do one of the following:

Prerequisites

Before you download a configuration file from a remote TFTP host, you must insure that the switch has the following:

- An empty memory slot.
- A separate out-of-band management port, if the traffic is being transmitted through the out-of-band management interface.

Procedure

1. Use the `copy tftp config <dest-file> <ip-addr> <remote-file> pc oobm` command to download a configuration file from a remote TFTP PC host.
2. Use the `copy tftp config <dest-file> <ip-addr> <remote-file> UNIX oobm` command to download a configuration file from a remote TFTP UNIX host.

To download a configuration file from a remote TFTP host through the data interface, do one of the following:

- Use the `copy tftp config <dest-file> <ip-addr> <remote-file> pc` command to download a configuration file from a remote TFTP PC host.
- Use the `copy tftp config <dest-file> <ip-addr> <remote-file> UNIX` command to download a configuration file from a remote TFTP UNIX host.

For more on using TFTP to download a file from a remote host, see "TFTP: Copying a Configuration File from a Remote Host" in Appendix A of the *Management and Configuration Guide* for your switch.

Example

The following command downloads a startup-config file named **test01.txt** from a (UNIX) TFTP server at IP address 10.10.28.14 to the first empty memory slot in the switch:

```
switch(config)# copy tftp config test-01 10.10.28.14 test-01.txt unix
```

Uploading a configuration file to a serially connected host

To upload a configuration file to a serially connected host, do one of the following:

Procedure

1. Use the `copy config <filename> xmodem pc` command to upload a configuration file to a serially connected PC host.
2. Use the `copy config <filename> xmodem unix` command to upload a configuration file to a serially connected UNIX host.

For more on using Xmodem to upload a file to a serially connected host, see "Xmodem: Copying a Configuration File to a Serially Connected PC or UNIX Workstation" in Appendix A of the *Management and Configuration Guide* for your switch.

Downloading a configuration file from a serially connected host

To download a configuration file from a serially connected host, do one of the following:

Procedure

1. Use the `copy xmodem config <dest-file> pc` command to download a configuration file from a serially connected PC host.
2. Use the `copy xmodem config <dest-file> unix` command to download a configuration file from a serially connected UNIX host.

For more on using Xmodem to copy a file from a serially connected host, see "Xmodem: Copying a Configuration File from a Serially Connected PC or UNIX Workstation" in Appendix A of the *Management and Configuration Guide* for your switch.

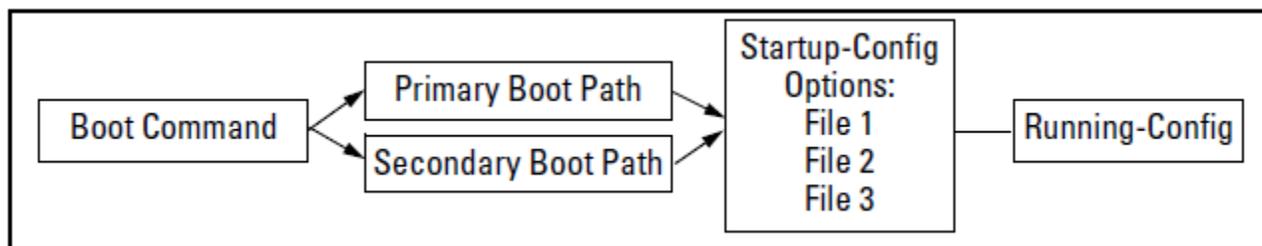
Multiple configuration files

In this mode of operation, you cannot preserve different startupconfig files across a reboot without using remote storage.

The switch allows up to three startup-config files with options for selecting which startup-config file to use for:

- A fixed reboot policy using a specific startup-config file for a specific boot path (primary or secondary flash)
- Overriding the current reboot policy on a per-instance basis

Figure 49: *Optional reboot process*



While you can still use remote storage for startup-config files, you can now maintain multiple startup-config files on the switch and choose which version to use for a reboot policy or an individual reboot.

This choice of which configuration file to use for the startup-config at reboot provides the following new options:

- The switch can reboot with different configuration options without having to exchange one configuration file for another from a remote storage location.
- Transitions from one software release to another can be performed while maintaining a separate configuration for the different software release versions.
- By setting a reboot policy using a known good configuration and then overriding the policy on a per-instance basis, you can test a new configuration with the provision that if an unattended reboot occurs, the switch will come up with the known, good configuration instead of repeating a reboot with a misconfiguration.

Operating notes for multiple configuration files

Multiple configuration storage in the switch. The switch uses three memory "slots", with identity (**id**) numbers of **1**, **2**, and **3**, as shown by the following output of the **show config files** command.

```
switch(config)# show config files
Configuration files:
```

```
id | act pri sec | name
---+-----+-----
 1 |          | oldConfig
 2 | *   *   *   | workingConfig
 3 |          |
```

A startup-config file stored in a memory slot has a unique, changeable file name. The switches covered in this guide can use the startup-config in any of the memory slots (if the software version supports the configured features). In the default configuration, if the switch was shipped from the factory with software installed in both the primary and secondary boot paths, then one startup-config file named "config1" is used for both paths and is stored in memory slot 1. Memory slots 2 and 3 are empty in this default configuration.

An asterisk (*) in the **act**, **pri**, or **sec** column has the following meaning:

- **act** column: The corresponding startup-config file is currently in use.
- **pri** column: The corresponding startup-config file is currently assigned to the primary boot path.
- **sec** column: The corresponding startup-config file is currently assigned to the secondary boot path.

Reboot policy. With multiple startup-config files in the switch you can specify a policy for the switch to use upon reboot. The options include:

- Use the designated startup-config file with either or both reboot paths (primary or secondary flash)
- Override the current reboot policy for one reboot instance by specifying a boot path (primary or secondary flash) and the startup-config file to use.

For a given reboot, the switch automatically reboots from the startup-config file assigned to the flash location (primary or secondary) being used for the current reboot. For example, when you first download a software version that supports multiple configuration files and boot from the flash location of this version, the switch copies the existing startup-config file (named `oldConfig`) into memory slot 2, renames this file to `workingConfig`, and assigns `workingConfig` as:

- The active configuration file
- The configuration file to use when booting from either primary or secondary flash

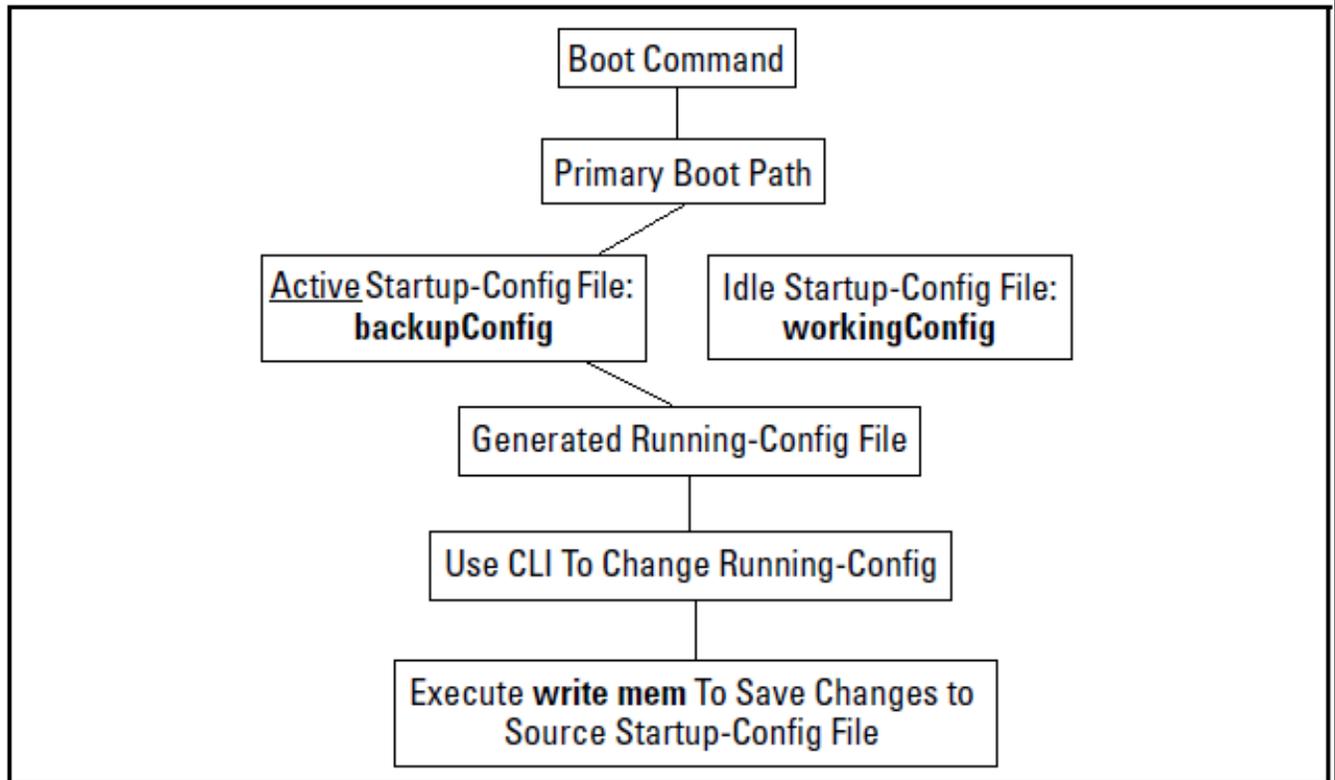
In this case, the switch is configured to automatically use the `workingConfig` file in memory slot 2 for all reboots.

Changes to the startup-config file. When the switch reboots, the startupconfig file supplies the configuration for the running-config file the switch uses to operate. Changes to the running-config file are written back to the startup-config file that was used at the last reboot. The changes are written when the **write-mem** command (or, in the Menu interface, the **Save** command) is executed. For example, suppose that a system administrator performs the following on a switch that has two startup-config files (**workingconfig** and **backupconfig**):

1. Reboot the switch through the Primary boot path using the startup-config file named **backupconfig**.
2. Use the CLI to make configuration changes in the running-config file, and then execute **write-mem**.

The result is that the startup-config file used to reboot the switch is modified by the actions in step 2.

Figure 50: Reboot process and making changes to the startup-config file



An alternate startup-config file. A new configuration file can be created for an alternate startup-config file. There are two methods for creating a new configuration file:

- Copy an existing startup-config file to a new filename, then reboot the switch, make the desired changes to the running-config file, then execute `write memory`.
- Erase the active startup-config file. This generates a new, default startupconfig file that always results when the switch automatically reboots after deletion of the currently active startup-config file.

The transition to multiple configuration files. At the first reboot with a software release supporting multiple configuration, the switch:

- Assigns the filename `oldConfig` to the existing startup-config file (which is stored in memory slot 1).
- Saves a copy of the existing startup-config file in memory slot 2 with the filename `workingConfig`.
- Assigns the `workingConfig` file as the active configuration and the default configuration for all subsequent reboots using either primary or secondary flash.

The following output of the **show config files** command shows the switch memory assignments after the first reboot from software that supports multiple configuration. In this state, the switch always uses the `workingConfig` file to reboot.

```
switch(config)# show config files
Configuration files:

id | act pri sec | name
---+-----+-----+-----+-----
 1 |          |      |      | oldConfig
 2 | *      *   * |      | workingConfig
```

Viewing the configuration of interfaces

Viewing the running configuration of interfaces

To view the running configuration of interfaces, do one of the following:

Procedure

1. Use the `show running-config [structured]` command to view the running configuration of all interfaces. Include the **structured** option to group the information in a logical manner.
2. Use the `show running-config interface port-list` command to view the running configuration of the specified port interfaces. Include the **structured** option to group the information in a logical manner.
3. Use the `show running-config interface loopback <0-7>` command to view the running configuration of the specified loopback interfaces. Include the **structured** option to group the information in a logical manner.
4. Use the `show running-config interface vlan <vlan-id-list>` command to view the running configuration of the specified VLAN interfaces. Include the **structured** option to group the information in a logical manner.

For the 3800 switches, these commands display the following prompt when executed in enhanced secure mode:

```
Do you want to show sensitive information(y/n)?
```

If 'y' is entered, the normal command output is displayed on the console. If 'n' is entered, all the sensitive information is hidden and will be displayed as asterisks ('*****'). The default option is 'n' when interactive mode is disabled. For more information, see the "Secure Mode" in the *Access Security Guide* for your switch.

Examples

The following example shows Running configuration output in preview mode.

```
switch(config)# preview-mode
ATTENTION: You are entering preview mode on this product. This mode, the
commands, features and functionality specific to this mode, and all output
from this mode are Hewlett Packard Enterprise Confidential and Proprietary.
You may use this mode at your own risk. Any defects or issues encountered
in this mode will be addressed per Hewlett Packard Enterprise's discretion.
Continue (y/n)? y
(Prev-mode)switch(config)# show running-config
```

Running configuration:

```
; JL075A Configuration Editor; Created on release #KB.16.01.0000x
; Ver #0c:01.7c.59.f4.7b.ff.ff.fc.ff.ff.3f.ef:

hostname "Aruba-3810M-16SFPP-2s"
module 1 type j1075x
module 2 type j1075y
module 3 type j1075z
snmp-server community "public" unrestricted
oobm
    ip address dhcp-bootp
    exit
vlan 1
```

```
    name "DEFAULT_VLAN"
    untagged 1-16
    ip address dhcp-bootp
    exit
preview-mode
```

The following example shows Running configuration output for interfaces A2 - A4

```
switch(eth-A2-A4)# show running-config
```

Running configuration:

```
; J8698A Configuration Editor; Created on release #K.15.10.0001
; Ver #02:0b:ef:e6
hostname "switch"
interface A2
    disable
    name "test1"
    flow-control
    broadcast-limit 80
    speed-duplex 100-full
    unknown-vlans Block
    qos priority 4
    lacp Passive
    gvrp join-timer 30
    gvrp leave-timer 60
    gvrp leaveall-timer 700
exit
interface A3
    disable name "test1"
    flow-control
    broadcast-limit 80
    speed-duplex 100-full
    unknown-vlans Block
    qos priority 4
    lacp Passive
    gvrp join-timer 30
    gvrp leave-timer 60
    gvrp leaveall-timer 700
exit
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A4,C1-C24,F1-F4
    ip address dhcp-bootp
    exit
interface A2
    dhcp-snooping trust
    bandwidth-min output 20 10 10 10 20 10 10 10
    rate-limit bcast in percent 75
    ipv6 access-group "check" in
    exit
interface A3
    dhcp-snooping trust
    bandwidth-min output 20 10 10 10 20 10 10 10
    rate-limit bcast in percent 75
    ipv6 access-group "check" in
    exit
```

The following example shows an example of the running config for a range of interfaces. The configuration information for interfaces A2 and A3 is now displayed together.

```
switch(config)# show running-config interface A2-A3
```

Running configuration:

```
interface A2
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
interface A3
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
```

The following example shows an example of the running config file for a range of interfaces after some configuration changes have been made.

```
switch(config)# no stack
switch(config)# mesh 2-3
Command will take effect after saving configuration and reboot.
```

```
switch(config)# write memory
switch(config)# reload
```

```
switch# show running-config interface 2-3
```

Running configuration:

```
interface 2
  untagged vlan 1
  mesh
  exit
```

```

interface 3
  flow-control
  untagged vlan 1
  mesh
  exit

```

The following example is an example of the running config output showing VLAN information.

```
switch(config)# show running-config
```

```

Running configuration:
; J8698A Configuration Editor; Created on release #K.15.10.0001
; Ver #02:0b:ef:e6
hostname "switch"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
ip routing
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A4,C1-C24,F1-F24
  ip address dhcp-bootp
  exit
vlan 2
  name "test-vlan-2"
  ip helper-address 4.1.1.1
  ip helper-address 5.1.1.1
  ip address 1.1.1.1 255.255.255.0
  ipv6 address 2001::/64 anycast
  ipv6 enable
  exit
vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address
  exit
vlan 4
  name "VLAN4"
  ip address 5.1.1.1 255.255.255.0
  ip bootp-gateway 5.1.1.1
  exit
logging 10.0.102.90
logging system-module ospf
ip route 5.1.1.0 255.255.255.0 vlan 4 distance 3

```

In the following example, the configuration information for VLAN 4 is now displayed in one place.

```
switch(config)# show running-config vlan 3-4
```

```
Running configuration:
```

```

vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address

```

```

    exit
vlan 4
    name "VLAN4"
    ip address 5.1.1.1 255.255.255.0
    ip bootp-gateway 5.1.1.1
    ip route 5.1.1.0 255.255.255.0 distance 3
    exit

```

Below is an example of the running config for a range of VLANs after configuration changes have been made to selected VLANs.

```

switch(config)# dhcp-snooping
switch(config)# vlan 14
switch(vlan-14)# exit
switch(config)# vlan 15
switch(vlan-15)# exit
switch(config)# vlan 23
switch(vlan-23)# exit
switch(config)# dhcp-snooping vlan 14-15
switch(config)# static-mac 00:11:22:33:44:55 vlan 23 interface A3
switch(config)# spanning-tree instance 2 vlan 15

switch(config)# show running-config vlan 14-15

```

Running configuration:

```

vlan 14
    name "VLAN14"
    no ip address
    dhcp-snooping
    exit
vlan 15
    name "VLAN15"
    no ip address
    dhcp-snooping
    spanning-tree instance 2
    exit

```

Viewing the startup configuration of interfaces

To view the startup configuration of interfaces, do one of the following:

- Use the `show config` command to view the startup configuration of all interfaces.
- Use the `show config interface port-list` command to view the startup configuration of the specified port interfaces.
- Use the `show config interface loopback <0-7>` command to view the startup configuration of the specified VLAN interfaces.

For the 3800 switches, these commands display the following prompt when executed in enhanced secure mode:

```
Do you want to show sensitive information(y/n)?
```

If 'y' is entered, the normal command output is displayed on the console. If 'n' is entered, all the sensitive information is hidden and will be displayed as asterisks ('*****'). The default option is 'n' when interactive mode is disabled. For more information, see the "Secure Mode" in the *Access Security Guide* for your switch.

Examples

The following example shows startup configuration output.

```
switch(config)# show config
```

Startup configuration:

```
; J8698A Configuration Editor; Created on release #K.14.54C
; Ver #02:0b:ef:e6
hostname "switch"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A4,C1-C9,C15-C24,F1-F24
  ip address dhcp-bootp
  no untagged C10-C14
  exit
vlan 5
  name "VLAN5"
  untagged C10-C14
  ip address 5.1.1.1 255.255.255.128
  exit
interface loopback 5
  ip address 7.1.1.1
  exit
interface loopback 7
  ip address 12.1.1.1
  exit
snmp-server community "public" unrestricted
```

Following is an example of the startup config output for a selected VLAN.

```
switch(vlan-5)# show config vlan 5
```

Startup configuration:

```
vlan 5
  name "VLAN5"
  untagged C10-C14
  ip address 5.1.1.1 255.255.255.128
  exit
```

The following shows an example of the startup config output for a range of interfaces for a specific VLAN.

Figure 51: Startup config output for a range of interfaces for a specific VLAN

```
switch(vlan-5)# show config interface C10-C13

Startup configuration:

interface C10
    untagged vlan 5
    exit
interface C11
    untagged vlan 5
    exit
interface C12
    untagged vlan 5
    exit
interface C13
    untagged vlan 5
    exit
```

Using automatic configuration update with DHCP Option 66

Prerequisites

To use automatic configuration update with DHCP Option 66, you must do the following:

- Enable one or more DHCP servers with Option 66.
- Insure that one or more TFTP servers have the desired configuration file.
- Insure that the configuration files to be updated were generated on the switch.
- Enable the configuration file to update with Option 66, as described in [Enabling and disabling the configuration file update using Option 66](#) on page 110.

HPE switches are initially booted up with the factory-shipped configuration file. The automatic configuration update provides a way to automatically download a different configuration file from a TFTP server using DHCP Option 66.

