



Release Notes: Version W.14.49 Software *for the HP ProCurve Series 2910al Switches*

These release notes include information on the following:

- W.14.49 is supported on the following switches:
 - HP ProCurve 2910al-24G Switch (J9145A)
 - HP ProCurve 2910al-24G-PoE+ Switch (J9146A)
 - HP ProCurve 2910al-48G Switch (J9147A)
 - HP ProCurve 2910al-48G-PoE+ Switch (J9148A)
- Download switch software and documentation from the Web ([page 1](#))
- Support notes and known issues ([page 8](#))
- A listing of software enhancements in recent releases ([page 10](#))
- A listing of software fixes ([page 78](#))
-

© Copyright 2010 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

5900-0244

July 2010

Applicable Product

HP ProCurve 2910al-24G Switch (J9145A)

HP ProCurve 2910al-24G-PoE+ Switch (J9146A)

HP ProCurve 2910al-48G Switch (J9147A)

HP ProCurve 2910al-48G-PoE+ Switch (J9148A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

SSH on ProCurve Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

[http:// www.openssh.com](http://www.openssh.com).

SSL on ProCurve Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

<http://www.openssl.org>.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.hp.com

Contents

Software Management	1
Download Switch Documentation and Software from the Web	1
Viewing or Downloading the Software Manual Set	1
Downloading Software Updates for Your Switch	1
TFTP Download from a Server	2
Xmodem Download From a PC or Unix Workstation	2
Saving Configurations While Using the CLI	4
ProCurve Switch, Routing Switch, and Router Software Keys	5
Minimum Software Versions for Series 2910al Switch Features	6
Operating System and Web Browser Compatibility Table	7
Clarifications	8
Virtual Stacking/Management VLANs	8
Known Issues	8
Version W.14.30	8
Version W.14.03	8
Enhancements	10
Version W.14.15 Enhancements	10
SNTP Client Authentication	10
Version W.14.28 Enhancements	19
Dynamic IP Lockdown	19
Additional Products Supported	27
Version W.14.31 Enhancements	27
Banner Enhancements	27
Extended Ping and Traceroute	28
Ping Error Message Improvement	28
TELNET Negotiate About Window Size (NAWS) Initiation Enhancement	28
Version W.14.35 Enhancements	29

Additional Products Supported	29
Version W.14.36 Enhancements	29
Enhancement to AAA Accounting	29
Version W.14.38 Enhancements	47
Unauthenticated VLAN Access (Guest VLAN Access) Enhancement	47
Version W.14.39 Enhancements	48
Access Control Debug Logging	48
Port-based Debug Logging Enhancement	51
Management Access Security Enhancements	51
Web Authentication Message Enhancement	54
Version W.14.40 Enhancements	60
Multicast ARP Support	60
Version W.14.44 Enhancements	60
SNMP Traps	60
Version W.14.47 Enhancements	65
Entry-count Parameter Added to “show” Command	65
Version W.14.49 Enhancements	65
Custom Default Configuration	65
LLDP PoE+ Enhancements	72
Software Fixes	78
Version W.14.03	78
Version W.14.04 through W.14.07	78
Version W.14.08 through W.14.10	78
Version W.14.11 through W.14.13	78
Version W.14.14	78
Version W.14.15	78
Version W.14.16	80
Version W.14.17 through W.14.25	80
Version W.14.26	81
Version W.14.27	81
Version W.14.28	81
Version W.14.29	83

Version W.14.30	84
Version W.14.31	86
Version W.14.32 through W.14.34	87
Version W.14.35	87
Version W.14.36	87
Version W.14.37	89
Version W.14.38	89
Version W.14.39	90
Version W.14.40	99
Version W.14.41	100
Version W.14.42	101
Version W.14.43	101
Version W.14.44	101
Version W.14.45	103
Version W.14.46	104
Version W.14.47	104
Version W.14.48	107
Version W.14.49	107

Software Management

Download Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from the HP Networking Web site. Check the Web site frequently for the latest software release available for your switch.

Viewing or Downloading the Software Manual Set

Go to: www.hp.com/networking/support and select **Manuals**.

You may want to bookmark this Web page for easy access in the future.

Downloading Software Updates for Your Switch

Switch software updates are available from the HP networking Web site www.hp.com/networking/software. After obtaining the software update file from the Web site, you can use one of the following methods to update the switch:

- 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.
 - Use the **copy tftp** command in the switch's CLI (see below).
- 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.
 - Use the **copy xmodem** command in the switch's CLI (page 2).
- Use the USB port to download a software file from a USB flash drive.
- Use the download utility in ProCurve Manager Plus.

Note

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, for archive purposes or to be used in another switch of the same model.

TFTP Download from a Server

This section describes how to use the Command Line Interface (CLI) to download software to the switch. You can also use the menu interface for software downloads. For more information, refer to the *Management and Configuration Guide* for your switch.

Syntax: `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 A_14_03.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve switch # copy tftp flash 10.28.227.103 W.14.03x.swi
The primary OS image will be deleted. continue [y/n]? Y
01403W
```

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 re-appears, 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 that holds the new software (primary or secondary), using the following command:

Syntax: `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.

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the Installation and Getting Started Guide you received with the switch 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 Windows NT, you would use the Send File option in the Transfer drop down menu.)

Using Xmodem and a terminal emulator, you can download a switch software file to either primary or secondary flash using the CLI.

Syntax: copy xmodem flash [< primary | secondary >]

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 115200 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:

```
ProCurve (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 logout of the switch and change your terminal emulator speed and allow the switch to AutoDetect your new higher baud rate (i.e. 115200 bps)

2. Execute the following command in the CLI:

```
ProCurve # 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 on **Transfer**, then **Send File**.
 - b. Type the file path and name in the **Filename** field.
 - c. In the Protocol field, select **Xmodem**.
 - d. Click on the **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 ([step 1](#)), use the same command to return it to its previous setting. (HP recommends a baud rate of 9600 bits per second 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 that holds the new software (primary or 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.

Saving Configurations While Using the CLI

The switch operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls switch operation. Rebooting the switch erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the running configuration to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the “permanent” configuration. When the switch reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

When you use the CLI to make a configuration change, the switch places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the switch reboots, the change will be lost. There are two ways to save configuration changes while using the CLI:

- Execute **write memory** from the Manager, Global, or Context configuration level.
- When exiting from the CLI to the Main Menu, press **[Y]** (for Yes) when you see the “save configuration” prompt:

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

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
A	Switch 2615-8-PoE and Switch 2915-8G-PoE
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	J.xx.xx.biz Secure Router 7000dl Series (7102dl and 7203dl) J.xx.xx.swi Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 3500 Series (3500-24, 3500-24-PoE, 3500-48 and 3500-48-PoE), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8200zl (8206zl and 8212zl) and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG, 6600-48G and 6600-48G-4XG).
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530

Software Letter	ProCurve Networking Products
WM	ProCurve Access Point 10ag
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	ProCurve 6120G/XG and 6120XG Blade Switches
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Minimum Software Versions for Series 2910al Switch Features

For Software Features. To view a tabular listing of major switch software features and the minimum software version each feature requires:

1. Visit the HP networking Web site at www.hp.com/networking/software.
2. Click on **HP ProCurve LAN Products software feature matrix**.

For Switch 2910al Hardware Accessories.

ProCurve Device	Minimum Supported Software Version
HP ProCurve 630 Redundant External Power Supply (J9443A)	W.14.35
HP ProCurve 10-GbE SFP+ 1m Cable (J9281B)	W.14.28
HP ProCurve 10-GbE SFP+ 3m Cable (J9283B)	W.14.28
HP ProCurve 10-GbE SFP+ 7m Cable (J9285B)	W.14.28
HP ProCurve 10-GbE SFP+ 1m Cable (J9281A)	W.14.03
HP ProCurve 10-GbE SFP+ 3m Cable (J9283A)	W.14.03
HP ProCurve 10-GbE SFP+ 7m Cable (J9285A)	W.14.03
HP ProCurve 10-GbE SFP+ SR Transceiver (J9150A)	W.14.03
HP ProCurve 10-GbE SFP+ LR Transceiver (J9151A)	W.14.03
HP ProCurve 10-GbE SFP+ LRM Transceiver (J9152A)	W.14.03
HP ProCurve 2910al-24G Switch (J9145A)	W.14.03
HP ProCurve 2910al-24G-PoE+ Switch (J9146A)	W.14.03
HP ProCurve 2910al-48G Switch (J9147A)	W.14.03
HP ProCurve 2910al-48G-PoE+ Switch (J9148A)	W.14.03

Operating System and Web Browser Compatibility Table

The switch Web agent supports the following combinations of computer operating system browsers:

Operating System	Tested Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Vista SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2003 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2008 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows 7	Internet Explorer 8 (IE 7 not supported) Firefox 3.0, 3.5
MAC OS	Firefox 3.0, 3.5 (IE 7 and IE 8 not supported)

Clarifications

The following clarification applies to documentation for the ProCurve Series 2910al Switches as of June 2009.

Virtual Stacking/Management VLANs

A ProCurve switch that is configured as a Stack Member can no longer be managed by the Stack Commander if it is also configured with a Management VLAN. This is by design. The Management VLAN is configured when the network administrator desires an isolated, non-routable VLAN for use in managing the network. Virtual Stacking is intended to conserve IP addresses on the network by allowing the management of up to 16 Switches through the IP address of the Commander Switch. Due to the expectation that Stack Members will not have their own IP address, stacking traffic was not designed to traverse a Management VLAN. Virtual Stacking and Management VLANs should therefore be considered mutually exclusive features.

Known Issues

Version W.14.30

The following known issues are open as of software version W.14.30.

- **CLI (PR_0000044047)** — Trunks with an invalid group name of “mesh” are present in the configuration even after updating to W.14.30. Note that meshing is not supported by the switch.

Version W.14.03

The following known issues are open as of software version W.14.03.

- **PoE (PR_0000016644)** — If the PoE portion of the power supply fails, the switch may still indicate that it is delivering PoE power to the ports when it is not.
- **Flow Control (PR_0000015824)** — Fiber ports do not notify the link partner of changes to the flow control configuration, resulting in a potential mismatch of flow control settings on each side of the link.
- **Redundant Power (PR_0000015519)** — When the switch is connected to Redundant Power Supply (RPS) only (the only part supported on the 2910al switches), and the power is removed from the HP ProCurve 620 RPS/EPS, power is lost to the PoE ports and is not restored when the HP ProCurve 620 is again powered up. A reload of the switch is required to restore PoE power delivery.

- **PoE (PR_0000014907)** — When a cable delivering 30W of class 4 power is physically disconnected from the switch, an over-current message is displayed. Note that the switch does remove power from the port appropriately, and the over-current counter for the port does not increase when this happens. The event log message is similar to the following.

00562 ports: port <number> PD Over Current indication.

Enhancements

This section lists only the software versions that contain enhancements. Enhancements are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each new software version includes all the enhancements added in the previous versions.

W.14.03 is the first software version for the HP ProCurve 2910al Switches.

Version W.14.15 Enhancements

SNTP Client Authentication

Version W.14.15 includes the following enhancements.

- **Enhancement (PR_0000010201)** — Support was added for SNTP client authentication.

Overview

Enabling SNTP authentication allows network devices such as HP ProCurve switches to validate the SNTP messages received from an NTP or SNTP server before updating the network time. NTP or SNTP servers and clients must be configured with the same set of authentication keys so that the servers can authenticate the messages they send and clients (HP ProCurve switches) can validate the received messages before updating the time.

This enhancement provides support for SNTP client authentication on HP ProCurve switches, which addresses security considerations when deploying SNTP in a network.

For more information about SNTP operation in general, see the chapter “Time Protocols” in the *Management and Configuration Guide* for your switch.

Requirements

The following must be configured to enable SNTP client authentication on the switch.

SNTP Client Authentication Support

- Timesync mode must be SNTP. Use the **timesync sntp** command. (SNTP is disabled by default.)
- SNTP must be in unicast or broadcast mode.
- The MD5 authentication mode must be selected.
- An SNTP authentication key-identifier (**key-id**) must be configured on the switch and a value (**key-value**) must be provided for the authentication key. A maximum of 8 sets of **key-id** and **key-value** can be configured on the switch.

- Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys will be used for SNTP authentication.
- If the SNTP server requires authentication, one of the trusted keys has to be associated with the SNTP server.
- SNTP client authentication must be enabled on the ProCurve switch. If client authentication is disabled, packets are processed without authentication. All of the above steps are necessary to enable authentication on the client.

SNTP Server Authentication Support

Note

SNTP server is not supported on ProCurve products.

The following must be performed on the SNTP server:

- The same authentication key-identifier, trusted key, authentication mode and key-value that were configured on the SNTP client must also be configured on the SNTP server.
- SNTP server authentication must be enabled on the server.

If any of the parameters on the server are changed, the parameters have to be changed on all the SNTP clients in the network as well. The authentication check will fail on the clients otherwise, and the SNTP packets will be dropped.

Configuring the Key-Identifier, Authentication Mode, and Key Value

This command configures the **key-id**, **authentication-mode**, and **key-value**, which are required for authentication. It is executed in the global configuration context.

Syntax: sntp authentication key-id <key-id> authentication-mode <md5> key-value <key-string> [trusted]
no sntp authentication key-id <key-id>

Configures a key-id, authentication-mode (MD5 only), and key-value, which are required for authentication.

*The **no** version of the command deletes the authentication key.*

Default: No default keys are configured on the switch.

key-id: *A numeric key identifier in the range of 1-4,294,967,295 (2^{32}) that identifies the unique key value. It is sent in the SNTP packet.*

key-value <key-string>: *The secret key that is used to generate the message digest. Up to 32 characters are allowed for <key-string>.*