Enabling and disabling the configuration file update using Option 66

Procedure

1. Use the `dhcp config-file-update` command to enable the configuration update using Option 66.
2. Use the `no dhcp config-file-update` command to disable the configuration update using Option 66.

The configuration file update using Option 66 is enabled by default.

Possible scenarios for updating the configuration file

The following table shows various network configurations and how Option 66 is handled.

Scenario	Behavior
Single Server serving Multiple VLANs	<ul style="list-style-type: none"> • Each DHCP-enabled VLAN interface initiates DHCPDISCOVER message, receives DHCPOFFER from the server, and send DHCPREQUEST to obtain the offered parameters. • If multiple interfaces send DHCPREQUESTs, it is possible that more than one DHCPACK is returned with a valid Option 66. • Evaluating and updating the configuration file occurs only on the primary VLAN. • Option 66 is ignored by any interfaces not belonging to the primary VLAN.
Multiple Servers serving a Single VLAN	<ul style="list-style-type: none"> • Each DHCP-enabled VLAN interface initiates one DHCPDISCOVER and receives one or more DHCPOFFER messages. • Each interface accepts the best offer. • Option 66 is processed only for the interface belonging to the primary VLAN.
Multiple Servers serving Multiple VLANs	<ul style="list-style-type: none"> • Each DHSP-enabled VLAN interface initiates DHCPDISCOVER and receives one or more DHCPOFFER messages. • Each interface accepts the best offer. • Option 66 is processed only for the interface belonging to the primary VLAN.
Multi-homed Server serving Multiple VLANs	<ul style="list-style-type: none"> • The switch perceives the multi-homed server as multiple separate servers. • Each DHCP-enabled VLAN interface initiates DHCPDISCOVER and receives one DHCPOFFER message. • Each interface accepts the offer. • Option 66 is processed only for the interface belonging to the primary VLAN.

Operating notes about automatic configuration

Replacing the existing configuration file: After the switch has completed the DHCP transaction on the Primary VLAN, the two options will cause the switch to download the configuration file from the TFTP server. After the DHCP client downloads the configuration file, the switch compares the contents of that file with the existing configuration file. If the content is different, the new configuration file replaces the existing file and the switch reboots.

Option 66 and the IP address of a TFTP server: Option 66 includes the IP address of the TFTP server from which the configuration file is downloaded.

Option 67 and the configuration file name: Option 67 includes the name of the configuration file. If the DHCPACK contains this option, it overrides the default name for the configuration file (switch.cfg)

Global DHCP parameters: Global parameters are processed only if received on the primary VLAN.

Best Offer: The "Best Offer" is the best DHCP or BootP offer sent by the DHCP server in response to the DHCPREQUEST sent by the switch. The criteria for selecting the "Best Offer" are:

- DHCP is preferred over BootP
- If two BootP offers are received, the first one is selected
- For two DHCP offers:
 - The offer from an authoritative server is selected
 - If there is no authoritative server, the offer with the longest lease is selected

Log messages: The file transfer is implemented by the existing TFTP module. The system logs the following message if an incorrect IP address is received for Option 66: "Invalid IP address <ip-address> received for DHCP Option 66".

Overview of switch configuration

Switch configuration involves:

- How switch memory manages configuration changes
- How the CLI implements configuration changes
- How the menu interface and WebAgent implement configuration changes
- How the switch provides software options through primary/secondary flash images
- How to use the switch's primary and secondary flash options, including displaying flash information, booting or restarting the switch, and other topics

Configuration file management

The switch maintains two configuration files, the **running-config** file and the **startup-config** file.

Table 8: Switch memory operation

Running Config File	Startup-config File
Volatile Memory	Flash (Non-Volatile Memory)
Controls switch operation. When the switch boots, the contents of this file are erased and replaced by the contents of the startup-config file. If no configuration changes have been made in the CLI since the switch was last booted, the running-config file is identical to the startup-config file.	Preserves the most recently saved configuration through any subsequent reboot.
CLI configuration changes are written to this file. To use the CLI to save the latest version of the file to the startup-config file, you must execute the write memory command.	
*NOTE: Menu interface configuration changes are simultaneously written to both the running-config and the startup-config file.	

Booting the switch replaces the current running-config file with a new running-config file that is an exact copy of the current startup-config file.



NOTE

Any of the following actions boots the switch:

- Executing the **boot** or the **reload** command in the CLI
- Executing the **boot** command in the menu interface
- Pressing the Reset button on the front of the switch
- Removing, then restoring power to the switch

For more on reboots and the switch's dual-flash images, See [Using Primary and Secondary flash image options](#) on page 88.

Options for saving a new configuration. Making one or more changes to the running-config file creates a new operating configuration. **Saving** a new configuration means to overwrite (replace) the current startup-config file with the current running-config file. This means that if the switch subsequently reboots for any reason, it will resume operation using the new configuration instead of the configuration previously defined in the startup-config file. There are three ways to save a new configuration:

- **In the CLI:**

Use the **write memory** command. This overwrites the current startup-config file with the contents of the current running-config file.

- **In the menu interface:**

Use the **Save** command. This overwrites **both** the running-config file and the startup-config file with the changes you have specified in the menu interface screen.

- **In the WebAgent:**

Click **Save**. This overwrites **both** the running-config file and the startup-config file with the changes you have specified in the WebAgent screen.

Note that using the CLI instead of the menu or WebAgent gives you the option of changing the running configuration without affecting the startup configuration. This allows you to test the change without making it "permanent". When you are satisfied that the change is satisfactory, you can make it permanent by executing the **write memory** command. For example, suppose that you use the following command to disable port 5:

```
switch(config)# interface ethernet 5 disable
```

The above command disables port 5 in the running-config file, but not in the startup-config file. Port 5 remains disabled only until the switch reboots. If you want port 5 to remain disabled through the next reboot, use write memory to save the current running-config file to the startup-config file in flash memory.

```
switch(config)# write memory
```

If you use the CLI to make a configuration change and then change from the CLI to the Menu interface without first using write memory to save the change to the startup-config file, then the switch prompts you to save the change. For example, if you use the CLI to create VLAN 20, and then select the menu interface, VLAN 20 is configured in the running-config file, but not in the startup-config file. In this case you will see:

```
switch(config)# vlan 20
switch(config)# menu
Do you want to save current configuration [y/n]?
```

If you type 'y', the switch overwrites the startup-config file with the running-config file, and your configuration change(s) will be preserved across reboots. If you type 'n', your configuration change(s) will remain only in the running-config file. In this case, if you do not subsequently save the running-config file, your unsaved configuration changes will be lost if the switch reboots for any reason.

Storage and retrieval of configuration files. You can store or retrieve a backup copy of the startup-config file on another device. For more information, see "Transferring Switch Configurations" in the *Management and Configuration Guide* for your switch.

Managing interface access

Listing the current console/serial link configuration

Use the `show console` command to list the current console/serial link configuration.

Use of show console command

This example demonstrates the use of the `show console` command.

```
switch (config)# show console

Console/Serial Link

Inbound Telnet Enabled [Yes] : Yes
Web Agent Enabled [Yes] : Yes

Terminal Type [VT100] : VT100
Screen Refresh Interval (sec) [3] : 3
Displayed Events [All] : All
Baud Rate [speed-sense] : speed-sense
Flow Control [XON/XOFF] : XON/XOFF
Global Session Idle Timeout (sec) [0] : 0
Serial/USB Console Idle Timeout (sec) [not set] : not set
Current Session Idle Timeout (sec) : 0
```

Enabling and disabling inbound Telnet access

In the default configuration, inbound Telnet access is enabled.

Enabling and disabling inbound Telnet access

To enable inbound Telnet access, do one of the following:

Prerequisites

Before you enable or disable inbound Telnet access on a switch, you must insure that the switch has a separate out-of-band management port if you want to use an out-of-band management port for Telnet access. See Appendix I, "Network Out-of-Band Management" in this guide for more information about out-of-band management.

Procedure

1. Use the `telnet-server` command to enable inbound Telnet access through the data ports.
2. Use the following command to enable inbound Telnet access through specific ports: `telnet-server [listen < oobm | data | both >]`
Data ports (**listen data** option), out-of-band management ports (**listen oobm** option), or both data and out-of-band management ports (**listen both**) can be specified.

To disable inbound Telnet access, do one of the following:

- Use the `no telnet-server` command to disable inbound Telnet access through the data ports.
- Use the following command to disable inbound Telnet access through specific ports:

```
no telnet-server [ listen < oobm | data | both > ]
```

Data ports (**listen data** option), out-of-band management ports (**listen oobm** option), or both data and out-of-band management ports (**listen both**) can be specified.

Examples

To disable inbound Telnet access:

```
switch(config)# no telnet-server
```

To re-enable inbound Telnet access:

```
switch(config)# telnet-server
```

Initiating an outbound Telnet session to another device

Initiating an outbound Telnet session to another network device

To initiate an outbound Telnet session, do one of the following:

Prerequisites

Before you initiate an outbound Telnet session to another network device, you must insure that:

- The switch has a separate out-of-band management port, if you want to use an out-of-band management port for the outbound Telnet traffic. See Appendix I, "Network Out-of-Band Management" in this guide for more information about out-of-band management.
- Stacking is enabled, if you want to initiate an outbound Telnet session to a member switch that is a commander in a stack.

Procedure

1. Use the following command to initiate an outbound Telnet session through a data port:

```
telnet <ipv4-addr | ipv6-addr | hostname | switch-num>
```

2. Use the following command to initiate an outbound Telnet session through an out-of-band management port:

```
telnet < ipv4-addr | ipv6-addr | hostname | switch-num > oobm
```

In these commands, the destination device for the outbound Telnet session is specified as an IPv4 address, IPv6 address, hostname, or stack number (1-16) of a member switch.

Examples

If the host "Labswitch" is in the domain abc.com, you can enter the following command and the destination is resolved to "Labswitch.abc.com":

```
switch(config)# telnet Labswitch
```

You can also enter the full domain name of the host in the command:

```
switch(config)# telnet Labswitch.abc.com
```

You can use the **show telnet** command to display the resolved IP address.

Figure 52: *The show telnet command displaying resolved IP addresses*

```
switch(config)# show telnet

Telnet Activity

-----
Session  : ** 1
Privilege: Manager
From     : Console
To       :

-----
Session  : ** 2
Privilege: Manager
From     : 12.13.14.10
To       : 15.33.66.20

-----
Session  : ** 3
Privilege: Operator
From     : 2001:db7:5:0:203:4ff:fe0a:251
To       : 2001:db7:5:0:203:4ff1:fddd:12
```

Web-management interface configuration for idle timeout

An administrator sets the idle timeout for the WebUI management interface and specifies a session timeout page that is displayed to the user when the WebUI management session ends.

Use the following command to configure the Web-management interface for idle timeout:

```
web-management [management-url <URL>] [support-url <URL>] [plaintext] [ssl<TCP-PORT>] [idle-timeout <300-7200>]
```

The following parameters are specified to configure the Web-management interface for idle timeout:

Management-url

Specify URL to load when the [?] button is clicked on the device's web interface.

Support-url

Specify URL to load when the Support tab is clicked on the device's web interface.

Plaintext

Indicates that the http server has to be enabled with no security. If no parameters are specified, `plaintext` is implied. The plaintext server always listens on the well-known port 80.

SSL

Indicates that the http server has to be enabled with Secure Sockets Layer support. TCP port on which the https server must listen for connections. If the TCP port is not specified, the default is port 443.

The `ssl` and `plaintext` variants of the command function independently of each other. Enabling `http+ssl` does not automatically prevent the device from accepting plaintext connections; you must explicitly disable plaintext connections with the command `[no] web-management plaintext`.

Idle-timeout

Specifies the idle timeout for web management sessions. This ranges from 300 seconds to 7200 seconds. The default value is 600 seconds.

The following example shows WebUI Idle timeout

```
switch(config)# web-management
idle-timeout Set the idle timeout for web management sessions.
management-url Specify URL for web interface [?] button.
plaintext Enable or disable the http server (insecure).
ssl Enable or disable the https server (secure).
support-url Specify URL for web interface support page.
switch(config)# web-management idle-timeout
<300-7200> Enter an integer number.
```

Enabling and disabling inbound WebAgent access

In the default configuration, inbound WebAgent (web browser) access, that is, inbound HTTP access, is enabled.

Enabling and disabling inbound WebAgent access

To enable inbound WebAgent access, do one of the following:

Prerequisites

Before you enable or disable inbound WebAgent access on a switch, you must insure that the switch has a separate out-of-band management port if you want to use an out-of-band management port for WebAgent access. See Appendix I, "Network Out-of-Band Management" in this guide for more information about out-of-band management.

Procedure

1. Use the `web-management` command to enable inbound WebAgent access through the data ports.
2. Use the following command to enable inbound WebAgent access through specific ports:

```
web-management [ listen < oobm | data | both > ] Data ports (listen data option), out-of-band management ports (listen oobm option), or both data and out-of-band management ports (listen both) can be specified.
```

To disable inbound WebAgent access, do one of the following:

- Use the `no web-management` command to disable inbound WebAgent access through the data ports.
- Use the following command to disable inbound WebAgent access through specific ports:

```
no web-management [ listen < oobm | data | both > ] Data ports (listen data option), out-of-band management ports (listen oobm option), or both data and out-of-band management ports (listen both) can be specified.
```

Examples

To disable inbound WebAgent access:

```
switch(config)# no web-management
```

To re-enable inbound WebAgent access:

```
switch(config)# web-management
```

Reconfiguring the console/serial link settings

Use the following command to reconfigure the console/serial link settings:

```
console
[terminal <vt100|ansi|none>]
[screen-refresh <1|3|5|10|20|30|45|60>]
[baud-rate <speed-sense|1200|2400|4800|9600|19200|38400|57600|1155200>]
[flow-control <xon/xoff|none>]
[idle-timeout <0-7200>]
```

```
[events [<none>|all|not-info|critical|debug>]
[local-terminal <vt100|none|ansi>]
```

Considerations for setting idle-timeout, baud rate, and flow control settings:

- If the **console idle-timeout** expires, any outbound Telnet or SSH sessions open on the switch are terminated.
- If you change the baud rate or flow control settings, you must make the corresponding changes in your console access device. Otherwise, you may lose connectivity between the switch and your terminal emulator due to differences between terminal and switch settings for these two parameters.

All console parameter changes except **events** require that you save the configuration with **write memory** and then execute **boot** before the new console configuration will take effect.

Switch models supporting redundant management, console settings, such as mode, flow-control, and baud-rate, are the same on both management modules. There cannot be individual settings for each management module.

This example (Executing a series of console commands) shows how to configure the switch with the following:

- VT100 operation
- 19,200 baud
- No flow control
- 600 second (10 minutes) idle timeout
- Critical log events

```
switch(config)# console terminal vt100
This command will take effect after saving the
configuration and rebooting the system.
```

```
switch(config)# console baud-rate 19200
This command will take effect after saving the
configuration and rebooting the system.
```

```
switch(config)# console flow-control none
This command will take effect after saving the
configuration and rebooting the system.
```

```
switch(config)# console idle-timeout 600
switch(config)# console events critical
switch(config)# write memory
switch(config)# reload
```

Software version support of console/serial link settings

In software release versions K.15.12 and greater, the **console inactivity-timer <minutes>** command has been deprecated and replaced by the **console idle-timeout <seconds>** command. As an example:

```
switch(config)#console inactivity-timer 2
```

is now equivalent to:

```
switch(config)#console idle-timeout 120
```

In addition, the serial or USB console idle timeout can be controlled separately if needed. The **console idle-timeout serial-usb seconds** command allows for this behavior. As an example:

```
switch(config)#console idle-timeout 120
switch(config)#console idle-timeout serial-usb 15
```

This sequence of commands will set the Telnet/SSH idle timeout to 120 seconds and the serial-usb idle timeout to 15 seconds. Another example:

```
switch(config)#console idle-timeout 120
switch(config)#console idle-timeout serial-usb 0
```

This sequence of commands will set the Telnet/SSH idle timeout to 120 seconds and the serial-usb idle timeout to 0, or, in other words, to never time out.

The **console inactivity-timer minutes** command will continue to be accepted in version, but it will be converted to the new command format in the running configuration. This command conversion will also happen on a software update to version if the **console inactivity-timer minutes** command was part of the previous configuration.

These settings can be displayed using **show console**.

Interface-access parameters

The interface access in the switch operates properly by default. However, you can modify interface-access parameters to suit your particular needs.

The following table lists the interface-access parameters that are modifiable and their default values. In most cases, the default values are acceptable for standard operation.

Parameter	Default value
Idle-Timeout	10 Minutes (disabled)
Inbound Telnet Access	Enabled
Outbound Telnet Access	n/a
WebAgent Access	Enabled
Terminal type	VT-100
Event Log event types to list (Displayed Events)	All
Baud Rate	Speed Sense
Flow Control	XON/XOFF



Basic switch security is through passwords. You can gain additional security by using the security features described in the *Access Security Guide* for your switch. You can also simply block unauthorized access via the WebAgent or Telnet (as described in this section) and installing the switch in a locked environment.

Terminal line width and length settings

For console/serial link and inbound telnet sessions, the switch output:

- Uses whatever width is set by the terminal program. If width is not specified, 80 characters is the default.
- Automatically wraps on word boundaries (such as spaces) for non-columnar output
- Automatically wraps on column boundaries for columnar output

Hewlett Packard Enterprise recommends that you do not set your terminal width (`terminal width <y>`) above 150 columns. (Windows telnet displays up to 156 characters on 1280 pixelwide display, so 150 is comfortably within this).

Window size negotiation for a telnet session

When a telnet connection is established with a switch, the switch always uses the default values of 80 columns by 24 lines for the window dimensions. The window can be resized by either dragging the corner of the window, or by executing the `terminal length <x> width <y>` CLI command and then configuring the telnet client with those dimensions. The new window dimensions are lost after that telnet session ends.

When the telnet connection is established with a switch, either the switch or the telnet client needs to initiate the inquiry about the availability of NAWS. If NAWS is available, you can resize the window by dragging the corner of the window to the desired size. The telnet software uses NAWS to tell the switch what the new window dimensions are. If the switch supports the requested window dimensions, it uses them for all future interactions. If the switch does not support those window dimensions, it refuses them and the telnet client requests an alternate set of window dimensions. The negotiation continues until the telnet client and the switch agree on the window dimensions.

The switch currently responds to a request from the remote telnet client to negotiate window size. However, some telnet clients do not request to negotiate window size unless the switch's telnet server suggests that NAWS is available.

This feature allows window size negotiation to occur with telnet clients that support NAWS but do not try to use it unless it is suggested by the switch's telnet server. The switch's telnet server will suggest to the telnet client that NAWS is available.

Denying interface access

Use the `kill [<session-number>` command to terminate a currently running remote session. Interface access is denied when a remote session terminates.

The following example shows how to terminate a remote session using the kill command:

The switch supports up to five management sessions. The **show ip ssh** command lists the current management sessions. If you are using the switch's serial port for a console session and want to terminate an active Telnet session, you would do the following:

```

Switch(config)# show ip ssh

SSH Enabled      : Yes                Secure Copy Enabled : No
TCP Port Number  : 22                 Timeout (sec)       : 120
Host Key Type    : RSA                 Host Key Size       : 2048

Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
         rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
MACs     : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

Ses Type   | Source IP           | Port
---|-----+-----|-----|-----
1  console |                     |
2  telnet  |                     |
3  ssh    | 15.30.252.195      | 1531
4  inactive|                     |
5  inactive|                     |
6  inactive|                     |
Switch(config)# kill 2
Switch(config)# show ip ssh

SSH Enabled      : Yes                Secure Copy Enabled : No
TCP Port Number  : 22                 Timeout (sec)       : 120
Host Key Type    : RSA                 Host Key Size       : 2048

Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
         rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
MACs     : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

Ses Type   | Source IP           | Port
---|-----+-----|-----|-----
1  console |                     |
2  inactive|                     |
3  ssh    | 15.30.252.195      | 1531
4  inactive|                     |
5  inactive|                     |
6  inactive|                     |

```

Session 2 is an active Telnet session.

The kill 2 command terminates session 2.

Viewing and setting system information

Viewing system information

Use the `show system information` command to list the current system information.

Examples

This example demonstrates the use of the **show** command to list the current system information.

```

switch# show system information

Status and Counters - General System Information

System Name      : switch

```

```
System Contact      :
System Location     :

MAC Age Time (sec) : 300

Time Zone          : 0
Daylight Time Rule : None
```

Setting system information

Do one of the following to set system information:

Procedure

1. Use the following command to set a plain-language identity for the switch, which helps to distinguish one switch from another:

```
hostname <name-string> snmp-server [contact <system-contact>][location <system-location>]
```

Each field allows up to 255 characters. To help simplify administration, it is recommended that you set **hostname** to a character string that is meaningful within your system.

2. Use the `mac-age-time <10-1000000>`

command to set the MAC age time for learned MAC addresses. The default value is 300 seconds.

The MAC age time corresponds to the MAC Age Interval in the menu interface.

3. Use the following command to set the time zone and daylight-time rule:

```
time timezone <-720 - 840> time daylight-time-rule [ alaska | continental-us-and-canada | middle-europe-and-portugal | southern-hemisphere | western-europe | <user-defined> ]
```

The default daylight-time rule is none. For the time zone: east of the 0 meridian, the sign is "+"; west of the 0 meridian, the sign is "-". For example, the time zone setting for Berlin, Germany is +60 (zone + 1, or 60 minutes) and the time zone setting for Vancouver, Canada is -480 (zone - 8, or -480 minutes).

4. Use the `time [<hh>:<mm>[:<ss>]][<mm>/<dd>/[<yy>]<yy>]` command to set the time and date.

The CLI uses a 24-hour clock scheme; that is, hour (**hh**) values from 1 p.m. to midnight are input as 13 - 24, respectively.

Examples

Example

This example shows the use of the **time** command to set the switch to 9:45 a.m. on November 17, 2012:

```
switch(config)# time 9:45 11/17/12
```

This example shows the use of the **time** command to set the time zone and daylight time rule for Vancouver, Canada:

```
switch(config)# time timezone -480 daylight-time-rule
continental-us-and-canada
```

This example shows the use of the **mac-age-time** command to set the age time to seven minutes:

```
switch(config)# mac-age-time 420
```

This example shows the system information listing after executing the **hostname** command to name the switch "Blue" with "Next-4474" as the system contact, and "North-Data-Room" as the location:

```

=====-- CONSOLE - MANAGER MODE -----
Switch Configuration - Internet (IP) Service

Default Gateway :
Default TTL      : 64

IP Config [DHCP/Bootp] : Manual
IP Address      : 15.30.248.184
Subnet Mask     : 255.255.248.0

Actions->  Cancel   Edit   Save   Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.

```

System parameters

The following table lists the system parameters that are modifiable and their default values. Configuration of system information is optional, but recommended.

System parameter	Default value
System Name	switch product name
System Contact	n/a
System Location	n/a
Time Sync Method	300 seconds
Time Zone	None
Daylight Time Rule	0
Time	None
	January 1, 1990 at 00:00:00 at last power reset

MAC Age Time

Descriptions of the system parameters:

- **System Name:**
Using a unique name helps you to identify individual devices where you are using an SNMP network management tool.
- **System Contact and Location:**
This information is helpful for identifying the person administratively responsible for the switch and for identifying the locations of individual switches.
- **MAC Age Time:**

The number of seconds a MAC address the switch has learned remains in the switch's address table before being aged out (deleted). Aging out occurs when there has been no traffic from the device belonging to that MAC address for the configured interval.

- **Time Sync Method:**

Selects the method (TimeP or SNTP) the switch will use for time synchronization. For more on this topic, see the "Time Protocols" chapter in the latest *Management and Configuration Guide*.

- **Time Zone:**

The number of minutes your time zone location is to the West (+) or East (-) of Coordinated Universal Time (formerly GMT). The default **0** means that no time zone is configured. For example, the time zone for Berlin, Germany is + 60 (minutes) and the time zone for Vancouver, Canada is - 480 (minutes).

- **Daylight Time Rule:**

Specifies the daylight savings time rule to apply for your location. The default is **None**. (For more on this topic, See Appendix D, "Daylight Savings Time on switches.")

- **Time:**

Used in the CLI to specify the time of day, the date, and other system parameters.

Using the menu or WebAgent to configure IP addressing

Using the Switch Setup screen to quickly setup IP addressing

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, Hewlett Packard Enterprise recommends that you use the Switch Setup screen to quickly configure IP addressing.

To use the Switch Setup screen for quickly configuring IP addressing, do one of the following:

Procedure

1. Enter the `setup` command at the CLI Manager level prompt:

```
switch# setup
```

2. Select **8. Run Setup** in the Main Menu of the menu interface.

For more on using the Switch Setup screen, See the *Installation and Getting Started Guide* you received with the switch.

Using the menu to configure IP address, Gateway, and Time-To-Live (TTL)

Procedure

1. From the Main Menu, select:

```
2. Switch Configuration...
```

```
5. IP Configuration
```

2. If multiple VLANs are configured, a screen showing all VLANs appears. The Menu interface displays the IP address for any VLAN. If you use the CLI to configure the IP address on a VLAN, use the CLI **show ip** command to list them.
3. Press **[E]** (for **Edit**).
4. If the switch needs to access a router, for example, to reach off-subnet destinations, select the **Default Gateway** field and enter the IP address of the gateway router.
5. If you need to change the packet Time-To-Live (TTL) setting, select **Default TTL** and type in a value between 2 and 255.
6. To configure IP addressing, select **IP Config** and do one of the following:
 - a. If you want to have the switch retrieve its IP configuration from a DHCP or Bootp server, at the **IP Config** field, keep the value as **DHCP/ Bootp** and go to step 8.
 - b. If you want to manually configure the IP information, use the Space bar to select

Manual

and use the

[Tab]

key to move to the other IP configuration fields.

7. Select the **IP Address** field and enter the IP address for the switch.
8. Select the **Subnet Mask** field and enter the subnet mask for the IP address.
9. Press **[Enter]**, then **[S]**(for **Save**).

More Information

[DHCP/Bootp operation](#) on page 145

Using the WebAgent to configure IP addressing

Using the WebAgent to configure IP addressing

To configure IP addressing on the switch:

Prerequisites

Before you use the WebAgent to configure IP addressing, you must insure the switch has an IP address that is reachable through your network.

Procedure

1. In the navigation pane, click **Home**.
2. Click **Quick Setup**.
3. In the **Switch Quick Setup Parameters** box, click **Change**.
4. Enter the IP address and any other information such as the Subnet mask and Gateway.
5. Click **Save** to save your changes.
6. If you need further information on using the WebAgent, click **[?]** to access the web-based help available for the switch.

Using the CLI to configure IP Addressing, Gateway, and Time-To-Live (TTL)

Viewing the current IP configuration

Do one of the following:

- Use the `show ip` command to view the IP addressing for each VLAN that is configured in the switch.
If only the DEFAULT_VLAN exists, then its IP configuration applies to all ports in the switch. Where multiple VLANs are configured, the IP addressing is listed per VLAN. The display includes switch-wide packet time-to-live, and (if configured) the switch's default gateway and Timep configuration.
- Use the `show management` command to view the IP addressing and time server IP addressing that is configured on the switch.

Examples

The following example shows the switch's default IP addressing. In the factory default configuration (no IP addressing assigned), the switch's IP addressing appears as:

```
switch(config)# show ip  
  
Internet (IP) Service
```

```
IP Routing : Disabled
```

```
Default Gateway :  
Default TTL     : 64  
Arp Age        : 20  
Domain Suffix  :  
DNS server     :
```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP
-----	-----	-----	-----	-----
DEFAULT_VLAN	DHCP/Bootp			Std Local

With multiple VLANs and some other features configured, `show ip` provides additional information. The following example shows IP listing with non-default IP addressing configured

```
switch(config)# show ip
```

```
Internet (IP) Service
```

```
IP Routing : Disabled  
  
Default Gateway : 10.20.227.1  
Default TTL     : 64  
Arp Age        : 20  
Domain Suffix  :  
DNS server     :
```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP
-----	-----	-----	-----	-----
DEFAULT_VLAN	Manual	10.28.227.101	255.255.248.0	No No
VLAN22	Disabled			

Configuring an IP address and subnet mask on a VLAN

Use one of the following forms of the `vlan` command to configure an IP address and subnet mask:

- `vlan <vlan-id> ip address <ip-address>/<mask-length>`
- `vlan <vlan-id> ip address <ip-address> <mask-bits>`
- `vlan <vlan-id> ip address <dhcp-bootp>`

You must either include the ID of the VLAN for which you are configuring IP addressing or go to the context configuration level for that VLAN. (If you are not using VLANs on the switch—that is, if the only VLAN is the default VLAN—then the VLAN ID is always "1".)

The default IP address setting for the `DEFAULT_VLAN` is `DHCP/Bootp`. On additional VLANs you create, the default IP address setting is `disabled`.

Examples

The following example configures IP addressing on the default VLAN with the subnet mask specified in mask bits.

```
switch(config)# vlan 1 ip address 10.28.227.103 255.255.255.0
```

The following example configures the same IP addressing as the preceding example, but specifies the subnet mask by mask length.

```
switch(config)# vlan 1 ip address 10.28.227.103/24
```

Removing an IP address that is configured on a VLAN

Use one of the following forms of the **vlan** command to delete an IP address that is configured on a VLAN:

Procedure

1. no vlan <vlan-id> ip address <ip-address>/<mask-length>
2. no vlan <vlan-id> ip address <ip-address> <mask-bits>

Examples

The following example deletes an IP address configured on VLAN 1.

```
switch (config) no vlan 1 ip address 10.28.227.103/24
```

Multiple IP addresses configuration on a VLAN (multinetting)

Use one of the following forms of the **vlan** command to configure multiple IP addresses on a VLAN (multinetting).

- vlan <vlan-id> ip address <ip-address>/<mask-length>
- vlan <vlan-id> ip address <ip-address> <mask-bits>

The following is supported:

- Up to 2000 IP addresses for the switch.
- Up to 32 IP addresses for the same VLAN
- Up to 512 IP VLANs, that is, VLANs on which you can configure IP addresses
- Each IP address on a VLAN must be for a separate subnet, whether on the same VLAN or different VLANs.

The Internet (IP) Service screen in the Menu interface displays the first IP address for each VLAN. You must use the CLI show ip command to display the full IP address listing for multinetted VLANs.

Configuring and displaying multi netted VLAN

If you wanted to multinet VLAN_20 (VID = 20) with the IP addresses shown below, you would perform steps similar to the following. For this example, assume that the first IP address is already configured.

IP Address	VID	IP Address	Subnet Mask
1st address	20	10.25.33.101	255.255.240.0
2nd address	20	10.26.33.101	255.255.240.0
3rd address	20	10.27.33.101	255.255.240.0

```
switch(config)# vlan 20
switch(vlan-20)# ip address 10.26.33.101/20
switch(vlan-20)# ip address 10.27.33.101/20
```

```
switch(config)# show ip
```

```
Internet (IP) Service
```

```
IP Routing      : Disabled
```

```

Default Gateway : 10.20.227.1
Default TTL     : 64
Arp Age        : 20
Domain Suffix  :
DNS server     :

```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP	Std Local
DEFAULT_VLAN	Manual	10.20.30.100	255.255.240.0	No	No
VLAN_20	Manual	10.25.33.101	255.255.240.0	No	No
	Manual	10.26.33.101	255.255.240.0	No	No
	Manual	10.27.33.101	255.255.240.0	No	No

Multinetting on the default VLAN

To multinette the default VLAN, you would do the following:

```

switch(vlan-20)# vlan 1
switch(vlan-1)# ip address 10.21.30.100/20

```

```

switch(config)# show ip

```

Internet (IP) Service

```

IP Routing      : Disabled

Default Gateway : 10.20.227.1
Default TTL     : 64
Arp Age        : 20
Domain Suffix  :
DNS server     :

```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP	Std Local
DEFAULT_VLAN	Manual	10.20.30.100	255.255.240.0	No	No
	Manual	10.21.30.100	255.255.240.0	No	No
VLAN_20	Manual	10.25.33.101	255.255.240.0	No	No
	Manual	10.26.33.101	255.255.240.0	No	No
	Manual	10.27.33.101	255.255.240.0	No	No

Removing IP addresses from a multinetted VLAN

Use one of the following forms of the **vlan** command to delete an IP address that is configured on a multinetted VLAN:

Procedure

1. no vlan <vlan-id> ip address <ip-address>/<mask-length>
2. no vlan <vlan-id> ip address <ip-address> <mask-bits>

Configuring the optional default gateway

Prerequisites

Before you use the CLI to configure the optional default gateway, you must be at the global configuration level.

One default gateway can be manually assigned to the switch. The switch does **not** allow IP addressing received from a DHCP or Bootp server to replace a manually configured default gateway.

Configuring the optional default gateway

Use the `ip default-gateway <ip-address>` command to configure the optional default gateway:

Examples

The following example shows the configuration of the default gateway with the IP address 10.28.227.115.

```
switch(config)# ip default-gateway 10.28.227.115
```

Setting the Time-To-Live (TTL)

Prerequisites

Before you use the CLI to set the TTL, you must be at the global configuration level.

The Time-To-Live (TTL) is the maximum number of routers (hops) through which a packet can pass before being discarded. Each router decreases a packet's TTL by 1 before forwarding the packet. If a router decreases the TTL to 0, the router drops the packet instead of forwarding it.

Setting the TTL

Use the `ip ttl <number-of-hops>` command to set the TTL. The default value for the TTL is 64 and the range is 2 - 255.

Examples

The following example sets the TTL to 60.

```
switch(config)# ip ttl 60
```

Managing loopback interfaces

Adding a loopback interface



This task is not support by Switch 2530 (J9772A–J9783A) products.

Adding a loopback interface

To add a loopback interface on the switch:

Prerequisites

Before you use the CLI to add a loopback interface, you must be at the global configuration level.

Procedure

1. Use the `interface loopback <number>` command to create the loopback interface. The **number** argument is a value from 1 to 7.
2. Use the `ip address <ip address>` command to configure an IP address for the loopback interface.
3. You can configure up to 32 IP addresses on a loopback interface. You do not need to specify a network mask. A loopback interface uses the default subnet mask 255.255.255.255.

Examples

Figure 53: A loopback interface configured with one IP address

```
switch(config)# interface loopback 1
switch(config)# ip address 10.1.1.1
```

Figure 54: Loopback interfaces configured with multiple IP addresses

This example shows the addition of two loopback interfaces, each with two IP addresses configured.

```
switch(config)# interface loopback 0
switch(lo0)# ip address 172.16.101.8
switch(lo0)# ip address 172.16.101.9
switch(lo0)# exit
switch(config)# interface loopback 1
switch(lo1)# ip address 172.16.102.1
switch(lo1)# ip address 172.16.102.2
```

Removing a loopback interface

Prerequisites

Before you use the CLI to remove a loopback interface, you must be at the global configuration level.



This task is not support by Switch 2530 (J9772A–J9783A) products.

Removing a loopback interface

Use the `no interface loopback <number>` command to remove a loopback interface. The **number** argument is a value from 1 to 7, specifying the loopback interface to be removed.

You cannot remove the default loopback interface (number 0) with IP address 127.0.0.1.

Displaying loopback interface configurations

Do one of the following:

- Use the `show ip` command to display a list of the loopback interfaces, which are sorted according to the loopback number.

The list of loopback interfaces is displayed below other IP configuration parameters, such as packet TTL and ARP age-out values, and VLAN IP configurations. The default loopback interface (

- Use the `show ip route` command to display the loopback interfaces in a list of IP routing entries. The list is sorted according to the destination IP address.

Examples

The following example displays the IP addresses configured for two user-defined loopback interfaces(**lo1** and **lo2**).

```
switch# show ip

IP Routing : Enabled

      Default Gateway : 15.255.128.1
      Default TTL      : 64
```

```

Arp Age      : 20
Domain Suffix :
DNS server   :

```

VLAN	IP Config	IP Address	Subnet Mask	Proxy ARP	Std Local
DEFAULT_VLAN	Manual	10.0.8.121	255.255.0.0	No	No
VLAN2	Manual	192.168.12.1	255.255.255.0	No	No
VLAN3	Disabled				

Loopback	IP Config	Loopback Addresses IP Address	Subnet Mask
lo1	Manual	172.16.110.2	255.255.255.255
lo2	Manual	172.16.112.2	255.255.255.255
lo2	Manual	172.16.114.1	255.255.255.255

The following example displays the configuration of the default loopback interface (**lo0**) and one user-defined loopback interface (**lo2**).

```
switch# show ip route
```

IP Route Entries

Destination	Gateway	VLAN	Type	Sub-Type	Metric	Dist.
10.0.0.0/16	DEFAULT_VLAN	1	connected		1	0
127.0.0.0/8	reject		static		0	0
127.0.0.1/32	lo0		connected		1	0
172.16.10.121/32	lo2		static		1	0
172.16.100.0/24	10.0.8.11	1	ospf	IntraArea	1	1
172.16.102.0/24	VLAN2	2	connected		1	0

Summary of loopback interface configuration

Summary of loopback interface configuration:

- You can configure a loopback interface only from the CLI; you cannot configure a loopback interface from the WebAgent or Menu interface.
- Loopback interfaces share the same IP address space with VLAN configurations. The maximum number of IP addresses supported on a switch is 2048, which includes all IP addresses configured for both VLANs and loopback interfaces (except for the default loopback IP address 127.0.0.1).
- Each IP address that you configure on a loopback interface must be unique in the switch. This means that the address cannot be used by a VLAN interface or another loopback interface.
- For example, if you configure a VLAN with IP address 172.16.100.8/24, you cannot configure a loopback interface with IP address 172.16.100.8. In the same way, if you configure a loopback interface (lo1) with IP address 172.16.101.8, you cannot configure another loopback interface (lo2) with IP address 172.16.101.8.
- You can configure multiple IP addresses on a loopback interface (lo0 to lo7). Up to 32 IP addresses are supported on a loopback interface.

Overview of loopback interfaces

By default, each switch has an internal loopback interface (l00) with the IP address 127.0.0.1. This IP address is used only for internal traffic transmitted within the switch and is not used in packet headers in egress traffic sent to network devices.

You can configure up to seven other loopback interfaces (l01, l02, l03, and so on) on the switch to use to transmit network across the network. Each loopback interface can have multiple IP addresses. Routing protocols, such as RIP and OSPF, advertise the configured loopback addresses throughout a network or autonomous system.

User-defined loopback addresses provide the following benefits:

- A loopback interface is a virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. As a result, a loopback interface is useful for debugging tasks since its IP address can always be pinged if any other switch interface is up.
- You can use a loopback interface to establish a Telnet session, ping the switch, and access the switch through SNMP, SSH, and HTTP (WebAgent).
- A loopback IP address can be used by routing protocols. For example, you can configure the loopback IP address as the router ID used to identify the switch in an OSPF area. Because the loopback interface is always up, you ensure that the switch's router ID remains constant and that the OSPF network is protected from changes caused by downed interfaces.

OSPF does not require that you use an IP address as the router ID. OSPF only requires the router ID to be a unique value within the autonomous system (AS). However, if you configure the loopback IP address as the router ID, OSPF can reach the switch if any switch interface is up. (Normally, OSPF automatically configures the router ID with the IP address of a switch interface. The disadvantage is that if the interface goes down, OSPF can no longer ping the switch using the router ID even if other interfaces are operational.)

For more information about how to configure a loopback IP address to participate in an OSPF broadcast area, see the titled "(Optional) Assigning Loopback Addresses to an Area" in the *Multicast and Routing Guide*.