```
ProCurve(config)# sntp authentication key-id 55 authentication-mode md5 key-  
value secretkey1
```

Figure 1. Example of Setting Parameters for SNTP Authentication

Configuring a Trusted Key

Trusted keys are used in SNTP authentication. In unicast mode, a **trusted** key must be associated with a specific NTP/SNTP server. That key is used for authenticating the SNTP packet.

In unicast mode, a specific server is configured on the switch so that the SNTP client communicates with the specified server to get the date and time.

In broadcast mode, the SNTP client switch checks the size of the received packet to determine if it is authenticated. If the broadcast packet is authenticated, the key-id value is checked to see if the same key-id value is configured on the SNTP client switch. If the switch is configured with the same key-id value and the key-id value is configured as “trusted”, the authentication succeeds. Only trusted key-id value information is used for SNTP authentication.

If the packet contains key-id value information that is not configured on the SNTP client switch or the received packet contains no authentication information, it is discarded. The SNTP client switch expects packets to be authenticated if SNTP authentication is enabled.

When authentication succeeds, the time in the packet is used to update the time on the switch.

Enter the following command to configure a **key-id** as **trusted**.

Syntax: sntp authentication key-id <key-id> trusted
no sntp authentication key-id <key-id> trusted

*Trusted keys are used during the authentication process. The switch can be configured with up to eight sets of key-id/key-value pairs. One specific set must be selected for authentication; this is done by configuring the set as **trusted**.*

*The **key-id** itself must already be configured on the switch. To enable authentication, at least one **key-id** must be configured as **trusted**.*

*The **no** version of the command indicates the key is unreliable (not trusted).*

Default: No key is trusted by default.

Associating a Key with an SNTP Server

After a key is configured, it must be associated with a specific server.

Syntax: [no] sntp server priority <1-3> <ip-address | ipv6-address> <version-num> [key-id <1-4,294,967,295>]

*Configures a **key-id** to be associated with a specific server. The key itself must already be configured on the switch.*

*The **no** version of the command disassociates the key from the server. This does not remove the authentication key.*

Default: No key is associated with any server by default.

priority: *Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.*

<version-num> *Specifies the SNTP software version to use, and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3.*

Default: 3; range: 1 - 7.

key-id: *Optional command. The key identifier (range 1-4,294,967,295) sent in the SNTP packet. This **key-id** will be associated with the SNTP server specified in the command.*

```
ProCurve(config)# sntp server priority 1 10.10.19.5 2 key-id 55
```

Figure 2. Example of Associating a Key-Id with a Specific Server

Enabling SNTP Client Authentication

The **sntp authentication** command enables SNTP client authentication on the switch. If SNTP authentication is not enabled, SNTP packets are not authenticated.

Syntax: [no] sntp authentication

Enables the SNTP client authentication

*The **no** version of the command disables authentication.*

Default: SNTP client authentication is disabled by default.

Configuring Unicast and Broadcast Mode

To enable authentication, either unicast or broadcast mode must be configured. When authentication is enabled, changing the mode from unicast to broadcast or vice versa is not allowed. You must disable authentication and then change the mode.

To set the SNTP mode or change from one mode to the other, enter the appropriate command.

Syntax: sntp unicast
 sntp broadcast

Enables SNTP for either broadcast or unicast mode.

*Default: SNTP mode is disabled by default. SNTP does not operate even if specified by the CLI **timesync** command or by the menu interface **Time Sync Method** parameter.*

Unicast: *Directs the switch to poll a specific server periodically for SNTP time synchronization. The default value between each polling request is 720 seconds but can be configured. At least one manually configured server IP address is required.*

Note: *At least one **key-id** must be configured as **trusted** and it must be associated with one of the SNTP servers. To edit or remove the associated **key-id** information or SNTP server information. SNTP authentication must be disabled.*

Broadcast: *Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval (configurable up to 720 seconds) expires three times without the switch detecting a time update from the original server, the switch accepts a broadcast time update from the next server it detects.*

Displaying SNTP Configuration Information

The **show sntp** command displays SNTP configuration information, including any SNTP authentication keys that have been configured on the switch.

```
ProCurve(config)# show sntp

SNTP Configuration

SNTP Authentication : Enabled
Time Sync Mode: Sntp
SNTP Mode : Unicast
Poll Interval (sec) [720] : 720


Priority SNTP Server Address                Protocol Version KeyId
-----
1         10.10.10.2                        3                 55
2         fe80::200:24ff:fec8:4ca8          3                 55
```

Figure 3. Example of SNTP Configuration Information

To display all the SNTP authentication keys that have been configured on the switch, enter the **show sntp authentication** command.

```
ProCurve(config)# show sntp authentication

SNTP Authentication Information

SNTP Authentication : Enabled


Key-ID  Auth Mode  Trusted
-----
55      MD5        Yes
10      MD5        No
```

Figure 4. Example of show sntp authentication Command Output

To display the statistical information for each SNTP server, enter the **sntp statistics** command. The number of SNTP packets that have failed authentication is displayed for each SNTP server address.

```
ProCurve(config)# show sntp statistics
SNTP Statistics

Received Packets : 0
Sent Packets     : 3
Dropped Packets  : 0

SNTP Server Address                                Auth Failed Pkts
-----
10.10.10.1                                           0
fe80::200:24ff:fec8:4ca8                           0
```

Figure 5. Example of SNTP Authentication Statistical Information

Saving Configuration Files and the Include-Credentials Command

You can use the **include-credentials** command to store security information in the running-config file. This allows you to upload the file to a TFTP server and then later download the file to the ProCurve switches on which you want to use the same settings. For more information about the **include-credentials** command, see “Configuring Username and Password Security” in the *Access Security Guide* for your switch.

The authentication key values are shown in the output of the **show running-config** and **show config** commands only if the **include-credentials** command was executed.

When SNTP authentication is configured and **include-credentials** has not been executed, the SNTP authentication configuration is not saved.

```
ProCurve(config)# show config

Startup configuration:

.
.
.
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
.
.
.
```

SNTP authentication has been enabled and a key-id of 55 has been created.

Figure 6. Example of Configuration File with SNTP Authentication Information

In [Figure 6](#), the **include-credentials** command has not been executed and is not present in the configuration file. The configuration file is subsequently saved to a TFTP server for later use. The SNTP authentication information is not saved and is not present in the retrieved configuration file, as shown in [Figure 7](#).

```
ProCurve(config)#copy tftp startup-config 10.2.3.44 config1
.
.
.
Switch reboots...

Startup configuration
.
.
.
timesync sntp
sntp broadcast
sntp 50 sntp server priority 1 10.10.10.2 3
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4
.
.
.
```

The **sntp authentication** line and the **key-ids** are not displayed. You must reconfigure SNTP authentication.

Figure 7. Example of a Retrieved Configuration File When Include Credentials is not Configured

If **include-credentials** is configured, the SNTP authentication configuration is saved in the configuration file. When the **show config** command is entered, all of the information that has been configured for SNTP authentication displays, including the key-values.

```
ProCurve(config)# show config
```

```
Startup configuration:
```

```
.
.
.
include-credentials
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp authentication key-id 55 authentication-mode md5 key-value "secretkey1"
trusted
sntp authentication key-id 2 authentication-mode md5 key-value "secretkey2"
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
sntp server priority 3 10.10.4.60 3
.
.
.
```

Include-credentials is configured.

All of the SNTP authentication information displays in the configuration file, including the key-values.

Figure 8. Example of Saved SNTP Authentication Information when include-credentials is Configured

Version W.14.28 Enhancements

Dynamic IP Lockdown

Version W.14.28 includes the following enhancements.

- **Enhancement (PR_0000010517)** — Support is added for Dynamic IP Lockdown.

The Dynamic IP Lockdown feature is used to prevent IP source address spoofing on a per-port and per-VLAN basis. When dynamic IP lockdown is enabled, IP packets in VLAN traffic received on a port are forwarded only if they contain a known source IP address and MAC address binding for the port. The IP-to-MAC address binding can either be statically configured or learned by the DHCP Snooping feature.

Protection Against IP Source Address Spoofing

Many network attacks occur when an attacker injects packets with forged IP source addresses into the network. Also, some network services use the IP source address as a component in their authentication schemes. For example, the BSD “r” protocols (rlogin, rcp, rsh) rely on the IP source address for packet authentication. SNMPv1 and SNMPv2c also frequently use authorized IP address lists to limit management access. An attacker that is able to send traffic that appears to originate from an authorized IP source address may gain access to network services for which he is not authorized.

Dynamic IP lockdown provides protection against IP source address spoofing by means of IP-level port security. IP packets received on a port enabled for dynamic IP lockdown are only forwarded if they contain a known IP source address and MAC address binding for the port.

Dynamic IP lockdown uses information collected in the DHCP Snooping lease database and through statically configured IP source bindings to create internal, per-port lists. The internal lists are dynamically created from known IP-to-MAC address bindings to filter VLAN traffic on both the source IP address and source MAC address.

The 2910al switches can have 8192 manual bindings in the DHCP Snoop table and 4096 of the bindings can be applied to DIPLD (Dynamic IP Lockdown) at 64 bindings/port.

Prerequisite: DHCP Snooping

Dynamic IP lockdown requires that you enable DHCP snooping as a prerequisite for its operation on ports and VLAN traffic:

- Dynamic IP lockdown only enables traffic for clients whose leased IP addresses are already stored in the lease database created by DHCP snooping or added through a static configuration of an IP-to-MAC binding.

Therefore, if you enable DHCP snooping after dynamic IP lockdown is enabled, clients with an existing DHCP-assigned address must either request a new leased IP address or renew their existing DHCP-assigned address. Otherwise, a client's leased IP address is not contained in the DHCP binding database. As a result, dynamic IP lockdown will not allow inbound traffic from the client.

- It is recommended that you enable DHCP snooping a week before you enable dynamic IP lockdown to allow the DHCP binding database to learn clients' leased IP addresses. You must also ensure that the lease time for the information in the DHCP binding database lasts more than a week.

Alternatively, you can configure a DHCP server to re-allocate IP addresses to DHCP clients. In this way, you repopulate the lease database with current IP-to-MAC bindings.

- The DHCP binding database allows VLANs enabled for DHCP snooping to be known on ports configured for dynamic IP lockdown. As new IP-to-MAC address and VLAN bindings are learned, a corresponding permit rule is dynamically created and applied to the port (preceding the final deny any vlan <VLAN_IDs> rule as shown in the example in Figure 3). These VLAN_IDs correspond to the subset of configured and enabled VLANs for which DHCP snooping has been configured.
- For dynamic IP lockdown to work, a port must be a member of at least one VLAN that has DHCP snooping enabled.
- Disabling DHCP snooping on a VLAN causes Dynamic IP bindings on Dynamic IP Lockdown-enabled ports in this VLAN to be removed. The port reverts back to switching traffic as usual.

Filtering IP and MAC Addresses Per-Port and Per-VLAN

This section contains an example that shows the following aspects of the Dynamic IP Lockdown feature:

- Internal Dynamic IP lockdown bindings dynamically applied on a per-port basis from information in the DHCP Snooping lease database and statically configured IP-to-MAC address bindings
- Packet filtering using source IP address, source MAC address, and source VLAN as criteria

In this example, the following DHCP leases have been learned by DHCP snooping on port 5. VLANs 2 and 5 are enabled for DHCP snooping.

IP Address	MAC Address	VLAN ID
10.0.8.5	001122-334455	2
10.0.8.7	001122-334477	2
10.0.10.3	001122-334433	5

Figure 9. Sample DHCP Snooping Entries

The following example shows an IP-to-MAC address and VLAN binding that have been statically configured in the lease database on port 5.

IP Address	MAC Address	VLAN ID
10.0.10.1	001122-110011	5

Figure 10. An Example of a Static Configuration Entry

Assuming that DHCP snooping is enabled and that port 5 is untrusted, dynamic IP lockdown applies the following dynamic VLAN filtering on port 5:

```
permit 10.0.8.5 001122-334455 vlan 2
permit 10.0.8.7 001122-334477 vlan 2
permit 10.0.10.3 001122-334433 vlan 5
permit 10.0.10.1 001122-110011 vlan 5
deny any vlan 1-10
permit any
```

Figure 11. Example of Internal Statements used by Dynamic IP Lockdown

Note that the **deny any** statement is applied only to VLANs for which DHCP snooping is enabled. The **permit any** statement is applied only to all other VLANs.

Enabling Dynamic IP Lockdown

To enable dynamic IP lockdown on all ports or specified ports, enter the **ip source-lockdown** command at the global configuration level. Use the no form of the command to disable dynamic IP lockdown.

Syntax: [no] ip source-lockdown [port-list]

Enables dynamic IP lockdown globally on all ports or on specified ports on the routing switch.

Operating Notes

- Dynamic IP lockdown is enabled at the port configuration level and applies to all bridged or routed IP packets entering the switch. The only IP packets that are exempt from dynamic IP lockdown are broadcast DHCP request packets, which are handled by DHCP snooping.
- DHCP snooping is a prerequisite for Dynamic IP Lockdown operation. The following restrictions apply:

- DHCP snooping is required for dynamic IP lockdown to operate. To enable DHCP snooping, enter the **dhcp-snooping** command at the global configuration level.
- Dynamic IP lockdown only filters packets in VLANs that are enabled for DHCP snooping. In order for Dynamic IP lockdown to work on a port, the port must be configured for at least one VLAN that is enabled for DHCP snooping.

To enable DHCP snooping on a VLAN, enter the **dhcp-snooping vlan [vlan-id-range]** command at the global configuration level or the **dhcp-snooping** command at the VLAN configuration level.

- Dynamic IP lockdown is not supported on a trusted port. (However, note that the DHCP server must be connected to a trusted port when DHCP snooping is enabled.)

By default, all ports are untrusted. To remove the trusted configuration from a port, enter the **no dhcp-snooping trust <port-list>** command at the global configuration level.

For more information on how to configure and use DHCP snooping, refer to the “Configuring Advanced Threat Protection” chapter in the *Access Security Guide*.

- After you enter the **ip source-lockdown** command (enabled globally with the desired ports entered in *<port-list>*), the dynamic IP lockdown feature remains disabled on a port if any of the following conditions exist:
 - If DHCP snooping has not been globally enabled on the switch.
 - If the port is not a member of at least one VLAN that is enabled for DHCP snooping.
 - If the port is configured as a trusted port for DHCP snooping.

Dynamic IP lockdown is activated on the port only after you make the following configuration changes:

- Enable DHCP snooping on the switch.
- Configure the port as a member of a VLAN that has DHCP snooping enabled.
- Remove the trusted-port configuration.
- You can configure dynamic IP lockdown only from the CLI; this feature cannot be configured from the web management or menu interface.
- If you enable dynamic IP lockdown on a port, you cannot add the port to a trunk.
- Dynamic IP lockdown must be removed from a trunk before the trunk is removed.

Adding an IP-to-MAC Binding to the DHCP Binding Database

A switch maintains a DHCP binding database, which is used for dynamic IP lockdown as well as for DHCP and ARP packet validation. The DHCP snooping feature maintains the lease database by learning the IP-to-MAC bindings of VLAN traffic on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

Dynamic IP lockdown supports a total of 4K static and dynamic bindings with up to 64 bindings per port. When DHCP snooping is enabled globally on a VLAN, dynamic bindings are learned when a client on the VLAN obtains an IP address from a DHCP server. Static bindings are created manually with the CLI or from a downloaded configuration file.

When dynamic IP lockdown is enabled globally or on ports the bindings associated with the ports are written to hardware. This occurs during these events:

- Switch initialization
- Hot swap
- A dynamic IP lockdown-enabled port is moved to a DHCP snooping-enabled VLAN
- DHCP snooping or dynamic IP lockdown characteristics are changed such that dynamic IP lockdown is enabled on the ports

Potential Issues with Bindings

- When dynamic IP lockdown enabled, and a port or switch has the maximum number of bindings configured, the client DHCP request will be dropped and the client will not receive an IP address through DHCP.
- When dynamic IP lockdown is enabled and a port is configured with the maximum number of bindings, adding a static binding to the port will fail.
- When dynamic IP lockdown is enabled globally, the bindings for each port are written to hardware. If global dynamic IP lockdown is enabled and disabled several times, it is possible to run out of buffer space for additional bindings. The software will delay adding the bindings to hardware until resources are available.

Adding a Static Binding

To add the static configuration of an IP-to-MAC binding for a port to the lease database, enter the **ip source-binding** command at the global configuration level. Use the **no** form of the command to remove the IP-to-MAC binding from the database.

Syntax: [no] ip source-binding <vlan-id> <ip-address> <mac-address> <port-number>

<i>vlan-id</i>	<i>Specifies a valid VLAN ID number to bind with the specified MAC and IP addresses on the port in the DHCP binding database.</i>
<i>ip-address</i>	<i>Specifies a valid client IP address to bind with a VLAN and MAC address on the port in the DHCP binding database.</i>
<i>mac-address</i>	<i>Specifies a valid client MAC address to bind with a VLAN and IP address on the port in the DHCP binding database.</i>
<i>port-number</i>	<i>Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.</i>

Note

Note that the **ip source-binding** command is the same command used by the Dynamic ARP Protection feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC address bindings.

Verifying the Dynamic IP Lockdown Configuration

To display the ports on which dynamic IP lockdown is configured, enter the **show ip source-lockdown status** command at the global configuration level.

Syntax: show ip source-lockdown status

An example of the **show ip source-lockdown status** command output is shown in Figure 12. Note that the operational status of all switch ports is displayed. This information indicates whether or not dynamic IP lockdown is supported on a port.

```
ProCurve(config)# show ip source-lockdown status
Dynamic IP Lockdown (DIPLD) Information

Global State: Enabled

      Port      Operational State
      -----
      A1        Active
      A2        Not in DHCP Snooping vlan
      A3        Disabled
      A4        Disabled
      A5        Trusted port, Not in DHCP Snooping vlan
      . . . . .
```

Figure 12. Example of show ip source-lockdown status Command Output

Displaying the Static Configuration of IP-to-MAC Bindings

To display the static configurations of IP-to-MAC bindings stored in the DHCP lease database, enter the **show ip source-lockdown bindings** command.

Syntax: show ip source-lockdown bindings [<port-number>]

port-number (Optional) Specifies the port number on which source IP-to-MAC address and VLAN bindings are configured in the DHCP lease database.

An example of the **show ip source-lockdown bindings** command output is shown in [Figure 13](#).

```
ProCurve(config)# show ip source-lockdown bindings
```

Dynamic IP Lockdown (DIPLD) Bindings

Mac Address	IP Address	VLAN	Port	Not in HW
-----	-----	-----	-----	-----
001122-334455	10.10.10.1	1111	X11	
005544-332211	10.10.10.2	2222	Trk11	YES
.

Figure 13. Example of show ip source-lockdown bindings Command Output

In the **show ip source-lockdown bindings** command output, the “Not in HW” column specifies whether or not (YES or NO) a statically configured IP-to-MAC and VLAN binding on a specified port has been combined in the lease database maintained by the DHCP Snooping feature.

Debugging Dynamic IP Lockdown

To enable the debugging of packets dropped by dynamic IP lockdown, enter the **debug dynamic-ip-lockdown** command.

Syntax: debug dynamic-ip-lockdown

To send command output to the active CLI session, enter the **debug destination session** command.

Counters for denied packets are displayed in the **debug dynamic-ip-lockdown** command output. Packet counts are updated every five minutes. An example of the command output is shown in [Figure 14](#).

When dynamic IP lockdown drops IP packets in VLAN traffic that do not contain a known source IP-to-MAC address binding for the port on which the packets are received, a message is entered in the event log.