Retaining VLAN-1 IP addressing across configuration file downloads

Enabling IP preserve to retain VLAN-1 IP addressing

Procedure

1. IP Preserve retains VLAN-1 IP addressing across configuration file downloads.
2. To set up IP Preserve, insert the "ip preserve" at the end of a configuration file, as shown in the following example. Note that you do not execute IP Preserve by entering a command in the CLI.

```
; J9091A Configuration Editor; Created on release #K.15.14.0001
hostname "switch"
time daylight-time-rule None
.
.
.
password manager
password operator
ip preserve
```

Operating rules for IP preserve

When `ip preserve` is entered as the last line in a configuration file stored on a TFTP server:

- If the switch's current IP address for VLAN 1 was not configured by DHCP/ Bootp, IP Preserve retains the switch's current IP address, subnet mask, and IP gateway address when the switch downloads the file and reboots. The switch adopts all other configuration parameters in the configuration file into the startup-config file.
- If the switch's current IP addressing for VLAN 1 is from a DHCP server, IP Preserve is suspended. In this case, whatever IP addressing the configuration file specifies is implemented when the switch downloads the file and reboots. If the file includes DHCP/Bootp as the IP addressing source for VLAN 1, the switch will configure itself accordingly and use DHCP/ Bootp. If instead, the file includes a dedicated IP address and subnet mask for VLAN 1 and a specific gateway IP address, then the switch will implement these settings in the startup-config file.
- The `ip preserve` statement does not appear in `show config` listings. To verify IP Preserve in a configuration file, open the file in a text editor and view the last line.

Overview of IP preserve

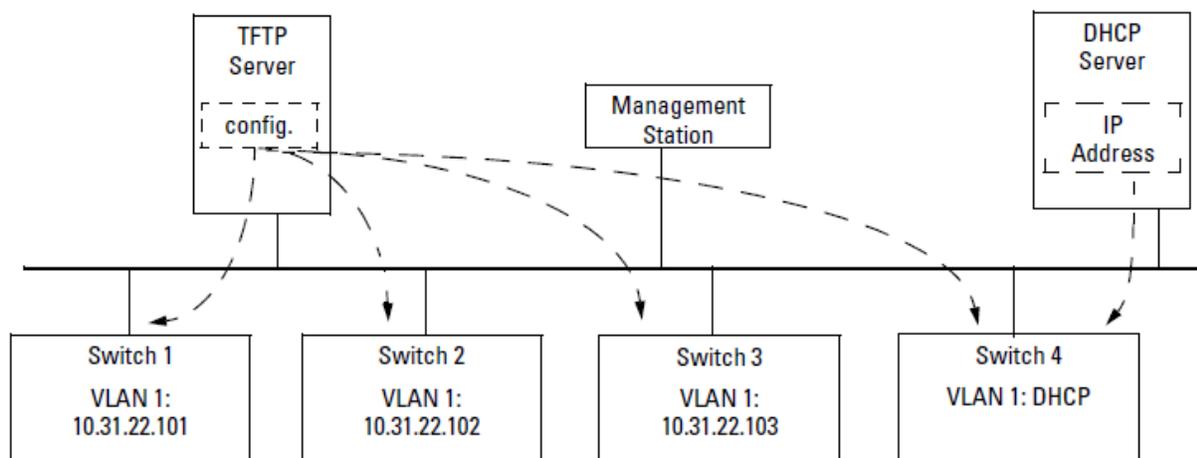
For the switches covered in this guide, IP Preserve enables you to copy a configuration file to multiple switches while retaining the individual IP address and subnet mask on VLAN 1 in each switch, and the Gateway IP address assigned to the switch. This enables you to distribute the same configuration file to multiple switches without overwriting their individual IP addresses.

To summarize the IP Preserve effect on IP addressing:

- If the switch received its most recent VLAN 1 IP addressing from a DHCP/ Bootp server, it ignores the `ip preserve` command when it downloads the configuration file, and implements whatever IP addressing instructions are in the configuration file.
- If the switch did not receive its most recent VLAN 1 IP addressing from a DHCP/Bootp server, it retains its current IP addressing when it downloads the configuration file.
- The content of the downloaded configuration file determines the IP addresses and subnet masks for other VLANs.

The following examples demonstrate the operation of IP Preserve:

Figure 55: Example of IP Preserve operation with multiple series switches



If you apply the following configuration file to the scenario that is shown in **Figure 55: Example of IP Preserve operation with multiple series switches** on page 134, switches 1 - 3 will retain their manually assigned IP addressing and switch 4 will be configured to acquire its IP addressing from a DHCP server.

Configuration file in TFTP server with DHCP/Bootp specified as the IP addressing source

```
switch(config)# show run

Running configuration:

; J9091A Configuration Editor; Created on release #K.15.10.0001

hostname "switch"
module 1 type J8702A
module 2 type J8705A
trunk A11-A12 Trk1 Trunk
ip default-gateway 10.10.10.115
snmp-server community "public" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A10,A13-A24,B1-B24,Trk1
    ip address dhcp-bootp
    exit
spanning-tree Trk1 priority 4
password manager
password operator
```

If you apply the following configuration file to the scenario that is shown in **Figure 55: Example of IP Preserve operation with multiple series switches** on page 134, switches 1 - 3 will still retain their manually assigned IP addressing. However, switch 4 will be configured with the IP addressing included in the file.

Configuration file in TFTP server with dedicated IP addressing, instead of DHCP/Bootp

```
switch# show run

Running configuration:

; J9091A Configuration Editor; Created on release #K.15.10.0001

hostname "switch"
module 1 type J8702A
module 2 type J8705A
trunk A11-A12 Trk1 Trunk
ip default-gateway 10.10.10.115
snmp-server community "public" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged A1,A7-A10,A13-A24,B1-B24,Trk1
    ip address 10.12.17.175 255.255.255.0
    tagged A4-A6
    no untagged A2-A3
    exit
vlan 2
    name "VLAN2"
    untagged A2-A3
    no ip address
    exit
spanning-tree Trk1 priority 4
password manager
password operator
```

Configuring a single source IP address for software applications

Specifying the source IP address

Only one source IP address can be specified for each software application.

Do one of the following:

- Use the following command to specify the source IP address for the specified software application.

```
ip source-interface  
< radius | sflow | snmp | syslog | tacacs | telnet | tftp >  
< loopback <id> | vlan <vlan-id> | address <ip-address> >
```

- Use the following command to specify the source IP address for all software applications.

```
ip source-interface all  
< loopback <id> | vlan <vlan-id> | address <ip-address> >
```

- **loopback <id> :**

Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.

- **vlan <vlan-id> :**

Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.

- **address <ip-address> :**

Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.

Canceling the source IP address assignment

When the source IP address assignment for a software application is canceled, the application reverts to its default behavior and the system determines the source IP address of outgoing application-specific IP packets at packet transmission time.

Do one of the following:

- Use the following command to cancel the source IP address assignment for the specified software application.

```
no ip source-interface  
< radius | sflow | snmp | syslog | tacacs | telnet | tftp >
```

- Use the following command to cancel the source IP address assignment for all software applications.

```
no ip source-interface all
```

Viewing source IP address configurations

Do one of the following:

- Use the following command to view the source IP address configuration for the specified protocol.

```
show ip source-interface  
[ radius | sflow | snmp | tacacs | telnet | tftp | syslog ]
```

- Use the following command to view the source IP address configuration for all protocols.

```
show ip source-interface
```

Examples

The following example shows a specific IP address assigned for the RADIUS application protocol

```
switch(config)# ip source-interface radius address 10.10.10.2
```

```
switch(config)# show ip source-interface radius
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Radius	Configured IP Address	vlan 3	10.10.10.2

The following example shows a VLAN interface assigned as the source IP address for the TACACS application protocol

```
switch(config)# ip source-interface tacacs vlan 22
```

```
switch(config)# show ip source-interface tacacs
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Tacacs	Configured IP Interface	vlan 22	10.10.10.4

The following example shows Source IP address configurations for all application protocols

```
switch(config)# show ip source-interface
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Tacacs	Configured IP Interface	vlan 22	
Radius	Configured IP Address		10.10.10.2
Syslog	Configured IP Interface	vlan 10	
Telnet	Outgoing Interface		
Tftp	Outgoing Interface		
Sntp	Outgoing Interface		
Sflow	Outgoing Interface		

Viewing source IP selection policy status

Do one of the following:

- Use the following command to view the source IP selection policy status for the specified protocol.

```
show ip source-interface status  
[ radius | sflow | sntp | tacacs | telnet | tftp | syslog ]
```

- Use the following command to view the source IP selection policy status for all protocols.

```
show ip source-interface status
```

The following example shows Source IP selection policy status for all application protocols

```
switch(config)# show ip source-interface status
```

Source-IP Status Information

Protocol	Admin Selection Policy	Oper Selection Policy
Tacacs	Configured IP Interface	Configured IP Interface
Radius	Configured IP Address	Configured IP Address
Syslog	Configured IP Interface	Outgoing Interface
Telnet	Outgoing Interface	Outgoing Interface
Tftp	Outgoing Interface	Outgoing Interface
Sntp	Outgoing Interface	Outgoing Interface
Sflow	Configured IP Address	Configured IP Address

More Information

[The source IP selection policy](#) on page 141

Viewing full source IP details

The full source IP details for an application protocol include the source IP selection policy status, the source IP address configuration, and the state of the source IP interface.

Do one of the following:

- Use the following command to view the full source IP details for the specified protocol.

```
show ip source-interface detail  
[ radius | sflow | sntp | tacacs | telnet | tftp | syslog ]
```

- Use the following command to view the full source IP details for all protocols.

```
show ip source-interface detail
```

Examples

The following example shows detailed information displayed for the Tacacs application protocol.

```
switch(config)# show ip source-interface detail tacacs
```

Source-IP Detailed Information

```
Protocol : Tacacs  
Admin Policy      : Configured IP Interface  
Oper Policy       : Outgoing Interface  
Source IP Interface : Vlan 22  
Source IP Address  : 10.10.10.4  
Source Interface State : Down
```

The following example shows detailed information displayed for each application protocol.

```
switch(config)# show ip source-interface detail
```

Source-IP Detailed Information

```
Protocol : Tacacs  
Admin Policy      : Configured IP Interface  
Oper Policy       : Configured IP Interface  
Source IP Interface : vlan 22  
Source IP Address  : 10.10.10.4  
Source Interface State : Up
```

```

Protocol : Radius
Admin Policy      : Configured IP Address
Oper Policy      : Configured IP Address
Source IP Interface : vlan 3
Source IP Address : 10.10.10.2
Source Interface State : Up

Protocol : Syslog
Admin Policy      : Configured IP Interface
Oper Policy      : Configured IP Interface
Source IP Interface : vlan 10
Source IP Address : 10.10.10.10
Source Interface State : Up

Protocol : Telnet
Admin Policy      : Configured IP Interface
Oper Policy      : Configured IP Interface
Source IP Interface : loopback 1
Source IP Address : 10.10.10.11
Source Interface State : Up

Protocol : Tftp
Admin Policy      : Outgoing Interface
Oper Policy      : Outgoing Interface
Source IP Interface : N/A
Source IP Address : N/A
Source Interface State : N/A

Protocol : Sntp
Admin Policy      : Outgoing Interface
Oper Policy      : Outgoing Interface
Source IP Interface : N/A
Source IP Address : N/A
Source Interface State : N/A

Protocol : Sflow
Admin Policy      : Outgoing Interface
Oper Policy      : Outgoing Interface
Source IP Interface : N/A
Source IP Address : N/A
Source Interface State : N/A

```

Viewing protocol configuration and status information

Use the following command to view configuration and status information for the specified application protocol. The displayed information includes the operational source IP selection policy.

```
show [ radius | sflow | sntp | tacacs | telnet | tftp | syslog ]
```

Examples

The following example shows the details for the Radius application protocol

```

switch(config)# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0

```

```
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :
Dynamic Authorization UDP Port : 3799
Source IP Selection : Configured IP address
```

The following example shows the details for the Telnet application protocol

```
switch(config)# show telnet

Telnet Activity

Source IP Selection: 10.10.10.11

-----
Session   : ** 1
Privilege: Manager
From      : Console
To        :
```

The following example shows details for the SNTP application protocol

```
switch(config)# show sntp

SNTP Configuration

SNTP Authentication : Disabled
Time Sync Mode: Timep
SNTP Mode : disabled
Poll Interval (sec) [720] : 720
Source IP Selection: Outgoing Interface
```

Configuration error messages

The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.

Overview of single source IP addresses for software applications

A single source IP address can be configured for the following software applications:

- RADIUS
- SFlow
- SNMP
- System Logging applications
- TACACS
- Telnet
- TFTP

The above IP-based software applications use a client-server communication model, that is, the client's source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

The source IP selection policy

The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- **Outgoing Interface**—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.
- **Configured IP Address**—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- **Configured IP Interface**—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed.

The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy, as shown in the following example.

The administratively-assigned source IP selection policy differing from the operational policy

```
switch(config)# show ip source-interface detail tacacs
```

```
Source-IP Detailed Information
```

```
Protocol : Tacacs
Admin Policy           : Configured IP Interface
Oper Policy            : Outgoing Interface
Source IP Interface    : Vlan 22
Source IP Address      : 10.10.10.4
Source Interface State : Down
```

Below is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

A specific IP address assigned for the RADIUS application protocol

```
switch(config)# ip source-interface radius address 10.10.10.2
```

```
switch(config)# show ip source-interface radius
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Radius	Configured IP Address	vlan 3	10.10.10.2

In the example below, a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

Using a VLAN interface as the source IP address for TACACS

```
switch(config)# ip source-interface tacacs vlan 22
```

```
switch(config)# show ip source-interface tacacs
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Tacacs	Configured IP Interface	vlan 22	10.10.10.4

The next example shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

Using a VLAN interface as the source IP Address for logging (Syslog)

```
switch(config)# ip source-interface syslog vlan 10
```

```
switch(config)# show ip source-interface syslog
```

```
Source-IP Configuration Information
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Syslog	Configured IP Interface	vlan 10	10.10.10.10

More Information

[Viewing source IP selection policy status](#) on page 137

IP configuration features

IP configuration features:

Feature	Default
IP Address and Subnet Mask	DHCP/Bootp
Multiple IP Addresses on a VLAN	n/a
Default Gateway Address	none
Packet Time-To-Live (TTL)	64 seconds
Time Server (Timep) ¹	DHCP
Single Source IP Addressing	outgoing IP address

¹ For more on this topic, see the "Time Protocols" chapter in the latest *Management and Configuration Guide*.

IP address and subnet mask. Configuring the switch with an IP address expands your ability to manage the switch and use its features. By default, the switch is configured to automatically receive IP addressing on the default VLAN from a DHCP/Bootp server that has been configured correctly with information to support the switch. (See **DHCP/Bootp operation** on page 145 for information on setting up automatic configuration from a server.) However, if you are not using a DHCP/Bootp server to configure IP addressing, use the menu interface or the CLI to manually configure the initial IP values. After you have network access to a device, you can use the WebAgent to modify the initial IP configuration if needed.

For information on how IP addressing affects switch operation, See **Effects of IP addressing on switch operation** on page 143.

Multinetting: assigning multiple IP addresses to a VLAN. For a given VLAN you can assign up to 32 IP addresses. This allows you to combine two or more subnets on the same VLAN, which enables devices in the combined subnets to communicate normally through the network without needing to reconfigure the IP addressing in any of the combined subnets.

Default gateway operation. The default gateway is required when a router is needed for tasks such as reaching off-subnet destinations or forwarding traffic across multiple VLANs. The gateway value is the IP address of the next-hop gateway node for the switch, which is used if the requested destination address is not on a local subnet/VLAN. If the switch does not have a manually-configured default gateway and DHCP/Bootp is configured on the primary VLAN, then the default gateway value provided by the DHCP or Bootp server will be used. If the switch has a manually configured default gateway, then the switch uses his gateway, even if a different gateway is received via DHCP or Bootp on the primary VLAN. This is also true for manually configured TimeP, SNTP, and Time-To-Live(TTL). (In the default configuration, VLAN 1 is the Primary VLAN.)

For more information on Primary VLANs, see the *Advanced Traffic Management Guide*.

For more information on TimeP and SNTP, see the "Time Protocols" chapter in the *Management and Configuration Guide*.

Packet Time-To-Live (TTL). This parameter specifies the maximum number of routers (hops) through which a packet can pass before being discarded. Each router decreases a packet's TTL by 1 before forwarding the packet. If decreasing the TTL causes the TTL to be 0, the router drops the packet instead of forwarding it. In most cases, the default setting (64) is adequate.

Effects of IP addressing on switch operation

Without an IP address and subnet mask compatible with your network, the switch can be managed only through a direct terminal device connection to the Console RS-232 port. You can use direct-connect console access to take advantage of features that do not depend on IP addressing. However, to realize the full capabilities HPE proactive networking offers through the switch, configure the switch with an IP address and subnet mask compatible with

your network. The following table lists the general features available with and without a network-compatible IP address configured.

Table 9: Features available with and without IP addressing on the switch

Features available without an IP Address	Additional features available with an IP Address and subnet mask
<ul style="list-style-type: none"> • Direct-connect access to the CLI and the menu interface • DHCP or Bootp support for automatic IP address configuration, and DHCP support for automatic Timep server IP address configuration • Multiple Spanning Tree Protocol • Port settings and port trunking • Switch meshing • Console-based status and counters information for monitoring switch operation and diagnosing problems through the CLI or menu interface • VLANs and GVRP • Serial downloads of software updates and configuration files (Xmodem) • Link test • Port monitoring • Password authentication • Quality of Service (QoS) • Authorized IP manager security 	<ul style="list-style-type: none"> • WebAgent access, with configuration, security, and diagnostic tools, plus the Alert Log for discovering problems detected in the switch along with suggested solutions • SNMP network management access for network configuration, monitoring, problem-finding, and reporting, analysis, and recommendations for changes to increase control and uptime • TACACS+, RADIUS, SSH, SSL, and 802.1X authentication • Multinetting on VLANs • Telnet access to the CLI or the menu interface • IGMP • TimeP and SNTP server configuration¹ • TFTP download of configurations and software updates • Access Control Lists (ACLs) • IP routing, Multicast Routing • VRRP router redundancy • PIM-DM and PIM-SM • Radius • Ping test

¹ For more information on TimeP and SNTP, see the “Time Protocols” chapter in the *Management and Configuration Guide*.

Network preparations for configuring DHCP/Bootp

In its default configuration, the switch is configured for DHCP/Bootp operation. However, the DHCP/Bootp feature will not acquire IP addressing for the switch unless the following tasks have already been completed:

- For Bootp operation
 - A Bootp database record has already been entered into an appropriate Bootp server
 - The necessary network connections are in place
 - The Bootp server is accessible from the switch
- For DHCP operation
 - A DHCP scope has been configured on the appropriate DHCP server
 - The necessary network connections are in place
 - A DHCP server is accessible from the switch



Designating a primary VLAN other than the default VLAN affects the switch’s use of information received via DHCP/Bootp. For more on this topic, See the describing VLANs in the *Advanced Traffic Management Guide* for your switch.

After you reconfigure or reboot the switch with DHCP/Bootp enabled in a network providing DHCP/Bootp service, the switch does the following:

- Receives an IP address and subnet mask and, if configured in the server, a gateway IP address and the address of a Tftp server.
- If the DHCP/Bootp reply provides information for downloading a configuration file, the switch uses TFTP to download the file from the designated source, then reboots itself. (This assumes that the switch or VLAN has connectivity to the TFTP file server specified in the reply, that the configuration file is correctly named, and that the configuration file exists in the TFTP directory.)

Overview of IP Addressing

You can configure IP addressing through all the switch's interfaces. You can also:

- Easily edit a switch configuration file to allow downloading the file to multiple switches without overwriting each switch's unique gateway and VLAN 1 IP addressing.
- Assign up to 32 IP addresses to a VLAN (multinetting).
- Select an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

Why configure IP addressing? In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by the ports on the switch. However, to enable specific management access and control through your network, you will need IP addressing. **Effects of IP addressing on switch operation** on page 143 shows the switch features that depend on IP addressing to operate.