```
ProCurve(config)# debug dynamic-ip-lockdown

DIPLD 01/01/90 00:01:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 1 packets
DIPLD 01/01/90 00:06:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 294 packets
DIPLD 01/01/90 00:11:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:16:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:21:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 299 packets
DIPLD 01/01/90 00:26:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:31:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:36:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 299 packets
DIPLD 01/01/90 00:41:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:46:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:51:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
DIPLD 01/01/90 00:56:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 299 packets
DIPLD 01/01/90 01:01:25 : denied ip 192.168.2.100 (0)
(PORT 4) -> 192.168.2.1 (0), 300 packets
```

Figure 14. Example of debug dynamic-ip-lockdown Command Output

Additional Products Supported

- **Enhancement (PR_0000039363)** — Support is added for the “B” version of HP ProCurve SFP+ Direct Attach Cables (DAC) listed below. The “B” version DACs are compliant with the January 2009 version of the Multi-Source Agreement (MSA), SFF-8472 Rev 10.4. Additionally, the “B” version DACs interoperate with the Intel NIC (Intel 10 Gigabit AF DA Dual Port Server Adapter).

J9281B HP ProCurve 10-GbE SFP+ 1m Cable

J9283B HP ProCurve 10-GbE SFP+ 3m Cable

J9285B HP ProCurve 10-GbE SFP+ 7m Cable

Version W.14.31 Enhancements

Banner Enhancements

- **Enhancement (PR_0000018513)** — Banner enhancements were made.

The enhancements to the Message of The Day (MOTD) banner apply to the following authentication types:

- Local
- RADIUS
- TACACS

The enhancements are:

- The MOTD banner size is increased to 1280 characters.
- If the MOTD is configured, the copyright, switch identification, and software version are not displayed on the splash screen; only the customer-defined banner is displayed.
- When passwords are configured on the switch, there will not be a prompt to “press any key to continue”. This prompt will still appear if a password is not configured.

Example Banner Configurations

Default Banner with No Password Configured. When the MOTD is not configured and there is no password, the default login page displays. The information includes the switch identification, software version, copyright statement and default banner. The “press any key to continue” prompt displays. When any key is pressed, the banner is cleared and the CLI prompt displays.

Default Banner with Password Configured. When passwords are configured on the switch, but the MOTD is not configured, the default login page displays. A prompt for the password appears. After a correct password is entered, the default banner clears and the CLI prompt displays.

Customized Banner without Password Configured. When a custom MOTD banner is configured and there is no password required, the custom MOTD banner displays followed by the “press any key to continue” prompt. When any key is pressed, the custom banner is cleared and the CLI prompt displays.

Customized Banner with Password Configuration. When a custom MOTD banner is configured on the switch and a password is required, the custom banner displays, followed by the password prompt. Entering the correct password clears the banner and displays the CLI prompt.

Extended Ping and Traceroute

- **Enhancement (PR_0000040721)** — Extended ping and traceroute are now available.

Ping Error Message Improvement

- **Enhancement (PR_0000042579)** — Error messages returned from ping were updated to include a relevant VLAN reference.

TELNET Negotiate About Window Size (NAWS) Initiation Enhancement

- **Enhancement (PR_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation.

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 an HP ProCurve 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.

Making Window Size Negotiation Available for a Telnet Session. 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 update 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.

Version W.14.35 Enhancements

Additional Products Supported

- **Enhancement (PR_0000044737)** — Support is added for the following new product.
J9443A - HP ProCurve 630 Redundant / External Power Supply
-

Version W.14.36 Enhancements

Enhancement to AAA Accounting

- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting.

Accounting Services

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot.

Accounting Service Types

The switch supports four types of accounting services:

- **Network accounting:** Provides records containing the information listed below on clients directly connected to the switch and operating under Port-Based Access Control (802.1X):
 - Acct-Session-Id
 - Acct-Status-Type
 - Acct-Terminate-Cause
 - Acct-Authentic
 - Acct-Delay-Time
 - Acct-Input-Packets
 - Acct-Output-Packets
 - Acct-Input-Octets
 - Nas-Port
 - Acct-Output-Octets
 - Acct-Session-Time
 - User-Name
 - Service-Type
 - NAS-IP-Address
 - NAS-Identifier
 - Calling-Station-Id
 - **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:
 - Acct-Session-Id
 - Acct-Status-Type
 - Acct-Terminate-Cause
 - Acct-Authentic
 - Acct-Delay-Time
 - Acct-Session-Time
 - User-Name
 - Service-Type
 - NAS-IP-Address
 - NAS-Identifier
 - Calling-Station-Id
-

- **System accounting:** Provides records containing the information listed below when system events occur on the switch, including system reset, system boot, and enabling or disabling of system accounting.

- Acct-Session-Id • Acct-Delay-Time • NAS-Identifier
- Acct-Status-Type • NAS-IP-Address

- **Commands accounting:** Provides records containing information on CLI command execution during user sessions.

- Acct-Session-Id • User-Name • Calling-Station-Id
- Acct-Status-Type • NAS-IP-Address • HP-Command-String
- Service-Type • NAS-Identifier • Acct-Delay-Time
- Acct-Authentic • NAS-Port-Type

The switch forwards the accounting information it collects to the designated RADIUS server, where the information is formatted, stored, and managed by the server. For more information on this aspect of RADIUS accounting, refer to the documentation provided with your RADIUS server.

Operating Rules for RADIUS Accounting

- You can configure up to four types of accounting to run simultaneously: exec, system, network, and command.
- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. Use **show radius** to view the order. As long as the first server is accessible and responding to authentication requests from the switch, a second or third server will not be accessed. (For more on this topic, refer to [“Changing RADIUS-Server Access Order” on page 46.](#))
- If access to a RADIUS server fails during a session, but after the client has been authenticated, the switch continues to assume the server is available to receive accounting data. Thus, if server access fails during a session, it will not receive accounting data transmitted from the switch.

Acct-Session-ID Options in a Management Session

The switch can be configured to support either of the following options for the accounting service types used in a management session. (Refer to [“Accounting Service Types” on page 29.](#))

- unique Acct-Session-ID for each accounting service type used in the same management session (the default)
- same Acct-Session-ID for all accounting service types used in the same management session

Unique Acct-Session-ID Operation. In the Unique mode (the default), the various service types running in a management session operate as parallel, independent processes. Thus, during a specific management session, a given service type has the same Acct-Session-ID for all accounting actions for that service type. However, the Acct-Session-ID for each service type differs from the ID for the other types.

Note

In Unique Acct-Session-ID operation, the Command service type is a special case in which the Acct-Session-ID for each executed CLI command in the session is different from the IDs for other service types used in the session *and also* different for each CLI command executed during the session. That is, the ID for each successive CLI command in the session is sequentially incremented from the ID value assigned to the immediately preceding CLI command in that session.

The figure below shows *Unique mode* accounting operation for a new session in which two commands are executed, and then the session is closed.

User "fred" starts Exec Accounting session "003300000008".	Acct-Session-Id = "003300000008" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Delay-Time = 0
User "fred" then executes show ip , which results in this accounting entry. Notice the session ID (003300000009) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This incrementing of the session ID is normal operation for command accounting in the (default) Unique mode.	Acct-Session-Id = "003300000009" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "show ip" Acct-Delay-Time = 0
User "fred" executes the logout command. The session ID (00330000000A) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This is another instance of normal Command accounting operation in the Unique mode.	Acct-Session-Id = "00330000000A" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "logout" Acct-Delay-Time = 0
Terminate Exec Accounting Session "003300000008"	Acct-Session-Id = "003300000008" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Terminate-Cause = User-Request Acct-Session-Time = 29 Acct-Delay-Time = 0

Figure 15. Example of Accounting in the (Default) Unique Mode

Common Acct-Session-ID Operation. In this case, all service types running in a given management session operate as subprocesses of the same parent process, and the same Acct-Session-ID is used for accounting of all service types, including successive CLI commands.

User "fred" starts Exec Accounting session "00330000000B".	<pre> Acct-Session-Id = "00330000000B" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Delay-Time = 0 </pre>
User "fred" then executes show ip , which results in this command accounting entry. Because this example assumes Common Mode configuration, the session ID (00330000000B) assigned to this accounting entry is identical to the session ID assigned when the session was opened. No incrementing of the session ID is done for individual commands.	<pre> Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "show ip" Acct-Delay-Time = 0 </pre>
User "fred" executes the logout command. The session ID (00330000000B) used for the earlier Exec and Command accounting entries continues to be the same as was originally assigned to the session.	<pre> Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "logout" Acct-Delay-Time = 0 </pre>
Terminate Exec Accounting Session "00330000000B"	<pre> Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Terminate-Cause = User-Request Acct-Session-Time = 29 Acct-Delay-Time = 0 </pre>

Figure 16. Example of Accounting in Common Mode (Same Session ID Throughout)

Configuring RADIUS Accounting

RADIUS Accounting Commands	Page
[no] radius-server host < ip-address >	35
[acct-port < port-number >]	35
[key < key-string >]	35
[no] aaa accounting < exec network system > < start-stop stop-only > radius	39
[no] aaa accounting commands < stop-only interim-update > radius	
aaa accounting session-id < unique common >	37
[no] aaa accounting update	40
periodic < 1 - 525600 > (in minutes)	
[no] aaa accounting suppress null-username	40
show accounting	45
show accounting sessions	46
show radius accounting	45

Note

This section assumes you have already:

- Configured RADIUS authentication on the switch for one or more access methods
 - Configured one or more RADIUS servers to support the switch
-

Steps for Configuring RADIUS Accounting

1. Configure the switch for accessing a RADIUS server.

You can configure a list of up to three RADIUS servers (one primary, two backup). The switch operates on the assumption that a server can operate in both accounting and authentication mode. (Refer to the documentation for your RADIUS server application.)

- Use the same **radius-server host** command that you would use to configure RADIUS authentication.
- Provide the following:
 - A RADIUS server IP address.
 - Optional—a UDP destination port for authentication requests. Otherwise the switch assigns the default UDP port (1812; recommended).

- Optional—if you are also configuring the switch for RADIUS authentication, and need a unique encryption key for use during authentication sessions with the RADIUS server you are designating, configure a server-specific key. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server.
2. (Optional) Reconfigure the desired Acct-Session-ID operation.
 - **Unique (the default setting):** Establishes a different Acct-Session-ID value for each service type, and incrementing of this ID per CLI command for the Command service type. (Refer to “[Unique Acct-Session-ID Operation](#)” on page 31.)
 - **Common:** Establishes the same Acct-Session-ID value for all service types, including successive CLI commands in the same management session.
 3. Configure accounting types and the controls for sending reports to the RADIUS server.
 - **Accounting types:**
 - exec (page 29)
 - network (page 29)
 - system (page 30)
 - commands (page 30)
 - **Trigger for sending accounting reports to a RADIUS server:** At session start and stop or only at session stop
 4. (Optional) Configure session blocking and interim updating options
 - **Updating:** Periodically update the accounting data for sessions-in-progress.
 - **Suppress accounting:** Block the accounting session for any unknown user with no user-name access to the switch.

1. Configure the Switch To Access a RADIUS Server. Before you configure the actual accounting parameters, you should first configure the switch to use a RADIUS server. You need to repeat this step here only if you have not yet configured the switch to use a RADIUS server, your server data has changed, or you need to specify a non-default UDP destination port for accounting requests. Note that switch operation expects a RADIUS server to accommodate both authentication and accounting.

Syntax: [no] radius-server host < ip-address >

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration.*

[acct-port < port-number >]

Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option, the switch automatically assigns the default accounting port number. (Default: 1813)

[key < key-string >]

Optional. Specifies an encryption key for use during accounting or authentication sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.

Note: *If you save the config file using Xmodem or TFTP, the key information is not saved in the file. This causes RADIUS authentication to fail when the config file is loaded back onto the switch.*

For example, suppose you want the switch to use the RADIUS server described below for both authentication and accounting purposes.

- IP address: 10.33.18.151
- A non-default UDP port number of 1750 for accounting.
- An encryption key of “source0151” for accounting sessions.

For this example, assume that all other RADIUS authentication parameters for accessing this server are acceptable at their default settings, and that RADIUS is already configured as an authentication method for one or more types of access to the switch (Telnet, Console, etc.).

```
ProCurve(config)# radius-server host 10.33.18.151 acct-port 1750 key source0151
ProCurve(config)# write mem
ProCurve(config)# show radius
```

Status and Counters - General RADIUS Information

```
Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :
```

Server IP Addr	Auth Port	Acct Port	Encryption Key
10.33.18.151	1812	1750	source0151

Because the radius-server command includes an **acct-port** keyword with a non-default UDP port number of 1750, the switch assigns this value as the UDP accounting port.

Figure 17. Example of Configuring for a RADIUS Server with a Non-Default Accounting UDP Port Number

The radius-server command as shown in [Figure 17](#), above, configures the switch to use a RADIUS server at IP address 10.33.18.151, with a (non-default) UDP accounting port of 1750, and a server-specific key of “source0151”.

2. (Optional) Reconfigure the Acct-Session-ID Operation.

Syntax: aaa accounting session-id < unique | common >

Optional command to reconfigure the Acct-Session-ID mode to apply to the accounting service type records for a given management session.

unique: *Configures the switch to use a different Acct-Session-ID for each accounting service type. (Default setting)*

common: *Configures the switch to apply the same Acct-Session-ID to all accounting service types in the same management session.*

For more on these options, refer to [“Acct-Session-ID Options in a Management Session”](#) on page 30.

```
ProCurve(config)# aaa accounting session-id common
ProCurve(config)# show accounting

Status and Counters - Accounting Information

Interval(min) : 0
Suppress Empty User : No
Sessions Identification : Common

Type      | Method Mode
-----+-----
Network   | None
Exec      | None
System    | None
Commands  | None
```

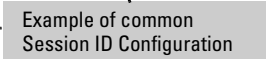


Figure 18. Accounting Configured for the Common Option

3. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server. Accounting Service Types.

Configure one or more accounting service types to track:

- **Exec:** Use **exec** if you want to collect accounting information on login sessions on the switch via the console, Telnet, or SSH.

- **System:** Use **system** if you want to collect accounting data when:
 - A system boot or reload occurs
 - System accounting is turned on or off

Note that there is no time span associated with using the **system** option. It simply causes the switch to transmit whatever accounting data it currently has when one of the above events occurs.

- **Network:** Use **network** if you want to collect accounting information on 802.1X port-based-access to the network by users connected to the physical ports on the switch.
- **Commands:** When commands accounting is enabled, an accounting notice record is sent after the execution of each command.

Accounting Controls. These options are enabled separately, and define how the switch will send accounting data to a RADIUS server:

- **Start-Stop:** Applies to the **exec**, **network**, and **system** accounting service types:
 - Send a “start record accounting” notice at the beginning of the accounting session and a “stop record notice” at the end of the session. Both notices include the latest data the switch has collected for the requested accounting type.
 - Do not wait for an acknowledgement.
- **Stop-Only:** Applies to the **network**, **exec**, **system**, and **command** service types, as described below:
 - Send a stop record accounting notice at the end of the accounting session. The notice includes the latest data the switch has collected for the requested accounting type (**network**, **exec**, or **system** service types). For the **commands** service type, sends the “Stop” accounting notice after execution of each CLI command.
 - Do not wait for an acknowledgment.
- **Interim-Update:** Applies only to the **command** service type, and is intended for use when the optional **common** session ID is configured. Enabling **interim-update** in this case results in the command accounting records appearing as enclosed sub-parts of the **exec** service type record for a given management session. (Using interim-update when the **unique** session ID is configured has no effect because in this case, the different service types appear as separate accounting processes with separate Acct-Session-ID values.

Note

Configuring **interim-update** for Command accounting results in all commands being reported as “update” records, regardless of whether common or unique is configured for the accounting session ID (page 37).

Syntax: [no] aaa accounting < exec | network | system > < start-stop | stop-only > radius
[no] aaa accounting command < stop-only | interim-only > radius

Configures RADIUS accounting service type and how data will be sent to the RADIUS server.

< exec | network | system | command >: *Specifies an accounting service type to configure. Refer to “Accounting Service Types” on page 37.*

start-stop: *Applies to exec, network, and system accounting service types. Refer to “Accounting Controls” on page 38.*

stop-only: *Applies to all accounting service types. Refer to “Accounting Controls” on page 38.*

interim-update: *Applies to the commands accounting service type. Refer to “Accounting Controls” on page 38*

Example. To configure RADIUS accounting on the switch with **start-stop** for Exec functions, **stop-only** for system functions, and **interim-update** for **commands** functions. This example continues from figure 18, where the session ID was configured as **common**.

```
ProCurve(config)# aaa accounting exec start-stop radius
ProCurve(config)# aaa accounting system stop-only radius
ProCurve(config)# aaa accounting commands interim-update radius
ProCurve(config)# show accounting
```

Status and Counters - Accounting Information

```
Interval(min) : 0
Suppress Empty User : No
Sessions Identification : Common
```

Type	Method	Mode
Network	None	
Exec	Radius	Start-Stop
System	Radius	Stop-Only
Commands	Radius	Interim-Update

Common is configured to apply the same Acct-Session-ID to all accounting records for a given switch management session.

Exec, System, and Commands accounting are active. (Assumes the switch is configured to access a reachable RADIUS server.)

Figure 19. Example of Configuring Accounting Types and Controls

Example. If the switch is configured with RADIUS accounting on the switch to use **start-stop** for Exec, System, and Command functions, as shown in [Figure 20](#), there will be an “Accounting-On” record when the switch boots up and an “Accounting-Off” record when the switch reboots or reloads. (Assume that Acct-Session-Id is configured for **common**.)

Record of Switch Bootstrap	Acct-Session-Id = "003600000001" Acct-Status-Type = Accounting-On NAS-IP-Address = 1.1.1.15 NAS-Identifier = "gsf_dosx_15" Acct-Delay-Time = 5
Record of User Session Start	Acct-Session-Id = "003600000002" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = Local NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" Calling-Station-Id = "0.0.0.0" Acct-Delay-Time = 0
Record of reload Command Issued	Acct-Session-Id = "003600000002" Acct-Status-Type = Interim-Update Service-Type = NAS-Prompt-User Acct-Authentic = Local NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "0.0.0.0" HP-Command-String = "reload" Acct-Delay-Time = 0
Record of System Accounting Off When Switch Reboots	Acct-Session-Id = "003600000001" Acct-Status-Type = Accounting-Off NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" Acct-Delay-Time = 0

Figure 20. Example of Accounting Session Operation with “start-stop” Enabled

4. (Optional) Configure Session Blocking and Interim Updating Options. These optional parameters give you additional control over accounting data.

- **Updates:** In addition to using a Start-Stop or Stop-Only trigger, you can optionally configure the switch to send periodic accounting record updates to a RADIUS server.
- **Suppress:** The switch can suppress accounting for an unknown user having no user name.

Syntax: [no] aaa accounting update periodic < 1 - 525600 >

*Sets the accounting update period for all accounting sessions on the switch. (The **no** form disables the update function and resets the value to zero.) (Default: zero; disabled)*

Syntax: [no] aaa accounting suppress null-username

Disables accounting for unknown users having no username. (Default: suppression disabled)

To continue the example in [Figure 19](#), suppose that you wanted the switch to:

- Send updates every 10 minutes on in-progress accounting sessions.
- Block accounting for unknown users (no username).

```
ProCurve(config)# aaa accounting update periodic 10
ProCurve(config)# aaa accounting suppress null-username
ProCurve(config)# show accounting
Status and Counters - Accounting Information

Interval(min) : 10
Suppress Empty User : Yes
Sessions Identification : Common

Type      | Method Mode
-----+-----
Network   | None
Exec      | Radius Start-Stop
System    | Radius Stop-Only
Commands  | Radius Interim-Update
```




Figure 21. Example of Optional Accounting Update Period and Accounting Suppression on Unknown User

Viewing RADIUS Statistics

General RADIUS Statistics

Syntax: show radius [host < ip-addr>]

*Shows general RADIUS configuration, including the server IP addresses. Optional form shows data for a specific RADIUS host. To use **show radius**, the server's IP address must be configured in the switch, which. requires prior use of the **radius-server host** command. (See [“Configuring RADIUS Accounting” on page 34.](#))*

```
ProCurve(config)# show radius
Status and Counters - General RADIUS Information
Deadtime(min) : 5
Timeout(secs) : 10
Retransmit Attempts : 2
Global Encryption Key : myg10balkey

                Auth  Acct
Server IP Addr  Port  Port  Encryption Key
-----
192.33.12.65    1812 1813  my65key
```

Figure 22. Example of General RADIUS Information from Show Radius Command

```
ProCurve(config)# show radius host 192.33.12.65
Status and Counters - RADIUS Server Information
Server IP Addr : 192.33.12.65
Authentication UDP Port : 1812           Accounting UDP Port : 1813
Round Trip Time       : 2               Round Trip Time       : 7
Pending Requests      : 0               Pending Requests      : 0
Retransmissions       : 0               Retransmissions       : 0
Timeouts              : 0               Timeouts              : 0
Malformed Responses   : 0               Malformed Responses   : 0
Bad Authenticators    : 0               Bad Authenticators    : 0
Unknown Types         : 0               Unknown Types         : 0
Packets Dropped       : 0               Packets Dropped       : 0
Access Requests       : 2               Accounting Requests    : 2
Access Challenges     : 0               Accounting Responses   : 2
Access Accepts        : 0
Access Rejects        : 0
```

Figure 23. RADIUS Server Information From the Show Radius Host Command

Table 1. Values for Show Radius Host Output

Term	Definition
Round Trip Time	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.
Access Requests	The number of RADIUS Access-Requests the switch has sent since it was last rebooted. (Does not include retransmissions.)
Accounting Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Responses	The number of RADIUS packets received on the accounting port from this server.

RADIUS Authentication Statistics

Syntax: show authentication

Displays the primary and secondary authentication methods configured for the Console, Telnet, Port-Access (802.1X), and SSH methods of accessing the switch. Also displays the number of access attempts currently allowed in a session.

show radius authentication

*Displays NAS identifier and data on the configured RADIUS server and the switch's interactions with this server. (Requires prior use of the **radius-server host** command to configure a RADIUS server IP address in the switch. See ["Configuring RADIUS Accounting" on page 34.](#))*

```
ProCurve(config)# show authentication
Status and Counters - Authentication Information
Login Attempts : 3
Respect Privilege : Disabled
```

Access Task	Login Primary	Login Secondary	Enable Primary	Enable Secondary
Console	Local	None	Local	None
Telnet	Radius	None	Radius	None
Port-Access	Local	None		
Webui	Local	None	Local	None
SSH	Radius	None	Radius	None
Web-Auth	ChapRadius	None		
MAC-Auth	ChapRadius	None		

Figure 24. Example of Login Attempt and Primary/Secondary Authentication Information from the Show Authentication Command

```
ProCurve(config)# show radius authentication
Status and Counters - RADIUS Authentication Information
NAS Identifier : ProCurve
Invalid Server Addresses : 0
```

Server IP Addr	UDP Port	Timeouts	Requests	Challenges	Accepts	Rejects
192.33.12.65	1812	0	2	0	2	0

Figure 25. Example of RADIUS Authentication Information from a Specific Server

RADIUS Accounting Statistics

Syntax: show accounting

Lists configured accounting interval, “Empty User” suppression status, session ID, accounting types, methods, and modes.

show radius accounting

*Lists accounting statistics for the RADIUS server(s) configured in the switch (using the **radius-server host** command).*

show accounting sessions

Lists the accounting sessions currently active on the switch.