IP addressing with multiple VLANs

In the factory default configuration, the switch has one, permanent default VLAN (named DEFAULT_VLAN) that includes all ports on the switch. Thus, when only the default VLAN exists in the switch, if you assign an IP address and subnet mask to the switch, you are actually assigning the IP addressing to the DEFAULT_VLAN.



- If multiple VLANs are configured, then each VLAN can have its own IP address. This is because each VLAN operates as a separate broadcast domain and requires a unique IP address and subnet mask. A default gateway (IP) address for the switch is optional, but recommended.
- In the factory default configuration, the default VLAN (named DEFAULT_VLAN) is the switch's **primary** VLAN. The switch uses the primary VLAN for learning the default gateway address. The switch can also learn other settings from a DHCP or Bootp server, such as (packet) Time-To-Live (TTL), and Tftp or SNMP settings. (Other VLANs can also use DHCP or BootP to acquire IP addressing. However, the switch's gateway, TTL, and Tftp or SNMP values, which are applied globally, and not per-VLAN, will be acquired through the primary VLAN only, unless manually set by using the CLI, Menu, or WebAgent. (If these parameters are manually set, they will **not** be overwritten by alternate values received from a DHCP or Bootp server.) For more on VLANs, see the titled "Static Virtual LANs" in the *Advanced Traffic Management Guide* for your switch.
- The IP addressing used in the switch must be compatible with your network. That is, the IP address must be unique and the subnet mask must be appropriate for your IP network.
- If you change the IP address through either Telnet access or the WebAgent, the connection to the switch will be lost. You can reconnect by either restarting Telnet with the new IP address or entering the new address as the URL in your web browser.

DHCP/Bootp operation

Overview. DHCP/Bootp is used to provide configuration data from a DHCP or Bootp server to the switch. This data can be the IP address, subnet mask, default gateway, Tftp Server address, and TFTP server address. If a TFTP server address is provided, this allows the switch to TFTP a previously saved configuration file from the

TFTP server to the switch. With either DHCP or Bootp, the servers must be configured prior to the switch being connected to the network.



The switches covered in this guide are compatible with both DHCP and Bootp servers.

The DHCP/Bootp process. Whenever the `IP Config` parameter in differences the switch or in an individual VLAN in the switch is configured to `DHCP/Bootp` (the default), or when the switch is rebooted with this configuration:

1. DHCP/Bootp requests are automatically broadcast on the local network. (The switch sends one type of request to which either a DHCP or Bootp server can respond.)
2. When a DHCP or Bootp server receives the request, it replies with a previously configured IP address and subnet mask for the switch. The switch also receives an IP Gateway address if the server has been configured to provide one. In the case of Bootp, the server must first be configured with an entry that has the switch's MAC address. (To determine the switch's MAC address, See Appendix D, "MAC Address Management".) The switch properly handles replies from either type of server. If multiple replies are returned, the switch tries to use the first reply.)



If you manually configure default gateway, TTL, TimeP, and/or SNTP parameters on the switch, it ignores any values received for the same parameters via DHCP or Bootp.

If the switch is initially configured for DHCP/Bootp operation (the default), or if it reboots with this configuration, it begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to restart the process immediately.

DHCP operation. A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic. Depending on how the DHCP server is configured, the switch may receive an IP address that is temporarily leased. Periodically the switch may be required to renew its lease of the IP configuration. Thus, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. However, you can fix the address assignment for the switch by doing either of the following:

- Configure the server to issue an "infinite" lease.
- Using the switch's MAC address as an identifier, configure the server with a "Reservation" so that it will always assign the same IP address to the switch. (For MAC address information, See Appendix D, "MAC Address Management".)

For more information on either of these procedures, See the documentation provided with the DHCP server.

Bootp operation. When a Bootp server receives a request, it searches its Bootp database for a record entry that matches the MAC address in the Bootp request from the switch. If a match is found, the configuration data in the associated database record is returned to the switch. For many Unix systems, the Bootp database is contained in the `/etc/bootptab` file. In contrast to DHCP operation, Bootp configurations are always the same for a specific receiving device. That is, the Bootp server replies to a request with a configuration previously stored in the server and designated for the requesting device.

Bootp Database Record Entries. A minimal entry in the Bootp table file `/etc/bootptab` to update an IP address and subnet mask to the switch or a VLAN configured in the switch would be similar to this entry:

```
8212switch:\
  ht=ether:\
  ha=0030c1123456:\
  ip=10.66.77.88:\
  sm=255.255.248.0:\
```

```
gw=10.66.77.1:\
hn:\
vm=rfc1048
```

An entry in the Bootp table file `/etc/bootptab` to tell the switch or VLAN where to obtain a configuration file download would be similar to this entry:

```
8212switch:\
  ht=ether:\
  ha=0030c1123456:\
  ip=10.66.77.88:\
  sm=255.255.248.0:\
  gw=10.66.77.1:\
  lg=10.22.33.44:\
  T144="switch.cfg":\
  vm=rfc1048
```

where:

8212switch	is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you must use a unique symbolic name for each switch.
ht	is the "hardware type". For the switches covered in this guide, enter <code>ether</code> (for Ethernet). This tag must precede the ha tag.
ha	is the "hardware address". Use the switch's (or VLAN's) 12-digit MAC address.
ip	is the IP address to be assigned to the switch (or VLAN).
sm	is the subnet mask of the subnet in which the switch (or VLAN) is installed.
gw	is the IP address of the default gateway.
lg	TFTP server address (source of final configuration file)
T144	is the vendor-specific "tag" identifying the configuration file to download.
vm	is a required entry that specifies the Bootp report format. Use <code>rfc1048</code> for the switches covered in this guide.



The above Bootp table entry is a sample that will work for the switch when the appropriate addresses and file names are used.

More Information

[Using the menu to configure IP address, Gateway, and Time-To-Live \(TTL\)](#) on page 125

Viewing or downloading the software manual set

Procedure

1. Go to the Networking website <http://www.hpe.com/networking/support> to view or download product documentation.

Updating the switch software to a new version

Updating the switch software

Process overview:

Procedure

1. Go to the Networking website (<http://www.hpe.com/networking/support>) to download the new switch software file.

HPE periodically provides switch software updates through the Networking website. Check the website frequently for the latest software version available for your switch.

2. Review the **Best practices, recommendations, and precautions** on page 152.
3. Backup your configuration, as specified in **Backing up your current configuration and image** on page 149.
4. Do one of the following to download and install the new switch software:
 - a. For a TFTP transfer from a server, do either of the following:
 - Select **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option. For more information about using the switch's menu interface, see **Using the Menu Interface** on page 19.
 - In the switch's CLI, complete the **Downloading and installing software from a TFTP server** on page 150 task. Use the **copy tftp** command in the switch's CLI (see below).
 - b. For an Xmodem transfer from a PC or Unix workstation, do either of the following:
 - Select **Download OS** in the Main Menu of the switch's menu interface and select the **XMODEM** option. For more information about using the switch's menu interface, see **Using the Menu Interface** on page 19.
 - In the switch's CLI, complete the **Downloading and installing software from a PC or Unix workstation** on page 150 task.
 - c. For a transfer from a USB flash drive: In the switch's CLI, complete the **Downloading and installing software from a USB flash drive** on page 151 task.



Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, to archive or to be used in another switch of the same model.

Backing up your current configuration and image

Procedure

1. Save your current configuration (Config1) to backup configuration file (Config2).
 - a. Before copying the config, verify the current state of your system using the **show version**, **show flash** and **show config files** commands. For example:

```
Switch1# show version
Image stamp:   /sw/code/build/btm(t4a)
               Nov 6 2009 13:20:26
               K.14.47
               188
Boot Image:    Primary

Switch1# show flash
Image          Size(Bytes)   Date      Version
-----
Primary Image  : 9839140     11/06/09 K.14.47
Secondary Image : 0
Boot Rom Version: K.12.20
Default Boot   : Primary

Switch1# show config files

Configuration files:

 id | act pri sec | name
-----
  1 | *   *   *   | config1
  2 |     |     |
  3 |     |     |
```

- b. Create a backup configuration file and verify the change.

```
Switch1# copy config config1 config config2
Switch1# show config files

Configuration files:

 id | act pri sec | name
-----
  1 | *   *   *   | config1
  2 |     |     | config2
  3 |     |     |
```

2. Save the current config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60
Switch1_config_K_14_47.cfg
```



This step is necessary because switches do not support roll back (going from a newer software version to an older software version) without the ability to copy a backup config file onto the device.

3. Back up your current running image (primary) to the secondary image.

```
Switch1# copy flash flash secondary

Switch1# show flash
Image          Size(Bytes)   Date      Version
-----
Primary Image  : 9839140     11/06/09 K.14.47
Secondary Image : 9839140     11/06/09 K.14.47
```

```
Boot Rom Version: K.12.20
Default Boot      : Primary
```

4. Set your secondary image to boot with Config2.

```
Switch1# startup-default secondary config config2
Switch1# show config files
Configuration files:

```

id	act	pri	sec	name
1	*	*		config1
2			*	config2
3				

This step will enable you to revert from the new software version to your previous software version (K.14.47 in the examples shown in steps 1 through 3) with your previous configuration just by invoking the command **boot system flash secondary**.

Downloading and installing software from a TFTP server

Procedure

1. Use the following command, specifying the filename and the primary or secondary flash destination:

```
copy tftp flash <ip-address> <remote-os-file> [ primary | secondary ]
```

Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named K_15_10_0001.swi from a TFTP server with the IP address of 10.28.227.103 to the primary flash destination, execute the **copy** command as shown below:

```
switch# copy tftp flash 10.28.227.103 K_15_10_0001.swi
The primary OS image will be deleted. continue
continue[y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message

```
Validating and Writing System Software to FLASH...
```

3. When the CLI prompt reappears, the switch is ready to reboot to activate the downloaded software:

- a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary).
- b. Reboot the switch from the flash area (primary or secondary) that holds the new software, using the following command:

```
boot system flash [ primary | secondary ]
```

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the Software revision field.

Downloading and installing software from a PC or Unix workstation

Downloading and installing software from a PC or Unix workstation

To download software from a PC or Unix workstation:

Prerequisites

Before you download and install software from a PC or Unix workstation, insure that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (See your switch *Installation and Getting Started Guide* for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with most Windows systems, the Send File option in the Transfer drop-down menu supports the Xmodem protocol.)

Procedure

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 115,200 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 115200, execute this command:

```
switch(config)# console baud-rate 115200
```

(If you use this option, be sure to set your terminal emulator to the same baud rate.)

Changing the console baud-rate requires saving to the Startup Config with the **write memory** command. Alternatively, you can log out of the switch and change your terminal emulator speed and allow the switch to Auto-Detect your new higher baud rate (that is, 115,200 bps)

2. Use the following CLI command, specifying the primary or secondary flash destination:

```
copy xmodem flash [ primary | secondary ]
```

For example, the following command specifies the primary flash destination:

```
switch# copy xmodem flash primary
The primary OS image will be deleted. continue [y/n]? Y
Press 'Enter' and start XMODEM on your host...
```

3. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
 - a. Click **Transfer**, then **Send File**.
 - b. Type the file path and name in the **Filename** field.
 - c. In the Protocol field, select **Xmodem**.
 - d. Click **Send** button.

The download can take several minutes, depending on the baud rate used in the transfer.

4. If you increased the baud rate on the switch (1), use the same command to return it to its previous setting. (A baud rate of 9600 bits per second is recommended for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.
5. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary).
6. Reboot the switch from the flash area (primary or secondary) that holds the new software, using the following command:

```
boot system flash [ primary | secondary ]
```

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

Downloading and installing software from a USB flash drive

Downloading and installing software from a USB flash drive

To download software from a USB flash drive:

Prerequisites

Before you download and install software from a USB flash drive, insure that:

- The software version is stored on the USB flash drive and you know the file name (such as K_15_10_0001.swi).
- The USB flash drive is properly installed in the USB port on the switch.
- The USB flash drive is supported. Some USB flash drives may not be supported on your switch. For information on USB device compatibility, see the networking support (<http://www.hpe.com/networking/support>).

Procedure

1. Use the following CLI command, specifying the filename and the primary or secondary flash destination:

```
copy usb flash <filename> [ primary | secondary ]
```

For example, to download a software file named K_15_10_0001.swi from a USB flash drive to the secondary flash destination, execute the command as shown below:

```
switch# copy usb flash K_15_10_0001.swi secondary
The secondary OS image will be deleted. continue
[y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message:

```
Validating and Writing System Software to FLASH...
```

3. When the CLI prompt reappears, the switch is ready to reboot to activate the downloaded software:

- a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary).
- b. Reboot the switch from the flash area (primary or secondary) that holds the new software, using the following command:

```
boot system flash [ primary | secondary ]
```

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the Software revision field.

Best practices, recommendations, and precautions

Best practices for software updates



There is a slight change in the versioning system.

Software updates that contain significant new features and enhancements may be designated by an increment to both the major and minor release version numbers. That is, K.15.01.0031 represents a major update to software version(s) K.14.xx, and K.14.xx represents a major update to K.13.xx, and so forth. In addition, a future version (such as K.15.02.xxxx) may represent a minor release to version K.15.01.xxxx, but may still contain significant changes. To mitigate against potential migration issues when performing such updates, this section documents best practices for updating the switch, including contingency procedures for rolling back to previous software versions and saved configurations.

Recommendations and precautions for software updates

Before you update the switch software to a new version:

- We strongly recommend that you save a copy of your config file to an external location.
- We advise against rolling back (going from a newer software version to an older software version) without copying a backup config file to the device.

If you do choose to downgrade software using your existing config file, unpredictable changes in the config file and switch behavior may occur. If booting a K.15.01.0031 or later config file into a K.14.xx or earlier versions of software, the following commands may be removed from your config file:

- Any commands that are present in K.15.01.0031 (or later) but are not present in earlier versions of software
- logging
- snmp-server
- mirror-session
- auto-tftp
- filter source-port
- fault-finder
- interface loopback

After following these steps, you end up with the following results:

- Primary image will hold the new software image you want to install
- Secondary image will hold the image you are currently running
- Primary image will boot with Config1 (config file corresponding to new software version)
- Secondary image will boot with Config2* (config file corresponding to previous software version)

* The current config file must be copied to Config2, or you will be unable to revert if the need arises.



You might opt to use a different methodology in which the new software will be installed as the secondary and not the primary image, in which case you would use the commands **boot system flash secondary**, and/or **boot set-default flash secondary** to change the location of the default boot. However, since you will still need to take precautions to allow you to revert to your previous configuration. We strongly recommend that you follow the methods that are proposed in our update process. This will ensure that you can use our proposed rollback procedures if the need arise.

Validating switch software

Validating a software image

A software is valid if it has a valid digital signature, which is generated by HPE Code Signing Service (HPECSS). Switches that support digital signature verification will generate an error message if you attempt to download an image that is not digitally signed.

- To manually verify the software's digital signature when the switch does not support digital signature verification, use the following command:

```
verify signature flash {primary|secondary}
```

If the signature is valid, the following message is displayed:

```
Signature is valid.
```

- To bypass signature verification, use the **allow-no-signature** option in the **copy** command as follows:

```
copy {tftp|sftp|usb|xmodem} flash [<hostname/IP>]
[<filename>] {primary|secondary} allow-no-signatures
```

The **allow-no-signature** option is available on switches that support non-signed legacy software releases and must be used with caution. To determine support for your switch, go to: <http://www.hpe.com/networking/swvalidation>.

More Information

[Software signing and verification](#) on page 154

Software signing and verification

As an enhanced security feature, you can verify whether a software image being downloaded to or stored in your switch has, in fact, been provided by Networking without any modification or corruption.

Validation is based on the image signature that is generated and attached to the switch software by HPE Code Signing Service (HPECSS). Networking implemented digital signature validation starting with specific switch software versions. For a list of these software versions, go to: <http://www.hpe.com/networking/swvalidation>.



Once a switch software image has been digitally signed on a specific version, all later versions will also be signed.

Switches supporting digital signature verification will generate an error message if you attempt to download an image that is not digitally signed. For example, using the CLI commands described above to revert back to an image that is not signed from an image that is signed and supports verification would result in the following message:

```
This software image does
not contain a digital signature and
cannot be validated as originating
from HP. You may bypass this
validation by using the
'allow no-signature' option. Please
see www.hp.com/networking/swvalidation
for information about which versions
of software contain digital signatures.
```

When you use the **copy** command to download a properly signed image, the CLI logs the following syslog message:

```
Update: Firmware image contains valid signature.
```

Errors related to signature validation will generate one of the following log messages:

```
Update: Aborted. Downloaded file invalid.
```

```
Update: Aborted. Firmware image does not contain a signature.
```

```
Update: Aborted. Firmware image signature is not valid.
```

More Information

Validating a software image on page 153

Rolling back switch software

If you are downgrading to a software version that supports long user names and passwords, ignore the prerequisite. Software versions K.15.01.0032 and later support the longer user names and passwords

Prerequisite

Before downgrading to a software version that does not support long user names and passwords from a software version that supports them, complete one of the following tasks.

- Use the **passwordCLI** command or the Web browser interface, change usernames or passwords to be no more than 16 characters in length, and without any special characters. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear the values using the **no password all** CLI command. Then execute a CLI, **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear password values by using the "Clear" button on the switch. Then execute a CLI, **write memory** command (required if the **include-credentials** feature has ever been enabled).

Rolling back switch software

To roll back your switch from K.15.01.0031 to K.14.47, for example, follow the steps below:

1. Verify that your images and configuration are set correctly using the **show version**, **show flash** and **show config files** commands.

```
Switch1# show version
Image stamp:   /sw/code/build/btm(t5a)
               Apr 23 2010 05:43:42
               K.15.01.0031
               67
Boot Image:    Primary

Switch1# show flash
Image          Size(Bytes)   Date      Version
-----
Primary Image  : 11537788    04/23/10  K.15.01.0031
Secondary Image : 9839140    11/06/09  K.14.47
Boot Rom Version: K.15.09
Default Boot   : Primary

Switch1# show config files

Configuration files:

id | act pri sec | name
---+-----+-----+-----
 1 | *   *   *   | config1
 2 |     *   *   | config2
 3 |     *   *   |
```

2. Boot the switch using the secondary image (with config2).