```
ProCurve(config)# show accounting

Status and Counters - Accounting Information

Interval(min) : 5
Suppress Empty User : No
Sessions Identification : Common

Type      | Method Mode
-----+-----
Network   | None
Exec      | Radius Start-Stop
System    | Radius Stop-Only
Commands  | Radius Interim-Update
```

Figure 26. Listing the Accounting Configuration in the Switch

```
ProCurve(config)# show radius accounting

Status and Counters - RADIUS Accounting Information

NAS Identifier : ProCurve
Invalid Server Addresses : 0

                UDP
Server IP Addr  Port  Timeouts  Requests  Responses
-----
192.33.12.65   1813  0         1         1
```

Figure 27. Example of RADIUS Accounting Information for a Specific Server

```
ProCurve(config)# show accounting sessions

Active Accounted actions on SWITCH, User (n/a) Priv (n/a),
Acct-Session-Id 0x013E000000006, System Accounting record, 1:45:34 Elapsed
system event 'Accounting On
```

Figure 28. Example Listing of Active RADIUS Accounting Sessions on the Switch

Changing RADIUS-Server Access Order

The switch tries to access RADIUS servers according to the order in which their IP addresses are listed by the **show radius** command. Also, *when you add a new server IP address, it is placed in the highest empty position in the list.*

Adding or deleting a RADIUS server IP address leaves an empty position, but does not change the position of any other server addresses in the list. For example if you initially configure three server addresses, they are listed in the order in which you entered them. However, if you subsequently remove the second server address in the list and add a new server address, the new address will be placed second in the list.

Thus, to move a server address up in the list, you must delete it from the list, ensure that the position to which you want to move it is vacant, and then re-enter it. For example, suppose you have already configured the following three RADIUS server IP addresses in the switch:

```
ProCurve(config)# show radius
Status and Counters - General RADIUS Information
Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key : 10keyq
```

Server IP Addr	Auth Port	Acct Port	Encryption Key
10.10.10.1	1812	1813	
10.10.10.2	1812	1813	
10.10.10.3	1812	1813	

RADIUS server IP addresses listed in the order in which the switch will try to access them. In this case, the server at IP address 10.10.10.1 is first.

Note: If the switch successfully accesses the first server, it does not try to access any other servers in the list, even if the client is denied access by the first server.

Figure 29. Search Order for Accessing a RADIUS Server

Version W.14.38 Enhancements

Unauthenticated VLAN Access (Guest VLAN Access) Enhancement

Version W.14.38 includes the following enhancement.

■ **Enhancement (PR_0000038652)** - Unauthenticated VLAN Access (Guest VLAN Access).

When a PC is connected through an IP phone to a switch port that has been authorized using 802.1X or Web/MAC authentication, the IP phone is authenticated using client-based 802.1X or Web/MAC authentication and has access to secure, tagged VLANs on the port. If the PC is unauthenticated, it needs to have access to the insecure guest VLAN (unauthenticated VLAN) that has been configured for 802.1X or Web/MAC authentication. 802.1X and Web/MAC authentication normally do not allow authenticated clients (the phone) and unauthenticated clients (the PC) on the same port.

Mixed port access mode allows 802.1X and Web/MAC authenticated and unauthenticated clients on the same port when the guest VLAN is the same as the port's current untagged authenticated VLAN for authenticated clients, or when none of the authenticated clients are authorized on the untagged authenticated VLAN. Instead of having just one client per port, multiple clients can use the guest VLAN.

Authenticated clients always have precedence over guests (unauthenticated clients) if access to a client's untagged VLAN requires removal of a guest VLAN from the port. If an authenticated client becomes authorized on its untagged VLAN as the result of initial authentication or because of an untagged packet from the client, then all 802.1X or Web/MAC authenticated guests are removed from the port and the port becomes an untagged member of the client's untagged VLAN.

Characteristics of Mixed Port Access Mode

- The port keeps tagged VLAN assignments continuously.
- The port sends broadcast traffic from the VLANs even when there are only guests authorized on the port.
- Guests cannot be authorized on any tagged VLANs.
- Guests can use the same bandwidth, rate limits and QoS settings that may be assigned for authenticated clients on the port (via RADIUS attributes).
- When no authenticated clients are authorized on the untagged authenticated VLAN, the port becomes an untagged member of the guest VLAN for as long as no untagged packets are received from any authenticated clients on the port.
- New guest authorizations are not allowed on the port if at least one authenticated client is authorized on its untagged VLAN and the guest VLAN is not the same as the authenticated client's untagged VLAN.

Note

If you disable mixed port access mode, this does not automatically remove guests that have already been authorized on a port where an authenticated client exists. New guests are not allowed after the change, but the existing authorized guests will still be authorized on the port until they are removed by a new authentication, an untagged authorization, a port state change, and so on.

Configuring Mixed Port Access Mode

Syntax: [no] aaa port-access <port-list> mixed

Enables or disables guests on ports with authenticated clients.

Default: Disabled; guests do not have access

```
ProCurve(config)# aaa port-access 6 mixed
```

Figure 30. Example of Configuring Mixed Port Access Mode

Version W.14.39 Enhancements

Version W.14.39 includes the following enhancements.

Access Control Debug Logging

■ Enhancement (PR_0000016657) — Access Control Debug Logging

Debug logging provides real-time messages on the status of processes running on the switch. The access control changes deal mainly with the client authentication process.

The debug options include a new security branch that contains all the security features. The existing options are moved under a parent option of “security”. The new options also reside under the parent security option.

Existing Security Debug Options	New Security Debug Options
SSH	Radius
Dynamic Arp	Web-Auth (has subnodes)
Dsnoop	Port Access
agent	authenticator (802.1X)
events	mac-based
packets	supplicant (802.1X)
	web-based
Dynamic IP Lockdown	TACACS
	Port Security
	User Profile MIB

For more information about debug events, see “Using the Event Log for Troubleshooting Switch Problems” in the *Troubleshooting* chapter of the *Management and Configuration Guide* for your switch.

Syntax: debug security [arp-protect | dhcp-snooping | dynamic-ip-lockdown | port-access | port-security | radius-server | ssh | tacacs-server | user-profile-mib]

Displays debug messages for the selected option.

Default: Option is disabled.

```
ProCurve(config)# debug security ssh info
ProCurve(config)# debug security dhcp-snooping agent
ProCurve(config)# debug security port-access mac-based

ProCurve(config)# show debug

Debug Logging

Source IP Selection: Outgoing Interface
Destination:      Session

Enabled debug types:
security ssh (info)
security dhcp-snooping agent
security port-access mac-based
```

Figure 31. Example of Enabling Debug Messages for Selected Security Options

Events Logged

802.1X, Web/MAC, IDM, and DCA Authentication Debug Log Events

- A client authentication request is sent to RADIUS for a specific client on a port.
- A client authentication response is received from RADIUS for a specific client on a port.
- Access denied on a port because of conflicts with RADIUS-assigned attributes (VLAN).
- Displays RADIUS-assigned switch attributes for each user authenticated on the switch. VLAN attributes include tagged or untagged.
- Provides information on authentication process for a client, for example, client A detected on port B.
- Provides information about credentials obtained from a client if the client is rejected by the RADIUS server and placed on the Guest VLAN.
- Reauth timer information for Web Authentication.
- For Web Authentication, provides information on the protocols that are spoofed by Web Authentication (DHCP, DNS, ARP, EWA, redirect).
- When a client moves from one port to another, when enabled.
- When a client is deauthenticated due to reauth period, logoff period, or forced reauth.

Port Security Debug Log Events

- MAC addresses added through 802.1X or Web MAC authentication.
- MAC addresses that have been added, removed, learned, or aged on a port-security enabled port.

User Profile MIB Debug Log Events

- All clients that are added or removed from the user profile MIB through SNMP.

RADIUS and TACACS+ Debug Log Events

These debug log events cover management interface authentications (telnet, ssh, http, etc.) as well as access control authentication requests.

- Provides information about all RADIUS or TACACS+ request packets sent, for example, RADIUS request sent to server A for Client B on port 2.
- Provides information on all RADIUS or TACACS+ response packets received, for example, RADIUS response received on server A for Client B on port 2.
- All retries and timeouts for RADIUS or TACACS+ requests.
- All RADIUS drops due to bad attributes.

Port-based Debug Logging Enhancement

■ **Enhancement (PR_0000042147, PR_0000042840)**— Port-Based Debug Logging Enhancement

This enhancement provides debug logging with the ability to filter debug messages related to a specific set of configured ports. When the port filter is enabled for a debug type, only the messages that have inherently refer to a specific port will be filtered. All other messages for that debug type will still be sent to debug logging. The CLI command for this enhancement is below.