```
Switch1# boot system flash secondary
System will be rebooted from secondary image. Do
you want to continue [y/n]? y
```

Enter 'y' for yes, and the switch will boot from the secondary image (K.14.47, in this example) with the corresponding configuration for that software version (Config2).

Managing scheduled jobs

Schedule a job to run automatically

A job, that is command, can be scheduled to run on a recurring basis or after certain events. Use the following command to schedule a job:

```
job <name> at
job <Name> at [HH:]MM [on [MM/]DD] [config-save] <Command-str>
job <Name> at <Event> [config-save] <Command-str>
```

job

Schedule a command to run automatically in the future.

Name

The name of the job to add or delete.

at

Schedule when the job runs.

reboot

Run the job as soon as possible after every switch boot.

[HH:]MM

The time when the job has to run.

on

Schedule the job to run on specified days.

MM/DD

The date when the job has to run.

<31-1>

The day relative to the end of the month when the job has to run.

<1-31>

The day of the month when the job has to run.

WEEKDAY-LIST

The days of the week when the job has to run.

config-save

Save configuration changes made by the job.

Command-str

The command to execute when this job runs.



This command uses a new “weekday list” token type. A weekday list represents one or more days of the week and is stored internally. It allows users to specify a list of individual days or a range of days and use abbreviations. Examples of this weekday list are:

- Monday, Friday
 - Mon-Wed
 - mo,we-fr,su
-

Examples

The following example shows a pair of jobs that disable PoE during non-working hours

```
Switch(config)# job poe-on at 8:00 on mon-fri config-save "interface 1-24 power-over-ethernet"
Switch(config)# job poe-off at 17:00 on mon-fri config-save "no interface 1-24 power-over-ethernet"
```

The following example shows a job that block access to a server during weekends

```
Switch(config)# ip access-list extended block-server
Switch(config-ext-nacl)# deny ip any host 10.0.1.80
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# job allow at 8:00 on mon config-save "no interface 1-24 ip access-group block-server in"
Switch(config)# job deny at 17:00 on fri config-save " interface 1-24 ip access-group block-server in"
```

The following example shows a job that blinks the Chassis Locate LED when the switch reboots

```
Switch(config)# job reboot-led at reboot "chassislocate blink"
```

The following example shows a job that reboots the switch on the first day of each year

```
Switch(config)# job annual-reboot at 2:00 on 1/1 boot
```

Deleting a scheduled job

Use the command `no job <name>` to delete a scheduled job. The **name** argument specifies the job to be deleted.

Delete a scheduled job named “baz”

```
switch# show job

Job Scheduler Status and Configuration
Scheduler Status : Waiting for the system time to be set

-----
Name                               Event or   Save
Time                               Cfg        Command
-----
Burr..... reboot                Yes        chassislocate blink
baz                               reboot     No         show time
foo                               17:00 SxTWTxS No         savepower led

switch# no job baz
```

Viewing scheduled jobs

Do one of the following:

- Use the command `show job <Name>` to view details of a specific scheduled job.
- Use the command `show job` to view a list of all the scheduled jobs.

Names and commands that are longer than their column width are truncated with an ellipsis in the display. To assist administrators in diagnosing problems with jobs, there is a detail view for a single job. If the last job run produced any output, the first 255 characters of that output will be shown from the last job run whether that job was successful or not. A successful run will overwrite the error output from a previous failed run.

Examples

The following example displays the list of the scheduled jobs

```
switch# show job

Job Scheduler Status and Configuration
Scheduler Status : Waiting for the system time to be set

-----
Name                               Event or   Save
Time                               Cfg        Command
-----
Burr..... reboot                Yes        chassislocate blink
baz                               reboot     No         show time
foo                               17:00 SxTWTxS No         savepower led
```

The following example displays the details of a specific scheduled job

```
switch# show job baz
```

```
Job Information
Job Name      : baz
Runs At       : reboot
Config Save   : No
Run Count     : 1
Error Count   : 0
Command       : show time
Output from Last Run
-----
Mon Jan  1 00:00:44 1990
```

Time adjustments and scheduling jobs

Daylight savings time adjustments

When daylight savings time (DST) begins (“spring forward”), the local time jumps from 0200 to 0300. The Job Scheduler “catches up” by running all jobs scheduled between 0200 and 0300 the next time it wakes up. This prevents jobs from being skipped when they appear in the 0200 to 0300 time frame.

When daylight savings time (DST) ends (“fall back”), the local time jumps from 0200 to 0100. The Job Scheduler skips all jobs scheduled between 0100 and 0200 to allow local time to catch up. Those jobs already ran once before DST ended will not repeat.



If an administrator configures a new job during the repeat of the 0100 to 0200 hour on the day DST ends, the new job will not be run because the Job Scheduler skips that hour.

External adjustments

External adjustments to the system time can happen to correct for clock drift or for other administrative reasons. The new time update can come from SNTP, from a configuration command at the CLI, or from an SNMP SET of the system time MIB object. When a time adjustment takes place, the Job Scheduler task is called with the new clock value. Jobs scheduled during a time clock jump forward are run while any jobs scheduled during a time clock jump back are skipped.

Adjustment of more than 10 minutes are considered a major change and reset the Job Scheduler. Any jobs scheduled during a time clock jump forward are skipped while any jobs scheduled during a time clock jump back are repeated.

Calendar conflicts

Because the Job Scheduler MIB is more flexible than the CLI scheduling grammar, it is possible to create job schedules via SNMP that cannot be displayed by the CLI. The following rules are imposed on MIB values to limit them to what the CLI can display.

- If any bits are set in `hpicfJobSchedulerEvent`, all Calendar values are ignored. They may be set with SNMP, but are ignored when looking for jobs to run. The Calendar values are also ignored by the command `show running-config`.
- If any bit is set in `CalendarDayOfWeek`, then `CalendarMonth` and `CalendarDayOfMonth` are ignored.
- If no bits are set in `CalendarDayOfWeek` or `CalendarDayOfMonth`, then `CalendarMonth` is ignored.
- Only 1 bit may be set in the `CalendarMonth`, `CalendarDayOfMonth`, `CalendarHour`, and `CalendarMinute` objects. Attempting to set a value with more than 1 bit returns an `InconsistentValue` error.
- If no bits are set in `CalendarHour` and `CalendarMinute`, the job is considered to be in a transition state and not valid. This could happen when an SNMP management application is creating a job one object at a time. Jobs in this state are ignored by the scheduler and by the command `show running-config`.

The Job Scheduler

The Job Scheduler provides administrators the ability to schedule recurring commands or “jobs” on their switch. A feature of the Job Scheduler is the ability to schedule a command to run on a recurring basis or after certain events. For example, a command can be triggered to run by certain predefined events such as switch reboot.

There is no prompt for user input with this feature. Administrators using this feature can schedule commands such as enabling or disabling ports, turning on or off LEDs and Power-Over-Ethernet commands. All commands run with manager privilege in configuration context.

Jobs that are scheduled can be viewed or deleted.

Alternate configuration files

An alternate configuration that is saved to the switch is viewed or copied through the software currently running on the switch. This may result in a misleading portrayal of the configuration. For example, if a configuration is created on K.14.47 and saved as config2, and if it is then viewed or transferred while the switch is running K.15.01.0031, it will appear as though K.15.01.0031 has converted the configuration. However, the alternate configuration file, config2, will still be intact on the switch and load properly when the switch is booted into the same software version from which the configuration file originated.

When an enhancement introduces a feature that did not previously exist in the switch, it may present several challenges to the user.

Backwards compatibility of the configuration created with a version of software that supports a new feature or parameter is not guaranteed. Software versions that did not recognize or support a particular command or parameter will not be able to interpret that line in the configuration. For this reason, it is strongly recommended that network administrators always save their configuration **while still running the switch with the original software version**, and with a notation indicating the software version on which the configuration was saved. For example, a user might save a configuration for a switch running K.14.47 to a TFTP server with an IP address of 10.10.10.15 as follows:

```
switch-onK1447# copy running-config tftp
10.10.10.15 5406onK1447
```

If, for example, the user deems it necessary to revert to the use of K.14.47, the user can boot into it and then restore the saved config from the TFTP server.

Viewing or copying an alternate configuration that is saved to the switch flash can be accomplished only with the software that is currently running on the switch.

Here, for example, a configuration is created on K.14.47 and then saved to flash:

```
switch-onK1447# copy config config2 config
K1447config <cr>
```

And later, the configuration that was created on K.14.47 is viewed while the switch is running K.15.01.0031:

```
switch-onK1501# show config K1447config <cr>
```

The command output will show how the K.14.47 config would be interpreted **if it were to be used by the K.15.01.0031 software**. Copying the K1447config file to a TFTP server would similarly trigger an interpretation by the software performing the file transfer. Note, however, that this does not actually **change** the configuration. If the version is rolled back from K.15.01.0031 to K.14.47 with a command like the following (given that K.14.47 is stored in secondary flash), the K.14.xx formatted config is still intact and valid.

```
switch# boot system flash secondary config
K1447config
```

This "interpretation" during a TFTP or **show** command execution is inherent in the architecture of the switch. When switch features change significantly (such as the move from IPv4 support to IPv6 support), there may be configuration parameters from the previous config that cannot be translated by the switch for viewing while it is

running the new software. This necessitates storing configurations for each version of software to an external location, if the user would like to view the stored config prior to reloading it.

Switches provide a way to automatically adjust the system clock for Daylight Saving Time (DST) changes. To use this feature, define the month and date to begin and to end the change from standard time. In addition to the value "none" (no time changes), there are five predefined settings named:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The predefined settings follow these rules:

Alaska:

- Begin DST at 2 am on the second Sunday in March.
- End DST at 2 am on the first Sunday in November.

Canada and Continental US:

- Begin DST at 2 am on the second Sunday in March.
- End DST at 2 am on the first Sunday in November.

Middle Europe and Portugal:

- Begin DST at 2 am the first Sunday on or after March 25th.
- End DST at 2 am the first Sunday on or after September 24th.

Southern Hemisphere:

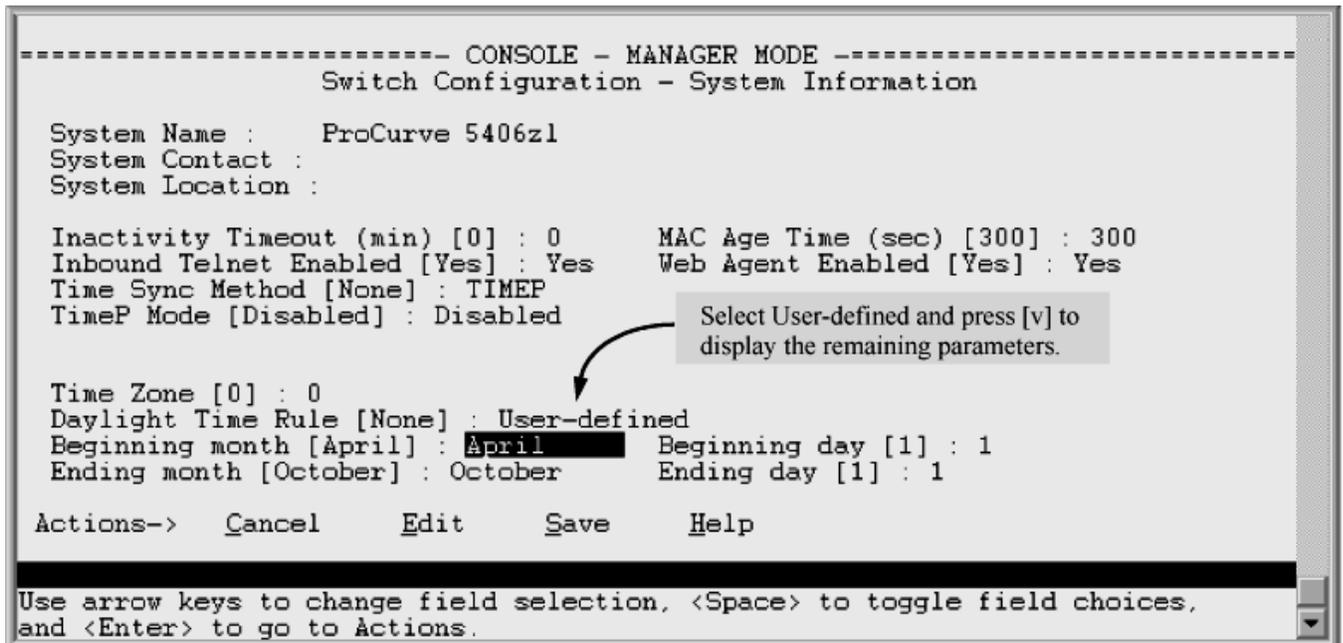
- Begin DST at 2 am the first Sunday on or after October 25th.
- End DST at 2 am the first Sunday on or after March 1st.

Western Europe:

- Begin DST at 2 am the first Sunday on or after March 23rd.
- End DST at 2 am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows you to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change. The menu interface screen looks like the following: (all month/date entries are at their default values):

Figure 56: Menu interface with "user-defined" daylight time rule option



Before configuring a "User defined" daylight time rule, it is important to understand how the switch treats the entries. Given the "Beginning day" and "Ending day", based on an algorithm from Sunday, the switch determines the date to change the system clock :

- If the configured day is a Sunday, the time changes at 2 am on that day.
- If the configured day is not a Sunday, the time changes at 2 am on the first Sunday after the configured day.

This is true for both the "Beginning day" and the "Ending day."

With that algorithm, you can use the value "1" to represent "first Sunday of the month," and a value equal to "number of days in the month minus 6" to represent "last Sunday of the month." This allows a single configuration for every year, no matter what date is the appropriate Sunday to change the clock.

Configuring the module power-saving option

Do one of the following:

- Use the command `savepower module <slot-list>` to turn off power for the modules in the specified slots.
- Use the command `savepower module all` to turn off power for all the modules.

The following example shows how to turn off power for the module in slot "c".

```
Switch(config)# savepower module c

Switch(config)# show savepower module

Module Save Power Information

Slot | Status
----+-----
A   | Disabled
B   | Disabled
C   | Enabled
D   | Disabled
E   | Disabled
```



NOTE

If a `savepower module <slot-list>` or a `savepower module all` command is immediately followed by a `no savepower module <slot-list>` or a `no savepower module all` command, the first slot in the list is powered down and then brought up.

More Information

[Overview of power-saving features](#) on page 172

Configuring the LED power-saving option

Do one of the following:

- Use the following command to turn off the chassis LEDs for the specified slots.

```
savepower led <slot-list>
[timer [MM/DD[/[YY]YY] HH:MM|now|duration [HH:MM[recur]]]
```

- Use the following command to turn off all the chassis LEDs.

```
savepower led all
[timer [MM/DD[/[YY]YY] HH:MM|now|duration [HH:MM[recur]]]
```

Each of these commands includes a timer option. When the timer is configured, the LEDs are turned off for the specified time period and duration. There is one system-wide timer.

The following example shows how to turn off LEDs beginning on 6/1 at 12:01 for 12 hours and repeat daily

```
Switch(config)# savepower led timer 06/01/2009 12:01
duration 12:00 recur
```

```
Switch(config)# show savepower led
```

```
Led Save Power Information
```

```
Alarm Start Time      : 06/01/09 12:01:07
Alarm Duration (HH:MM) : 12:00
Recurrent Status      : Enabled
```

```
Led Save Power Information
```

Slot		Status
----	+	-----
A		Disabled
B		Disabled
C		Disabled
D		Disabled
E		Disabled

More Information

[Overview of power-saving features](#) on page 172

Configuring the slot low-power option

Do one of the following:

- Use the command `savepower port-low-pwr <slot-list>` to put the specified slots into low-power mode.
- Use the command `savepower port-low-pwr all` to put the all the slots into low-power mode.

Slots will go into lower-power mode only if they are not linked. The slots that have the low-power option configured periodically monitor connections to determine if the link has become active. If a LAN cable is connected to one of the slots, that slot will come out of the low-power mode state after approximately two seconds (the monitoring period) and enter into normal power mode. The remaining slots continue to be in low-power mode.

The following example shows how to put slot "c" into low-power mode.

```
Switch(config)# savepower port-low-pwr c
Switch(config)# show savepower port-low-pwr

Port Save Power Information

Slot | Status
----+-----
A   | Disabled
B   | Disabled
C   | Enabled
D   | Disabled
E   | Disabled
```

More Information

[Overview of power-saving features](#) on page 172

Disabling power-saving options

Do one of the following to disable the power-saving option for modules. A module is powered on when its power-saving option is disabled.

- Use the command `no savepower module <slot-list>` to disable the power-saving option for the modules in the specified slots.
- Use the command `no savepower module all` to disable the power-saving option for all the modules.

Do one of the following to disable the power-saving option on chassis LEDs. An LED returns to its original state and any scheduled or running timer is canceled when the power-saving option is disabled on the LED.

- Use the command `no savepower led <slot-list>` to disable the power-saving option on the chassis LEDs for the specified slots.
- Use the command `no savepower led all` to disable the power-saving option on all the chassis LEDs.

Do one of the following to disable the low-power mode for slots. A slot returns to normal power mode when its low-power mode is disabled.

- Use the command `no savepower port-low-pwr <slot-list>` to disable the low-power mode for the specified slots.
- Use the command `no savepower port-low-pwr all` to disable the low-power mode for all the slots.

More Information

[Overview of power-saving features](#) on page 172

Enabling energy-efficient-ethernet (EEE)

Prerequisites

Before you enable energy-efficient-ethernet (EEE), you must insure that both sides of the link are EEE-capable to support the power-saving idle mode.

Energy-efficient-ethernet follows the 802.3az standard, which provides support for a system to operate in low-power idle mode during low-link use.

Enabling energy-efficient-ethernet (EEE)

To enable EEE on the specified port or a range of ports, use the following command:

```
int <port-list> energy-efficient-ethernet
```

Enable EEE on ports B5 through B7

```
Switch(config)# int B5-B7 energy-efficient-ethernet
```

```
Switch(config)# show energy-efficient-ethernet
```

Port	EEE Config	Current Status	txWake (µS)
B1	Enabled	Active	30
B2	Enabled	Inactive	-
B3	Disabled	Inactive	-
B4	Enabled	Unsupported	-
B5	Enabled	Active	30
B6	Enabled	Active	30
B7	Enabled	Inactive	-

More Information

[Overview of power-saving features](#) on page 172

Enabling advertisement of EEE TLVs

The layer 2 (data link layer) Energy-efficient-ethernet (EEE) capability is a feature that allows ports to negotiate the best optimizations for energy efficiency. Use the following command to enable the advertisement of Layer 2 EEE TLVs for a specified port or a range of ports.

```
lldp config <port-list> dot3TlvEnable eee_config
```

The following example shows how to enable the advertisement of Layer 2 EEE TLV for port B5.

```
Switch(config)# lldp config B5 dot3TlvEnable eee_config

Switch(config)# show lldp config B5

LLDP Port Configuration Detail

Port : B5
Adminstatus [Tx_Rx] : Tx_Rx
NotificationEnabled [False] : False
Med Topology Trap Enabled [False] : False

TLVs Advertised:
*port_descr
*system_name
*system_descr
*system_cap

*capabilities
*network_policy
*location_id
*poe

*macphy_config
*poe_config
*eee_config
```

More Information

[Overview of power-saving features](#) on page 172

Disabling EEE or advertisement of EEE TLV

To disable enable Energy-efficient-ethernet(EEE) on the specified port or a range of ports, use the following command:

```
no int <port-list> energy-efficient-ethernet
```

To disable the advertisement of Layer 2 EEE TLVs for a specified port or a range of ports, use the following command:

```
no lldp config <port-list> dot3TlvEnable eee_config
```

More Information

[Overview of power-saving features](#) on page 172

Hibernate mode

hibernate

Syntax

```
hibernate <seconds>
```

Description

Hibernate the system. This command saves the current configuration and powers off the system for the specified period. When the hibernation period expires, the switch will power up and boot using the normal boot process. A typical use case is to have the job scheduler execute the hibernate command. For example, put the switch into hibernate mode from midnight until 5 a.m.

During hibernation, the system will not respond to any network traffic and the console will be inaccessible. The only way to reboot the switch before the hibernation period expires is to press the **Mode** button on the front panel or cycle power, thus disabling the hibernate job and timer.

The system prompts for **y** or **n** confirmation before putting the system into hibernate mode.



This feature is available on the 2930M and only in standalone. It is disabled for stacks.

Command context

Manager

Parameters

<*seconds*>

Specifies the length of time, in seconds, that the system will remain in hibernate mode. Duration: 0 to 2147483647 seconds.

Example

Hibernate the switch for 8 minutes.