```
Switch# debug <security> <port-access | port-security | user-  
profile-mib> <optional detailed debug type> include port [PORT-LIST]
```

The following is used to remove all ports:

```
Switch# [no] debug <security> <port-access | port-security |  
user-profile-mib> <optional detailed debug type> include port
```

Management Access Security Enhancements

■ **Enhancement (PR_0000045680)**—Management Access Security Enhancements

This feature allows the configuration of access methods for IP Authorized Manager entries. Each of the management access methods will have its own set of authorized managers. The access methods include:

- SSH
- Telnet
- Web
- TFTP
- SNMP

You can configure the access method via the CLI, the menu, or through the web interface. The menu interface only supports IPv4. The following restrictions apply to all three methods of configuration.

- When no IP authorized manager rules are configured, the access method feature is disabled, that is, access is not denied.
- If the Management VLAN is configured, access can only be on that VLAN.
- Using the access method feature is optional. If no access method is configured, the access method defaults to “all”.
- If access is not specified, it defaults to “manager”.
- The IP mask defaults to 255.255.255.255.
- Up to 100 IP authorized manager entries are allowed.

Setting the Management Access Method—CLI

Enter the following command to configure the management access method using the CLI.

Syntax: [no] ip authorized-managers <ip-address> <ip-mask>> access [manager | operator]
access-method [all | ssh | telnet | web | snmp | tftp]
[no] ipv6 authorized-managers <ip-address> <ip-mask> access [manager | operator]
access-method [all | ssh | telnet | web | snmp | tftp]

Configures one or more authorized IP addresses.

access [manager | operator]

Configures the privilege level for <ip-address>. Applies only to access through telnet, SSH, SNMPv1, SNMPv2c, and SNMPv3.

Default: manager

access-method [all | ssh | telnet | web | snmp | tftp]

Configures access levels by access method and IP address. Each management method can have its own set of authorized managers.

Default: all

```
ProCurve(config)# ip authorized-managers 10.10.10.2 255.255.255.255 manager  
access-method ssh
```

Figure 32. Example of Configuring IP Authorized Manager Access Method SSH

```
ProCurve(config)# show ip authorized-manager  
  
IPv4 Authorized Managers  
-----  
  
Address : 10.10.10.10  
Mask    : 255.255.255.255  
Access  : Manager  
Access Method : ssh
```

Figure 33. Example of show authorized-managers Command with Access Method Configured

Setting the Management Access Method—Menu

Only IPv4 is supported when using the menu to set the management access method.

To access the menu screen, type **menu** at the switch prompt, then select **2. Switch Configuration**, then **6. IP Authorized Managers**. The menu screen for IP Managers displays. Click on **Edit** to make changes.

ProCurve		22-Apr-2008 20:17:53	
=====-- CONSOLE - MANAGER MODE =====			
Switch Configuration - IP Managers			
Authorized Manager IP	IP Mask	Access Level	Access Method
-----	-----	-----	-----
10.10.240.2	255.255.255.255	Manager	all
10.10.245.3	255.255.255.255	Operator	ssh
10.10.246.200	255.255.255.255	Operator	tftp
10.10.245.30	255.255.255.0	Operator	ssh
Actions->	Back	Add	Edit Delete Help

Figure 34. Example of Menu Showing Authorized Managers with Access Method

ProCurve	22-Apr-2008	20:17:53			
=====-- CONSOLE - MANAGER MODE =====					
Switch Configuration - IP Managers					
Authorized Manager IP: 10.10.245.3					
IP Mask [255.255.255.255]:255.255.255.255					
Access Level:Operator					
Access Method:ssh					
Actions->	Back	Add	Edit	Delete	Help

Figure 35. Example of Edit Menu for IP Managers

Setting the Management Access Method—Web Interface

To set the management access method in the web interface, click on the **Security** tab, and then click on the **Authorized Addresses** button. Fill in the fields with the correct information and click **Add**.

The Authorized Managers IP list in the web interface is the same list that was configured with the **ip authorized-managers** command in the CLI.

The screenshot displays the 'Authorized Addresses' configuration page. At the top, there are tabs for 'Identity', 'Status', 'Configuration', 'Security' (selected), and 'Diagnostics'. Under 'Security', there are sub-tabs: 'Device Passwords', 'Authorized Addresses' (selected), 'Port Security', and 'Intrusion Log'. The main area is titled 'Authorized IP Manager List' and contains a table with the following data:

Authorized Manager IP	IP Mask	Access Method	Access Level
10.10.10.10	255.255.255.255	all	Manager

Below the table, there are configuration options:

- Authorized Manager IP Type:** A dropdown menu set to 'IPv4'.
- IPv4/IPv6 Authorized Manager Address:** An empty text input field.
- Access Method:** A dropdown menu set to 'all'.
- IPv4 Subnet Mask/ IPv6 Prefix Length:** A text input field containing '255.255.255.255'. A tooltip explains: 'This allows you to specify which bits in the Manager IP address to compare against when validating an authorized manager.'
- Buttons: 'Add', 'Replace', and 'Delete'.

Figure 36. Example of Configuring Authorized Manager Access Method in the Web Interface

See “Using Authorized IP Managers” in the *Access Security Guide* for your switch for more information about authorized IP managers.

Web Authentication Message Enhancement

■ Enhancement (PR_0000045711)—Web Authentication Message Enhancement

This feature allows administrators to configure custom messages that are displayed when authentication with the RADIUS server fails. The messages are appended to the existing internal web page that displays during the authentication process. Messages can be configured using the CLI, or centrally using the RADIUS server, and can provide a description of the reason for the failure as well as possible steps to take to resolve the authentication issue. There is no change to the current web authentication functionality..

Syntax: [no] aaa port-access web-based access-denied-message <<access-denied-str> | radius-response>

Specifies the text message (ASCII string) shown on the web page after an unsuccessful login attempt. The message must be enclosed in quotes.

*The **no** form of the command means that no message is displayed upon failure to authenticate.*

Default: The internal web page is used. No message will be displayed upon authentication failure.

access-denied-str: *The text message that is appended to the end of the web page when there is an unsuccessful authentication request. The string can be up to 256 ASCII characters.*

radius-response: *Use the text message provided in the RADIUS server response to the authentication request.*

```
ProCurve(config)# aaa port-access web-based access-denied-message "Please
contact your system administrator to obtain authentication privileges."
```

Figure 37. Example of Configuring an Access Denied Message on the Switch

```
ProCurve(config)# show port-access web-based config

Port Access Web-based Configuration

DHCP Base Address      : 192.168.0.0
DHCP Subnet Mask       : 255.255.248.0
DHCP Lease Length      : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message : Custom:
    Please contact your system administrator to obtain authentication privileges.
```

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-auth Period	Unauth VLAN ID	Auth VLAN ID	Ctrl Dir
A1	Yes	1	No	300	60	1	2	both
A2	Yes	18	No	999999999	999999999	0	0	both
A3	Yes	22	No	999999999	999999999	4096	4096	both

Figure 38. Example of Output showing the Custom Access Denied Message

The example in [Figure 39](#) shows the text of the Access Denied Message when the **radius-response** option is configured.

```
ProCurve(config)# show port-access web-based config
```

Port Access Web-based Configuration

```
DHCP Base Address      : 192.168.0.0
DHCP Subnet Mask       : 255.255.248.0
DHCP Lease Length      : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message  : Retrieved from Radius
```

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-auth Period	Unauth VLAN ID	Auth VLAN ID	Ctrl Dir
A1	Yes	1	No	300	60	1	2	both
A2	Yes	18	No	300	999999999	0	0	both
A3	Yes	22	No	300	999999999	4096	4096	both

Figure 39. Example of Access Denied Message when radius-response is Configured

Unauthenticated clients may be assigned to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients, the port is blocked and no network access is available.

Web Page Display of Access Denied Message

The web page in [Figure 40](#) is an example of the denied access message that appears when **unauth-vid** is configured.

Invalid Credentials

Your credentials were not accepted. You may have limited network access. Please wait while the configuration completes.

Estimated time remaining: 35 seconds

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

Figure 40. Example of Web Page with Configured Access Denied Message When unauth-vid is Configured

Figure 41 shows an example of a web page displaying the access denied message when an **auth-vid** is not configured.

Invalid Credentials

Your credentials were not accepted. Please wait **96** seconds to retry. You will be redirected automatically to the login page.

Unauthorized access to this network is prohibited. Access to this network requires prior authorization from the System Administrator. Please obtain the credentials prior to logging in.

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

Figure 41. Example of Web Page with Configured Access Denied Message When unauth-vid is not Configured

The **show running-config** command displays the client's information, including the configured access denied message.

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

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-14,19-24,A1-A4
    ip address dhcp-bootp
    no untagged 15-18
    exit
vlan 100
    name "auth-vid"
    untagged 15-18
    ip address dhcp-bootp
    exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message "Please contact your system
administrator to obtain authentication privileges."
no autorun
```

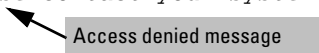


Figure 42. Example of Running Configuration Output Displaying Access Denied Message

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

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "ProCurve Switch 3500yl-24G"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-14,19-24,A1-A4
    ip address dhcp-bootp
    no untagged 15-18
    exit
vlan 100
    name "auth-vid"
    untagged 15-18
    ip address dhcp-bootp
    exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message radius-response
```

RADIUS response configured



Figure 43. Example of Running Configuration Output When RADIUS Response is Configured

Version W.14.40 Enhancements

Multicast ARP Support

- **Enhancement (PR_0000018427)**—Multicast ARP support enhancement.

To support IP multicasting, the multicast address range of 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF is reserved for Ethernet MAC addresses. The command **ip arp-mcast-replies** enables acceptance of the MAC addresses in the IP multicast range.

Syntax: [no] ip arp-mcast-replies

Enables or disables accepting multicast MAC addresses in the IP multicast address range in ARP requests and replies.

Default: Disabled.

```
ProCurve(config)# ip arp-mcast-replies
```

Figure 44. Example of Enabling the Acceptance of Multicast MACs in the IP Multicast Range

Version W.14.44 Enhancements

SNMP Traps

- **Enhancement (PR_0000045796)**—SNMP traps when MAC addresses are added to or deleted from a port.

When enabled, this feature allows the generation of SNMP traps for each MAC address table change. Notifications can be generated for each device that connects to a port and for devices that are connected through another device (daisy-chained).

Configuring SNMP Trap Generation

The **snmp-server enable traps mac-notify** command globally enables the generation of SNMP trap notifications.

Syntax: [no] snmp-server enable traps mac-notify [mac-move | trap-interval <0-120>]

Globally enables or disables generation of SNMP trap notifications.

trap-interval: *The time interval (in seconds) that trap notifications are sent. A value of zero disables the interval and traps are sent as events occur. If the switch is busy, notifications can be sent prior to the configured interval. Notifications may be dropped in extreme instances and a system warning is logged.*

The range is 0-120 seconds. Default: 30 seconds.

mac-move: *Configures the switch to capture data for MAC addresses that are moved from one port to another port. The **snmp-server enable traps mac-notify** command must have been enabled in order for this information to be sent as an SNMP notification.*

```
ProCurve(config)# snmp-server enable traps mac-notify trap-interval 60
```

Figure 45. Example of trap-interval Option

```
ProCurve(config)# snmp-server enable traps mac-notify mac-move
```

Figure 46. Example of mac-move Option

Additional mac-notify Options

Use the following command to configure SNMP traps for learned or removed MAC addresses on a per-port basis.

Note

The switch will capture learned or removed events on the selected ports, but will not send an SNMP trap unless mac-notify has been enabled with the **snmp-server enable traps mac-notify** command.

Syntax: [no] mac-notify traps <port-list> [learned | removed]

*When this command is executed without the **learned** or **removed** option, it enables or disables the capture of both learned and removed MAC address table changes for the selected ports in <port-list>.*

<port-list>: *Configures MAC address table changes capture on the specified ports. Use **all** to capture changes for all ports on the switch.*

learned: *Enables the capture of learned MAC address table changes on the selected ports.*

removed: *Enables the capture of removed MAC address table changes table on the selected ports.*

```
ProCurve(config)# mac-notify traps 5-6 learned
ProCurve(config)# show mac-notify traps 5-6

Mac Notify Trap Information

Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port    MAC Addresses trap learned/removed
-----
5       Learned
6       Learned
```

Figure 47. Example of Configuring Traps on a Per-Port Basis for Learned MAC Addresses

```
ProCurve(config)# mac-notify traps 3-4 removed
ProCurve(config)# show mac-notify traps
```

Mac Notify Trap Information

```
Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60
```

Port	MAC Addresses trap learned/removed
1	None
2	None
3	Removed
4	Removed

Figure 48. Example of Configuring Traps on a Per-Port Basis for Removed MAC Addresses

Interface Context Level Configuration

You can also execute the **mac-notify traps** command from the interface context.