```
switch# hibernate 480
```

```
This command will save the current configuration and then power off the system for the specified period. During that time the system will not respond to any network traffic and the console will be inaccessible. The only way to reboot the switch before the hibernation period expires will be to press the Mode button on the front panel or cycle power.
```

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

Viewing settings for power-saving and energy efficiency

Various versions of the **show** command are used to display current settings for power-saving options, Energy-efficient-ethernet (EEE), and EEE TLV.

Do one of the following to view settings:

- Use the command `show savepower module` to view the current settings for the module power-saving option.
- Use the command `show savepower led` to view the current settings for the LED power-saving option.
- Use the command `show savepower port-low-pwr` to view the current settings for the slot low-power option.
- Use the command `show energy-efficient-ethernet` to view the current settings for Energy-efficient-ethernet (EEE).
- Use the command `show lldp info local-device <port-list>` to view the current settings for EEE TLV on the specified local ports.
- Use the command `show lldp info remote-device <port-list>` to view the current settings for EEE TLV on the link partner of the specified port.

Display of the current settings for EEE TLV on the link partner of port B6

Display of the current settings for EEE TLV on the local port B5

Display of the current settings for the slot low-power option

Display of the current settings for the LED power-saving option

Display of the current settings for the module power-saving option

```
Switch(config)# show lldp info remote-device B6

LLDP Remote Device Information Detail

  Local Port      : B6
  ChassisType    : mac-address
  ChassisID      : 00 15 23 ff 2d 49
  PortType       : Local
  PortID         : 3
  SysName        : HP Switch
  System Desc    : HP Switch
  PortDesc       : 3
  Pvid           : 22
.
.
.
Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit        : 10
  Receive         : 10
  Echo Transmit   : 10
  Echo Receive    : 10
  Fallback Receive : 10
```

```
Switch(config)# show lldp info local-device B5

LLDP Local Port Information Detail

  Port      : B5
  PortType  : local
  PortID    : 5
  PortDesc  : B5
  Pvid      : 1

Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit        : 10
  Receive         : 10
  Echo Transmit   : 10
  Echo Receive    : 10
  Fallback Receive : 10
```

```
Switch(config)# show savepower port-low-pwr

Port Save Power Information

Slot | Status
----+-----
A    | Enabled
B    | Enabled
C    | Enabled
D    | Enabled
E    | Enabled
```

```
Switch(config)# show savepower led

Led Save Power Information

Alarm Start Time      : 06/01/09 12:01:07
Alarm Duration (HH:MM) : 12:00
Recurrent Status      : Enabled

Led Save Power Information

Slot | Status
----+-----
A    | Enabled
B    | Enabled
C    | Enabled
D    | Enabled
E    | Enabled
```

```
Switch(config)# show savepower module

Module Save Power Information

Slot | Status
----+-----
A    | Disabled
B    | Disabled
C    | Enabled
D    | Disabled
E    | Disabled
```

More Information

Overview of power-saving features on page 172

Displayed values for Energy-efficient-ethernet (EEE)

The displayed values for the energy efficient Energy-efficient-ethernet (EEE) status are explained in the following table.

Parameter	Description
EEE Config	The EEE configuration status, read from the configuration database.
<ul style="list-style-type: none"> Enabled Disabled 	<ul style="list-style-type: none"> EEE mode is enabled. EEE mode is disabled.
Current Status	Current EEE operational status.

Table Continued

Parameter	Description
<ul style="list-style-type: none"> Active 	The port is advertised and auto-negotiated EEE with link partner (an EEE-capable partner.) EEE mode is enabled.
<ul style="list-style-type: none"> Inactive 	Set to one of the following conditions: <ul style="list-style-type: none"> EEE configuration is disabled on the local port. Local port advertises EEE capabilities with "EEE disabled" link partner or non-EEE link partner. Auto-negotiation is mandatory for EEE to work. EEE configuration will not be applied if the port is in forced/manual (speed-duplex) mode. The current status will be 'inactive' for forced/manual mode port configuration. EEE is not supported for 10Base-T. The current status will be 'inactive' if the link is operating in 10Base-T mode.
<ul style="list-style-type: none"> Unsupported 	The local physical interface does not have EEE capability.
txWake	Current value of transmit wake-up time (in microseconds.)



The interface modules do not support adjustment of both transmit and receive wake-up times. Therefore, txWake is constant.

Power-saving features supported by modules

The modules support the power-saving features as indicated in the table below:

Product number	Description	LED power on/off	Slot auto low-power mode	Slot power on/off
J8702A	Switch zl 24 10/100/1000 PoE Module	Yes	Yes	Yes
J8705A	Switch zl 20 Gig-T + 4 mGBIC Module	Yes	Yes	Yes
J8706A	Switch zl 24-Port Mini-GBIC Module	Yes	No	Yes
J8707A	Switch zl 4-Port 10GbE X2 Module	Yes	No	Yes
J8708A	Switch zl 4-Port 10GbE CX4 Module	Yes	No	Yes

Table Continued

Product number	Description	LED power on/off	Slot auto low-power mode	Slot power on/off
J9307A	Switch 24-Port 10/100/1000 PoE+ zl Module	Yes	Yes	Yes
J9308A	Switch 20-Port 10/100/1000 PoE+/4-Port MiniGBIC zl Module	Yes	Yes	Yes
J9309A	Switch 4-Port 10Gbe SFP+ zl Module	Yes	No	Yes
J9478A	Switch 24-Port 10/100 PoE+ zl Module	Yes	Yes	Yes

Overview of power-saving features

There are several power-saving features that can be configured for the indicated switches and modules. The power-saving features include:

- Turn slot power on or off
- Turn LED power on or off
- Turn slot auto low-power mode on or off
- Use LLDP for Energy-Efficient-Ethernet

Slot power

The `savepower module` option shuts down the slot power for the specified modules in the order specified in the command. The ports on these modules no longer pass traffic. Any management traffic (SNMP, SSH, Telnet) that passes through these modules is interrupted. It can take up to two minutes to power down all the specified modules. Check the Event Log to see the current status of the module power down. This command applies to PoE/PoE+ modules as well as non-PoE/PoE+ modules.

LED power

The `savepower LED` option provides the ability to turn off specified slot LEDs or all LEDs. You can also configure a timer for turning off the chassis LEDs or the specified slot LEDs. There is one system-wide timer; all the selected slots will have the chassis LEDs turned off for the same amount of time.

When the timer option is configured, a timer for turning off the chassis LEDs or configured slot LEDs. The LEDs are turned off for the configured time period and duration.

<code>MM/DD [/ [YY] YY] HH:MM</code>	Specifies the date and time to start the timer.
<code>now</code>	Instantaneously turns off the LEDs. The configured timer is canceled and all the configured modules go into power-saving mode immediately.

Table Continued

`duration [HH:]MM`: The amount of time the LEDs remain turned off. (Optional) If the duration value is zero, when the timer starts, the LEDs are turned off indefinitely until the timer is canceled or the command is overridden with another command. Default: 0 (zero)

`recur`: (Optional) If specified, the LEDs are turned off on a daily basis at the configured time. The `recur` option is ignored if the duration is configured as zero. Default: disabled.

A new command overrides the previous command, regardless of the current state. For example, if a timer is active and new command is given, the currently running timer is canceled and the new timer is scheduled.

Slot auto low-power mode

The auto low-power mode option puts the slots into auto low-power mode if they are not linked. If a particular slot is specified, only that slot goes into auto low-power mode. Specifying `savepower port-low-pwr all` puts all the slots into auto low-power mode.

The ports in low-power mode periodically monitor to determine if the link has become active. If a LAN cable is connected to one of the ports, that port will come out of the low-power mode state after approximately 2 seconds (the monitor period) and enter into normal power mode. The remaining ports continue to be in low-power mode.

Energy-efficient-ethernet

Energy-efficient-ethernet (EEE) follows the 802.3az standard, which provides support for a system to operate in low-power idle mode during low-link use. This allows both sides of a link to disable or turn off a portion of the system's transmit/receive circuitry, saving power. When traffic is ready for transmission, the interface sends a "wake-up" message to the link partner to prepare to receive the traffic. The circuitry is returned to "normal" mode. Both sides of the link must be EEE-capable to support the power-saving idle mode.

Layer 2 (data link layer) EEE capability is a feature that allows fine-tuning for EEE that uses LLDP TLVs for the negotiation of physical link partners' wake-up time values. An EEE-capable port notifies its link partner about the EEE capabilities supported. The ports then negotiate how to best optimize energy efficiency.

More Information

[Configuring the LED power-saving option](#) on page 163

[Configuring the module power-saving option](#) on page 163

[Configuring the slot low-power option](#) on page 164

[Disabling EEE or advertisement of EEE TLV](#) on page 167

[Disabling power-saving options](#) on page 165

[Enabling advertisement of EEE TLVs](#) on page 166

[Enabling energy-efficient-ethernet \(EEE\)](#) on page 165

[Viewing settings for power-saving and energy efficiency](#) on page 168

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see [Support and other resources](#).

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

- 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

Accessing updates

- 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 download product updates:

Hewlett Packard Enterprise Support Center

www.hpe.com/support/hpesc

Hewlett Packard Enterprise Support Center: Software downloads

www.hpe.com/support/downloads

Software Depot

www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- 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:
www.hpe.com/support/AccessToSupportMaterials



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

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts

do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-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 the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise 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@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.

To find and maintain Networking devices, Hewlett Packard Enterprise recommends using the Network Discovery Tool. Note that this tool does not replace or augment full-featured Network Management software.

To install the Network Discovery Tool, follow these steps:

Procedure

1. From a PC (running Windows Vista SP2, Windows 7 SP1, 8, 2008 SP2 or R1 SP1, or later), type in the URL* for the Network Discovery Tool into a browser's address field and press Enter.
2. When asked, open the file. In the resulting folder, double-click the file setup. Accept running the install.
3. Upon completion, the tool runs automatically. (Note: If .NET is not installed on your system, you may be prompted to install it. Follow the installation instructions.)

*For additional information, contact <http://www.hpe.com/networking/support>.



When updating the Network Discovery Tool software, you must first uninstall the old version before installing the new one.

Run the Network Discovery Tool shortly after powering on newly installed devices. By default, only new Networking devices will display. Use the filter drop-downs to specify device age, type, and so on. Double-click on a device to start its web user interface.

For additional information, visit the Network Discovery Tool's internal help page.

RFC 4292

Switch families indicted in the **Abstract** section of the *Basic Operations Guide* enjoy full conformance of the RFC 4292.

RFC defines a portion of the Management Information Base (MIB) for use in managing objects related to the forwarding of Internet Protocol (IP) packets in an IP version-independent manner. It is to be noted that the MIB definition described herein does not support multiple instances based on the same address family type. However, it does support an instance of the MIB per address family.

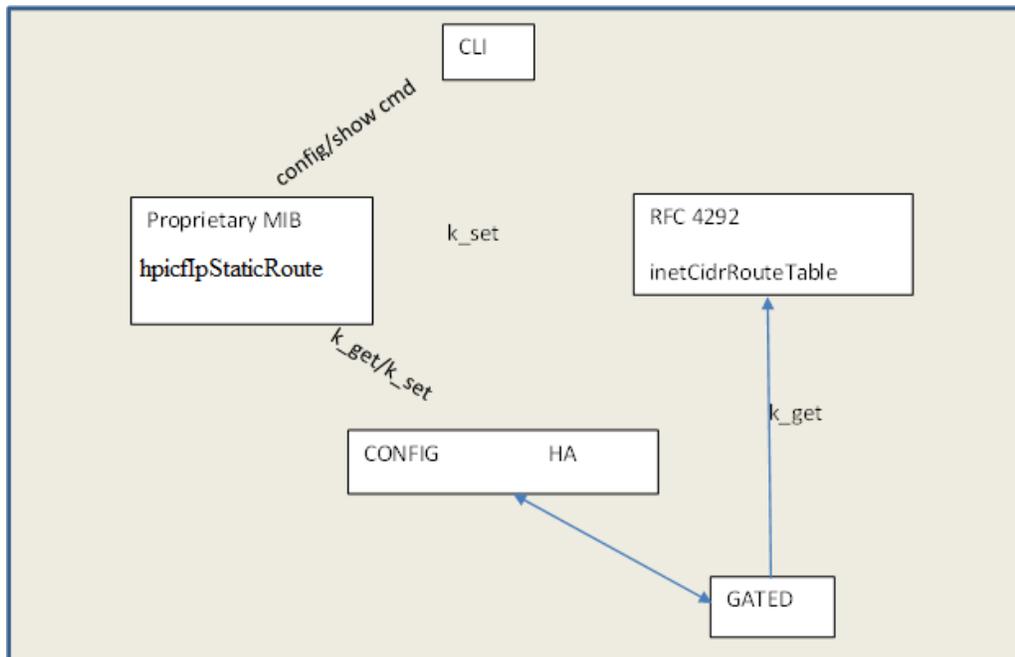
RFC 4292 supported operations

Both GET and SET operations are now supported on switches. RFC 4292 is supported in the following ways:

1. The set operation can create IPv4 and IPv6 static routes which include the functions for **Reject**, **Remote**, and **Blackhole**.
2. A column of any existing row with RowStatus "Active" will not be allowed for modification.
3. Rowstatus will not support "Create-and-wait".
4. There is an existing HPE proprietary MIB, `hpicfIpStaticRouteTable`, which is used to configure IPv4 and IPv6 static routes. Currently CLI commands use this proprietary MIB for configuration. This will remain unchanged.
5. The SET functions for `inetCidrRouteTable` (`k_test`, `k_ready`, `k_setDefaults` and `k_set`) are implemented. The implementation maps to the existing **SET** routines of `hpicfIpStaticRouteTable` with the necessary changes. Index of `InetCidrRouteTable` has `RoutePolicy` whereas `hpicfIpStaticRouteTable` has `IfIndex`. Both MIBs have 6 objects as index.
6. The current **GET** implementation of `inetCidrRouteTable` is directly accessing the Gated Routing table to retrieve all the routes which include Static and Dynamic. The **SET** routines will have to go through the `hpicfIpStaticRouteTable` **SET** functions as these routes are of type Static.

7. Creation, modification, or deletion of Dynamic route entry is not allowed. This can be achieved by validating the MIB column `inetCidrRouteProto` for Static or Dynamic protocol.
8. `gateD`(routing stack) does not discard any routes, so the value of `inetCidrRouteDiscards` MIB will always be 0.

Figure 57: MIB mapping



RFC 4292 MIB operations

To make the switch software fully compliant to RFC 4292, both **GET** and **SET** operations are supported as indicated in the table below.

Table 10: GET and SET operations

<code>inetCidrRouteTable</code>	Type	Access
<code>inetCidrRouteDestType*</code>	InetAddressType,	Not-accessible
<code>inetCidrRouteDest*</code>	InetAddress,	Not-accessible
<code>inetCidrRoutePfxLen*</code>	InetAddressPrefixLength,	Not-accessible
<code>inetCidrRoutePolicy*</code>	OBJECT IDENTIFIER,	Not-accessible
<code>inetCidrRouteNextHopType*</code>	InetAddressType,	Not-accessible
<code>inetCidrRouteNextHop*</code>	InetAddress	Not-accessible
<code>inetCidrRouteIfIndex</code>	InterfaceIndexOrZero,	Read-Create

Table Continued

inetCidrRouteTable	Type	Access
inetCidrRouteType	INTEGER,	Read-Create
inetCidrRouteProto	IANAipRouteProtocol,	Read-Only
inetCidrRouteAge	Gauge32,	Read-Only
inetCidrRouteNextHopAS	InetAutonomousSystemNumber,	Read-Create
inetCidrRouteMetric1	Integer32,	Read-Create
inetCidrRouteMetric2	Integer32,	Read-Create
inetCidrRouteMetric3	Integer32,	Read-Create
inetCidrRouteMetric4	Integer32,	Read-Create
inetCidrRouteMetric5	Integer32,	Read-Create
inetCidrRouteStatus	RowStatus	Read-Create
* INDEX OBJECTS		

JITC authorization requirements

The Joint Interoperability Test Command (JITC) conducts testing of national security systems and information technology systems hardware, software, and components. Hewlett Packard Enterprise is in compliance with JITC which provides the following.

- Logs of security-related events with new login credentials separate from operator or manager credentials.
- Log message when the event log wraps.
- Configuration commands that allow users to set the maximum number of concurrent sessions.
- Configuration commands which allow users to set the maximum number of concurrent sessions per user.
- Increase the delay between failed login attempts.



The HPE 3800 Switch and HPE 2920 Switch are currently UC APL certified.

Local authentication and authorization

JITC requires that access to security logs be provided through security user authentication and authorization. For more information about JITC security authentication and authorization, see the *Access Security Guide* for your switch.

Security user log access

Security user logs are accessible when both the authentication and authorization are local. A default group called the **default-security-group** is available in manager mode and has the privileges to execute the commands `copy security-log`, `show security-logging`, and `clear security-logging`. When a security user is attached to the group, they will only be able to execute these three commands. Other users will not be able to execute the commands, no matter whether they are an operator or manager.

For more information about JITC security user log creation and access, see the *Access Security Guide* for your switch.

Authentication and Authorization through RADIUS

For RADIUS authentication and authorization, the security user will be able to access to security log by configuring the file located on RADIUS server. For more information about JITC authentication and authorization through RADIUS, see the *Access Security Guide* for your switch.

Authentication and Authorization through TACACS

For TACACS authentication and authorization, the user can access to security log by configuring the file located on TACACS server. For more information about JITC security authentication and authorization, see the *Access Security Guide* for your switch.

Common access card (two-factor) authentication

Overview

A common access card (CAC) is a United States Department of Defense (DoD) smart card for multifactor authentication. CACs are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. In addition to its use as an ID card, a CAC is required for access to government buildings and computer networks.

Two-factor authentication

Part of the requirement necessary to satisfy the Federal Government Certification is two-factor authentication. Two-factor authentication is the redundant authentication of the CAC. For example, the CAC satisfies two-factor authentication by mandating that you have both the physical card and know the pin number associated with the card.

To provide support for CAC authentication, the requirement for the network is the establishment of SSH connections. Two-factor authentication constitutes authentication based on public key or certificate and username/password on the switch.

Restrictions

The following are some of the restrictions when working with CAC authentication:

- Support is not provided for any other management connections other than SSH.
- Support is not provided for any switch acting as CAC SSH client.
- Support is not provided for public-key authentication based on DSA and ECDSA public keys.
- The maximum number of client public keys that can be installed is 10.
- When there is failure in any one of the authentication methods, the SSH connection will not be established.
- The following table lists the invalid authentication methods for SSH.

login	enable
public-key	certificate
public-key	two-factor-certificate
certificate	public-key

Table Continued

login	enable
certificate	two-factor-public-key
two-factor-public-key	certificate
two-factor-public-key	two-factor-certificate
two-factor-certificate	public-key
two-factor-certificate	two-factor-public-key

Expected behaviors

With `include-credentials` command

- When the command `include-credentials` is enabled, public keys are stored both in configuration and flash files.
- When the command `no include-credentials` is executed, the client public key is stored only in the flash.
- When the command `no include-credentials store-in-config` is executed, behavior is then based on the user entry made with the `pop-up` message.

The command `switch(config)# no include-credentials store-in-config` will display a message similar to:

```
This will remove any switch passwords and inactive SSH
authorized keys from all configuration files. This will also restore
the functionality to store only a single set of passwords and authorized
keys on the switch.
```

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

```
The SSH authorized keys associated with the active configuration will be
deleted.
```

```
Would you like to retain these as the switch global SSH authorized keys
(y/n)? y
```

If the above option entered is "y", then the client public key will be available in the flash but not in the config.

If the above option entered is "n", then the client public key is neither available in the flash nor in the config.

Zeroization

When the zeroization command `switch(config)# crypto key zeroize ssh-client-key` is executed, the client public keys will be zeroized in the flash.

```
switch(config)# crypto key zeroize ssh-client-key
```

```
The manager key pair will be deleted, continue (y/n)? y
```

```
The command erase all zeroize will also perform the
zeroization of the key files in the flash.
```

```
The command erase all will only delete the key files from
```

```
flash.
```

Switch is moved to/from enhanced security mode

Since the secure mode change goes through zeroization, the client keys are deleted and the switch will revert to the default configuration without any client keys on the switch.

Attempting to configure a two-factor authentication method with no public key or username configured

If, during the download of the configuration file, the username and/or public key is not configured, then no action will be taken. A warning message will display similar to:

```
username and/or public key is not configured.
```

An RMON will be logged with the message that the authentication method is set to two-factor with some configuration missing.

When the user tries to connect using SSH, the connection will fail.

Deletion of the public key and/or username when the authentication method is set to two-factor authentication

For the following three scenarios:

- After the authentication method is set to two-factor, if the client public keys are deleted while the usernames still exists on the switch...
- After the authentication method being set to two-factor, if the username is deleted the public key exists on the switch...
- When both the public key and usernames are deleted while the authentication method is being set to two-factor authentication...

The new SSH connection will fail at either the public key authentication and/or username/password authentication. RMON will be logged with appropriate message on the switch.



An alternative solution is to block the deletion of the public key and/or username when the authentication method is set as two-factor authentication. With this approach, the impact of many configurations need to be taken care cautiously since the username/password can be configured through many interfaces such as SNMP, REST, WebUI, Menu, setup mgmt.-interfaces, and include-credentials.

Authentication method re-configured at run time

If the authentication method is reconfigured at run time, the modified authentication method will be applied when the new connection will be established.

Secure Mode

With this release, the 3810M switch in secure mode is in compliance with the Federal Information Processing Standards (FIPS). For more information, see the *Access Security Guide* of your switch.

Federal government certification

The following phase 3 certification features are included in the 16.03 release.

Local command audit logging

The logging of all administrative actions on a device is a requirement for NDcPP certification:

- All administrative actions (commands) must be logged locally.
- Enabling and disabling of command log storage is required.

- The identity of a user causing an event must be logged.
- When the command log is exhausted by 80% and wraparound occurs, the event must be logged and a trap must be generated.
- The logs have a maximum of 240 characters and are stored in the command log buffer. If the log message exceeds this maximum length, it is truncated and is not stored in the command log buffer.

Password storage in SHA-256 format

On Aruba switches, passwords can be configured either in plaintext or SHA-1 format. You can now configure the passwords in SHA-256 format as well. For more information, see the *Access Security Guide* of your switch.

SSH Re-keying

To comply with RFC 4251, session re-keying ensures that either the SSH server or the SSH client initiates a re-key. This results in a new set of encryption and integrity keys to be exchanged between them. Once the re-key is complete, new keys are used for further communication, which ensures that the same key is not used for a long duration and the security of the session is maintained. For more information, see the *Access Security Guide* of your switch.

OSPFv3 RFC compliance

This feature supports authentication for OSPFv3 routing traffic on Aruba devices via IPsec. The authentication support for OSPFv3 is provided in compliance with RFC 4552. Authentication is supported using AH protocol. Authentication and confidentiality support using ESP is not supported in this release. For more information, see the *IPv6 Configuration Guide* of your switch.

X.509v3 certificate extension RSA minimum key support

There are three requirements for NDcPP certification:

- Minimum secure RSA key size.
- Enforcement of TLS 1.1/TLS 1.2 for all TLS connections.
- Validation of extended key usage extension for X509v3 certificates.

As part of the minimum secure RSA key size requirement, an option has been added to the existing `tls` configuration command to support minimum TLS version support for cloud application requirement.

X.509v3 certificate authentication for SSH

This feature supports user-authentication in SSH using X.509v3-based certificates. For more information, see the *Access Security Guide* of your switch.

Enabling or disabling DLDP

Device Link Detection Protocol (DLDP) must be enabled globally and on one or more interfaces to begin monitoring. DLDP is disabled by default.

- To enable DLDP on the switch, use the command `dldp enable`.
- To disable DLDP on the switch, use the command `dldp disable`.
- To disable DLDP globally, use the command `no dldp enable`.

Setting the DLDP advertisement interval

Setting the DLDP advertisement interval appropriately for your network environment assures that DLDP can detect unidirectional links before network performance deteriorates. Hewlett Packard Enterprise recommends keeping the advertisement interval the same across the link partners.

- To set the advertisement interval, use the command `dldp interval <1-100>`, specifying a value between 1 and 100 seconds.
- To reset the advertisement interval to the default value of 5 seconds, use the command `no dldp interval`.

Enabling and disabling types of DLDP debugging

- To enable specific types of debugging for DLDP on the specified ports, use the following command:
`debug dldp all|error|event| packet|state-machine|timer <port-list>`
- To disable specific types of debugging for DLDP on the specified ports, use the following command:
`no debug dldp all|error|event| packet|state-machine|timer <port-list>`

Arguments:

all

Display all DLDP debug messages.

error

Display all DLDP error messages.

event

Display all the DLDP event messages.

packet

Display all DLDP packet messages.

stat-machine

Display all DLDP state machine messages.

timer

Display all DLDAP timer messages.

port-list

Display all DLDAP debug messages for the listed port.

Clearing statistics on DLDAP packets

Procedure

1. To clear statistics on DLDAP packets that pass through the specified ports, use the following command:

```
clear statistics dldap <port-list>
```

2. To clear statistics on DLDAP packets that pass through all ports, use the following command:

```
clear statistics dldap all
```

Viewing DLDAP configuration information and statistics

- To view the DLDAP statistics for the specified ports, use the command `show dldap statistics <port-list>`. The **port-list** argument specifies a single port, a list of ports, or a range of ports.
- To view the DLDAP statistics for all ports, use the command `show dldap statistics all`
- To view the DLDAP configuration information and statistics for the specified ports, use the command `show dldap <port-list>`. The **port-list** argument specifies a single port, a list of ports, or a range of ports.
- To view the DLDAP configuration information and statistics for all ports, use the command `show dldap all`.

The following examples show the DLDAP statistics for port number a1.

```
show dldap statistics a1
```

```
Status and Counters - Device Link Detection Protocol
Port : a1
Packets Sent                : 256
Packets Received            : 255
Invalid Packets Received    : 0
Authentication Failed Packets Received : 0
Valid Packets Received      : 255
```

The following example shows the DLDAP statistics for ports a1 through a3.

```
show dldap statistics a1-a3
```

```
Status and Counters - Device Link Detection Protocol
Port : a1
Packets Sent                : 256
Packets Received            : 255
Invalid Packets Received    : 0
Authentication Failed Packets Received : 0
Valid Packets Received      : 255
Port : a2
Packets Sent                : 256
Packets Received            : 255
Invalid Packets Received    : 0
Authentication Failed Packets Received : 0
Valid Packets Received      : 255
Port : a3
Packets Sent                : 256
Packets Received            : 255
Invalid Packets Received    : 0
Authentication Failed Packets Received : 0
Valid Packets Received      : 255
```

```

Port : a3
Packets Sent : 0
Packets Received : 0
Invalid Packets Received : 0
Authentication Failed Packets Received : 0
Valid Packets Received : 0

```

The following example shows the DLDAP configuration information and statistics for port number a1.

```
show dldap a1
```

The output will display sensitive information. Continue (y/n)?

```
Status and Configuration - Device Link Detection Protocol
```

```

Global Status : Enabled
Advertisement Interval (Sec) : 5
Authentication Mode : None
Authentication Password : Password
Unidirectional Shutdown Mode : Auto
DelayDown Timer Value (Sec) : 1
Number of DLDAP Enabled Ports : 2
Interface A1
DLDP Port State : Bidirectional
Number of Neighbors : 1 (Maximum number ever detected: 2)

```

Port	Port State	Link State	Neighbor MAC Address	Neighbor Port Index	Neighbor	Neighbor Aged Time
A1	Unidirectional	up	010fe2-000004	5	unconfirmed	0

The following example shows the DLDAP configuration information and statistics for ports a1 through a3.

```
show dldap a1-a3
```

The output will display sensitive information. Continue (y/n)?

```
Status and Configuration - Device Link Detection Protocol
```

```

Global Status : Enabled
Advertisement Interval (Sec) : 5
Authentication Mode : None
Authentication Password : Password
Unidirectional Shutdown Mode : Auto
DelayDown Timer Value (Sec) : 1
Number of DLDAP Enabled Ports : 2
Interface A1
DLDP Port State : Unidirectional
Number of Neighbors : 1 (Maximum number ever detected: 2)
Interface A2
DLDP Port State : Bidirectional
Number of Neighbors : 1 (Maximum number ever detected: 2)
Interface A3
DLDP Disabled

```

Port	Port State	Link State	Neighbor MAC Address	Neighbor Port Index	Neighbor	Neighbor Aged Time
------	------------	------------	----------------------	---------------------	----------	--------------------

A1	Unidirectional	up	40a8f0-9e2100	2	unconfirmed	0
A2	Bidirectional	down	010fe2-000004	3	unconfirmed	0

Setting the DLDAP delaydown timer

The DLDAP DelayDown timer specifies the delay, in seconds, before down ports are rechecked.

- To set the DLDAP DelayDown timer, use the command `dldap delaydown-timer <1-5>`, specifying a value between 1 and 5 seconds.
- To reset the DLDAP DelayDown timer to the default value of 1 second, use the command `no dldap delaydown-timer`.

Setting DLDAP unidirectional-shutdown mode

On the detection of a unidirectional link, the port can be shut down either automatically or manually. This setting controls whether the shutdown is automatic or manual.

Procedure

1. To set the DLDAP unidirectional-shutdown mode, use the following command:

```
dldap unidirectional-shutdown auto|manual
```

2. To reset the DLDAP unidirectional-shutdown mode to the default value (automatic shutdown), use the following command:

```
no dldap unidirectional-shutdown
```



When DLDAP detects a unidirectional port, an event is logged and the port must be shut down manually by an administrator. In the event that the link state is restored to bidirectional and the shutdown mode is manual, the user must manually bring up the port. Any dynamic change of the shutdown mode (that is, auto to manual) will take effect only when DLDAP is disabled globally and enabled again. Likewise, When the link state is restored to Bidirectional and the shutdown mode is manual, the user must manually bring up the port.

Also, any dynamic change of the shutdown mode (that is, auto->>manual/vice versa) will be taken into effect only when DLDAP is disabled globally and enabled back again

Setting the DLDAP authentication-mode

The authentication mode determines the type of authentication that DLDAP uses. By default, no authentication is used. Hewlett Packard Enterprise recommends keeping the authentication mode the same between link partners or it will fail and log errors.

- To set the DLDAP authentication mode, use the following command:

```
dldap authentication-mode none|md5|simple
```

- To reset the DLDAP authentication mode to the default value (no authentication), use the following command:

```
no dldap authentication-mode
```

This is equivalent to specifying **none** when setting the authentication mode.

Authentication modes:

none

Do not perform DLDAP authentication (default).

md5

Authenticate using MD5.

simple

Authenticate using a plain text password.

Setting or removing a DLDAP authentication password

- To set the DLDAP authentication password to a plain text value, use the following command:

```
dldap authentication-password simple
```

- To set the DLDAP authentication password to an encrypted value (a base64-encoded aes-256 encrypted string), use the following command:

```
dldap authentication-password encrypted
```

- To remove the DLDAP authentication password, use the following command:

```
no dldap authentication-password
```



When `encrypt-credentials` is enabled, the `encrypted` parameter is displayed. When configuring the authentication password after configuring the authentication mode, the authentication mode defaults to `none` (advertised in PDUs) regardless of which authentication mode you attempt to configure.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode will be `none` (advertised in PDUs) no matter which authentication mode you configure.

The following example shows disabled `encrypt-credentials`.

```
dldap authentication-password
```

simple

Set the authentication password to plain text.

The following example shows enabled `encrypt-credentials`.

```
dldap authentication-password
```

simple

Set the authentication password to plain text.

encrypted

Global encryption key, specified using a base64-encoded aes-256 encrypted string.

The following example shows both in secure mode.

```
dldap authentication-password simple
```

Password will be prompted interactively as above and sets the entered value in the configuration.

```
Enter Password:
```

```
Re-Enter Password:
```

In Download mode, the authentication password must be accepted as inline parameter only, and not be prompted interactively.

Include-credentials and encrypt-credentials considerations

The output of `show running-config` will be modified if `encrypt-credentials` is enabled or disabled. The `running-config` output changes when `include-credentials` or `encrypt-credentials` is enabled or disabled.

Table 11: Include/exclude credentials

Include credentials	Encrypt credentials	show run output	Reboot with Saved Config	Download config file
Disabled	Disabled	DLDP authentication-password will not be displayed.	The plain-text password in the Config will be used to update the protocol data structure.	Mis-Configuration (Password cannot be configured in this case because password is not available in downloaded config.)
Disabled	Enabled	DLDP authentication-password will not be displayed.	The encrypted password in the Config will be decrypted and used to update the protocol data structure.	Mis-Configuration (Password cannot be configured in this case because password is not available in downloaded config.)
Enabled	Disabled	DLDP authentication-password will be displayed in plain-text.	The plain-text password in the Config will be used to update the protocol data structure.	DLDP authentication-password stored as plain-text.
Enabled	Enabled	DLDP authentication-password will be displayed in encrypted form.	The encrypted password in the Config will be decrypted and used to update the protocol data structure.	DLDP authentication-password stored as encrypted.

dldp authentication-password

```
dldp authentication-password simple
```

```
Enter Password: ****
Re-Enter Password: ****
```

include-credentials and encrypt-credentials are disabled

```
show running-config
```

```
Running configuration:
```

encrypt-credentials is enabled and include-credentials is disabled

```
encrypt-credentials
```

```
show running-config
```

```
Running configuration:
```

include-credentials is enabled and encrypt-credentials is disabled

```
include-credentials
```

```
show running-config
```

```
Running configuration:
```

```
dldp authentication-password simple test
```

encrypt-credentials and include-credentials are enabled

```
encrypt-credentials
```

```
include-credentials
```

```
show running-config
```

```
Running configuration:
```

```
dldp authentication-password encrypted  
"QFg8OTxYyLMEnFvQt6o542tAmbk4RrH4d00C60oFokI="
```

Validation rules for DLDP

Table 12: *Validation rules for DLDP*

Validation	Error/Warning/Prompt
Verify if UDLD is enabled on a Port.	DLDP and UDLD cannot be enabled on a port at the same time.
Verify if DLDP is configured on a trunk.	Option cannot be set on a trunk.
Verify if DLDP is configured on more than 128 ports.	DLDP cannot be configured on more than %d ports.

Table Continued

Validation	Error/Warning/Prompt
Verify if DLDP is configured on mesh port.	DLDP cannot be enabled on mesh ports. Remove the port from the mesh before enabling DLDP.
Verify DLDP is configured on a port.	DLDP and UDLD cannot be enabled on a port at the same time.
Verify if DLDP is enabled while filtering DLDP MAC address.	This MAC address cannot be filtered when DLDP is enabled.
DLDP PKT received on a DLDP disabled port will *not be* forwarded and will be dropped by the switch.	DLDP is not supported on Distributed trunks that is, cannot be enabled on individual port of a DT trunk
If DLDP is globally disabled on the switch DLDP packets received will be reforward on the same vlan.	DLDP is not supported on DYN trunks
Verify mesh is configured on DLDP port.	Ports with DLDP enabled cannot be added to a mesh.
Verify if DLDP MAC address is being filtered.	DLDP cannot be enabled when the MAC address 010fe2-000001 is filtered.
Verify if the password contains invalid characters.	Invalid password. The password cannot contain the special characters \, ? and ”.
Verify the given password length.	Authentication password must be 1 to 16 characters long.

Restrictions for DLDP

- DLDP is mutually exclusive with UDLD running on the port and some of the other protocol running on the switch.
- DLDP is not supported on Distributed trunks that is, cannot be enabled on individual port of a DT trunk.
- DLDP is not supported on DYN trunk
- DLDP PKT received on a DLDP disabled port will **not** be forwarded and will be dropped by the switch. If DLDP is globally disabled on the switch, DLDP pkts received will be reforward on the same VLAN.

Overview of device link detection protocol (DLDP)



DLDP is active on the following switches:

- Aruba 2530 Switches
- Aruba 2920 Switch
- Aruba 2930F Switches
- Aruba 3810 Switches
- HPE 2620 Switch
- HPE 3800 Switches
- HPE 5400R Switches (both v2 and v3 blades)

Device link detection protocol (DLDP) is switch technology that detects any unidirectional link failures that can occur in a network. Typically these unidirectional link failures occur among devices connected through fiber-optic or copper twisted pair (such as category 5 twisted pair) cables. Upon detecting a link failure, the link PHY will be

kept UP and will be blocked in the hardware. All the upper layer protocols of the switch software (STP, LACP, and so on) will see the interface as DOWN.

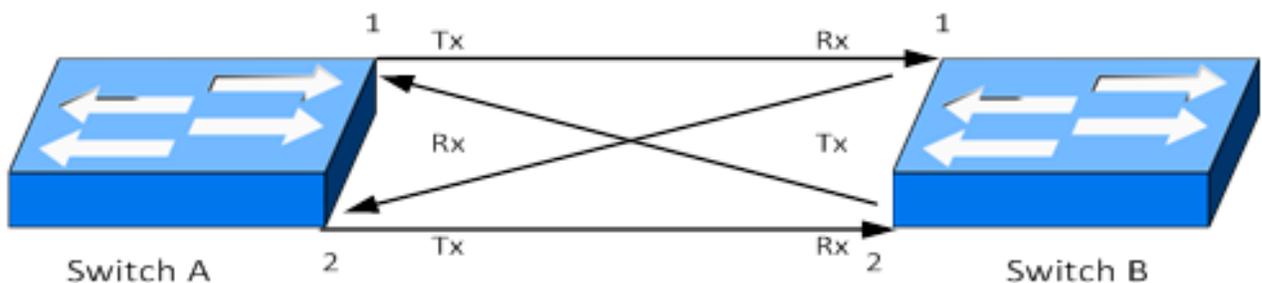
Enabling and disabling DLDP: Enable or disable the Device Link Detection Protocol (DLDP) to monitor link status. DLDP must be enabled globally and on one or more interfaces to begin monitoring. DLDP is disabled by default.

Advertisement interval: This is the interval between sending DLDP advertisement packets. Setting the DLDP advertisement interval appropriately for your network environment assures that DLDP can detect unidirectional links before network performance deteriorates. Hewlett Packard Enterprise recommends keeping the advertisement interval the same across the link partners or DLDP can fail and produce an error log.



DLDPDUs are sent as untagged PKTs on default VLAN. No support for tagged advertisements.

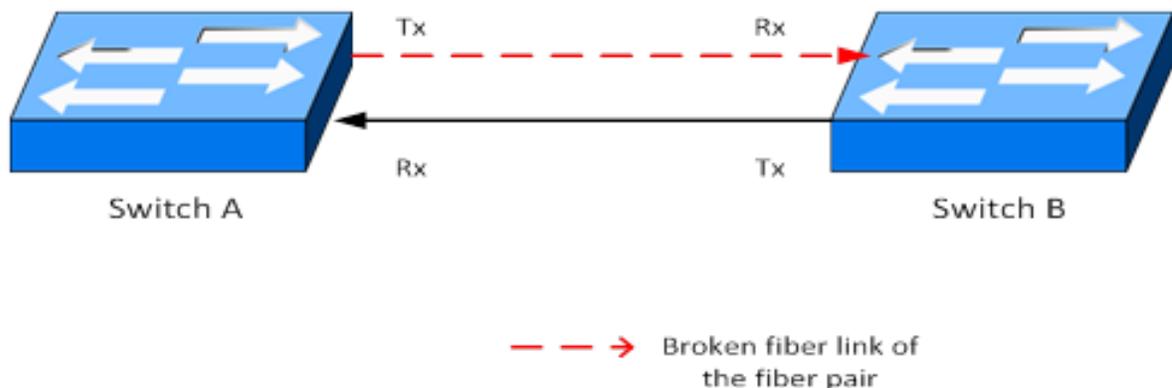
Figure 58: Link



DLDP can be enabled on a maximum of 128 ports with each DLDP enabled port can have up to 4 neighbors (with the exception of the switch 2530).

On the Switch 2530, DLDP can be enabled on a maximum of 12 ports with each DLDP enabled port allowed up to 4 neighborhoods.

Figure 59: Broken link





Mobile web interface is available on the following switches:

- Switch 2530
- Switch 2620

The Mobile Web Interface feature provides a subset of functionality currently available in the existing web interface but designed for use on mobile devices such as smart phone or tablet.

Viewing web management-to-server configurations

Use the command `Show web-management` to view the web management-to-server configuration.

The SSL Port is displayed only if HTTPS Access is enabled. The Idle Timeout and Support URL are displayed if either HTTP or HTTPS is enabled.

The following example shows the display of web management-to-server configuration.

```
show web-management

Web Management - Server Configuration
HTTP Access      : Enabled
HTTPS Access     : Enabled
SSL Port        : 433
Idle Timeout     : 7200 seconds
```

Validation rules

Validation	Error/Warning/Prompt
Valid VLAN-ID?	Invalid VLAN ID