```
ProCurve(config)# int 11
ProCurve(int-11)# mac-notify traps learned
```

Figure 49. Example of the Interface Context for mac-notify traps Command

Displaying the MAC Notify Traps Configuration Information

Use the **show mac-notify traps** command to display information about SNMP trap configuration.

Syntax: show mac-notify traps [port-list]

Displays SNMP trap information for all ports, or each port in the port-list.

```
ProCurve(config)# show mac-notify traps

Mac Notify Trap Information

Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port    MAC Addresses trap learned/removed
-----
1       None
2       None
3       Removed
4       Removed
5       Learned
6       Learned
```

Figure 50. Example of Information for SNMP Trap Configuration

The configured **mac-notify** commands display in the **show running-configuration** output.

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

Running configuration:

; J9087A Configuration Editor; Created on release #R.11.XX

hostname "ProCurve Switch"
snmp-server community "public" Unrestricted
snmp-server host 15.255.133.236 "public"
snmp-server host 15.255.133.222 "public"
snmp-server host 15.255.133.70 "public"
snmp-server host 15.255.134.235 "public"
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-28
  ip address dhcp-bootp
  exit
snmp-server enable traps mac-notify mac-move
snmp-server enable traps mac-notify trap-interval 60
snmp-server enable traps mac-notify
mac-notify traps 5-6 learned
mac-notify traps 3-4 removed
```

The mac-notify commands that were configured.

Figure 51. Example of Running Config File With mac-notify Parameters Configured

Version W.14.47 Enhancements

Entry-count Parameter Added to “show” Command

- **Enhancement (PR_0000040979)**— Entry-count parameter added to “show” command

The entry-count parameter is added to these two commands: **show access-list** and **show policy**. When either of those commands is used with the **entry-count** parameter, the switch displays the number of configured class, policy, and ACL entries.

Version W.14.49 Enhancements

Custom Default Configuration

- **Enhancement (PR_0000045685)**—Allows creation of a custom default configuration for the switch.

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:

- Use a customized configuration file as a default configuration file
- 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.

Note

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.

Creating the Custom Default Configuration File

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. An example is shown in [Figure 52](#).

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

ProCurve(config)# write memory
```

Figure 52. Example of Creating a Config File with the Desired Features

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 in [Figure 53](#).

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

Figure 53. Example of Copying the Startup Configuration File to the Custom Default Configuration File

Copying an Existing Configuration File to the Custom Default Configuration File

The switch can have up to 3 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.) To copy a configuration file that exists in flash memory to the custom default configuration file, use this command.

Syntax: copy config < source-filename > default-config

Copies the configuration file specified in <source-filename> to the custom default configuration file.

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

Figure 54. Copying the abc.cfg Config File to the Custom Default Config File

Copying the Custom Default Config File onto the Switch

Using TFTP.

To copy a configuration file stored on a TFTP server to the custom default configuration file, use the **copy tftp default-config** command.

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

Copies the stored configuration file on the TFTP server specified by <ip-addr> to the custom default configuration file.

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

Figure 55. Copying a Stored Config File to the Default Config File Using TFTP

Using XMODEM.

To copy a configuration file to the custom default configuration file using XMODEM, use the **copy xmodem default-config** command.

Syntax: copy xmodem default-config

Copies the configuration file specified by the XMODEM server device to the custom default configuration file.

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

Figure 56. Copying a Stored Config File to the Custom Default Config File Using XMODEM

Using USB.

To copy a configuration file to the custom default configuration file using USB, use the **copy usb default-config** command.

Syntax: copy usb default-config <stored config file name>

Copies the stored configuration file on the USB stick to the custom default configuration file.


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

Figure 57. Copying a Stored Config File to the Custom Default Config File Using USB

Copying the Custom Default Config File Off the Switch

Using TFTP.

To transfer a custom default configuration file off the switch using TFTP, enter the following command.

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

Copies the custom default configuration file to the stored_config.cfg file on the TFTP server.

Using XMODEM.

To transfer a custom default config file off the switch using XMODEM, enter the following command.

Syntax: copy default-config xmodem

Copies the custom default configuration file to the configuration file specified by the XMODEM server device.

Using USB.

To transfer a custom default configuration file off the switch using USB, enter the following command.

Syntax: copy default-config usb stored_config.cfg

Copies the custom default configuration file to the stored_config.cfg file on the USB device.

Using SFTP and SCP to Transfer the Custom Configuration

While the switch supports an SSH server with SCP and/or SFTP running on it, the switch is not an SCP or SFTP client. 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 that can be accessed by the switch.

Note

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 products now at: www.ProCurve.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>
```

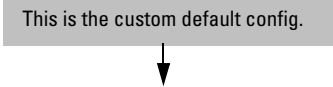


Figure 58. Example of Using SFTP

Erasing a Configuration File

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.

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

Figure 59. Example of Erasing the Startup Config File When a Default Custom Config File Exists

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.

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

Figure 60. Example of Erasing the Startup Config File When a Default Custom Config File Does Not Exist

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

```
ProCurve(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]?
```

Figure 61. Example of Erasing the Custom Default Config File

Displaying the Configuration Files

The **show config files** command displays the existing configuration files and indicates that a custom default configuration file exists.

```
ProCurve(config)# show config files

Configuration files:

id | act pri sec | name
---+-----+-----
1   *   *     | config
2                   | secondaryconfig
3                   | Kconfig

=====
A Custom default configuration file exists.
```

A custom default configuration file exists.

Figure 62. Example Output Displaying 3 Configuration Files

Enter the command **show default-config** to display the custom default configuration.

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

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.XX

hostname "ProCurve Switch"
module 1 type J86xxA
module 2 type J86xxA
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
```

These parameters were configured in the custom default configuration file.

Figure 63. Example of Output for Custom Default Configuration File

If a custom default configuration file exists and you erase the current active config file (using the **erase startup-config** command), then issue the **show running-config** command, the output will display the contents of the custom default configuration file. The custom default configuration file is loaded upon bootup. See [Figure 64](#).

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

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.XX

hostname "ProCurve Switch"
module 1 type J86xxA
module 2 type J86xxA
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 64. Example of Output of Custom Default Config File When Current Active Config File Erased

Troubleshooting Custom Default Configuration Files

- If the switch won't boot because of a problem with the custom default configuration file, the file can be removed using the ROM mode interface.
- The custom default configuration file cannot be erased using the front panel buttons on the switch. If the switch can be booted, use the **erase default-config** command to remove the custom default configuration file.

LLDP PoE+ Enhancements

- **Enhancement (PR_0000046912)**—Adds support for LLDP PoE+.

Overview

The data link layer classification (DLC) for PoE provides more exact control over the power requirement between a PSE and PD. The DLC works in conjunction with the physical layer classification (PLC) and is mandatory for any Type-2 PD that requires more than 12.95 watts of input power.

Note

DLC is defined as part of the IEEE 802.3at standard.

The power negotiation between a PSE and a PD can be implemented at the physical layer or at the data link layer. After the link is powered at the physical layer, the PSE can use LLDP to repeatedly query the PD to discover the power needs of the PD. Communication over the data link layer allows finer control of power allotment, which makes it possible for the PSE to supply dynamically the power levels needed by the PD. Using LLDP is optional for the PSE but mandatory for a Type 2 PD that requires more than 12.95 watts of power.

If the power needed by the PD is not available, that port is shut off.

PoE Allocation

There are two ways LLDP can negotiate power with a PD:

- Using LLDP MED TLVs: Disabled by default. Can be enabled using the **int <port-list> PoE-lldp-detect [enabled | disabled]** command, as shown below. LLDP MED TLVs sent by the PD are only used to negotiate power if the LLDP PoE+ TLV is disabled or inactive; if the LLDP PoE+ TLV is sent as well (not likely), the LLDP MED TLV is ignored.
- Using LLDP PoE+ TLVs: Enabled by default. The LLDP PoE+ TLV is always advertised unless it has been disabled. It is enabled using the **lldp config <port-list> dot3TlvEnable poeplus_config** command. See [“Enabling Advertisement of PoE+ TLVs” on page 74](#) for the command syntax.) It always takes precedence over the LLDP MED TLV.

Enabling **PoE-lldp-detect** allows the data link layer to be used for power negotiation. When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied is increased. PoE and LLDP interact to meet the current power demands.

Syntax: int <port-list> PoE-lldp-detect [enabled | disabled]

Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP.

Default: Disabled

For example, you can enter this command to enable LLDP detection:

```
ProCurve(config)# int 7 PoE-lldp-detect enabled
```

or in interface context:

```
ProCurve(eth-7)# PoE-lldp-detect enabled
```

Note

Detecting PoE information via LLDP only affects power delivery; it does not affect normal Ethernet connectivity.

You can view the settings by entering the **show power-over-ethernet brief** command:

```
HPswitch(config)# show power-over-ethernet brief
```

Status and Counters - Port Power Status								
PoE Port	Power Enable	LLDP Detect	Power Priority	Alloc By	PoE Val	Configured Type	Detection Status	Power Class
A1	Yes	enabled	low	usage	5	Phone-1	Delivering	0
A2	Yes	disabled	low	usage	17		Searching	1
A3	Yes	disabled	low	usage	17		Searching	0
A4	Yes	disabled	low	usage	17		Searching	2
A5	Yes	disabled	low	usage	17		Searching	0
A6	Yes	disabled	low	value	17	Phone-2	Searching	0
A7	Yes	enabled	low	value	5		Delivering	0
A8	Yes	disabled	low	value	17		Searching	0

Figure 65. Example of Port with LLDP Configuration Information Obtained from the Device

Enabling Advertisement of PoE+ TLVs

To initiate the advertisement of power with PoE+ TLVs, the following command is configured with the **poeplus_config** option.

Syntax: `lldp config <port-list> dot3TlvEnable poeplus_config`

Enables advertisement of data link layer power using PoE+ TLVs. The TLV is processed only after the physical layer and the data link layer are enabled. The TLV informs the PSE about the actual power required by the device.

Default: Enabled

Displaying PoE When Using LLDP Information

Displaying LLDP Port Configuration.

To display information about LLDP port configuration, use the **show lldp config** command.

Syntax: show lldp config <port-list>

Displays the LLDP port configuration information, including the TLVs advertised.

```
HPSwitch(config)# show lldp config 4

LLDP Port Configuration Detail

Port : 4
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
* poeplus_config

IpAddress Advertised:
```

Figure 66. Example of LLDP Port Configuration Information with PoE

Figure 67 shows an example of the local device power information using the **show lldp info local-device <port-list>** command.


```
HPswitch(config) show lldp info local-device A1
```

LLDP Local Port Information Detail

```
Port      : A1
PortType  : local
PortId    : 1
PortDesc  : A1
```

Poe Plus Information Detail

```
Poe Device Type      : Type2 PSE
Power Source         : Primary
Power Priority        : low
PD Requested Power Value : 20 Watts
PSE Actual Power Value : 20 Watts
```

Figure 67. Example of Local Device Power Information

Figure 68 shows an example of the remote device power information using the **show lldp info remote-device <port-list>** command.

```
HPswitch(config) show lldp info remote-device A3
```

LLDP Remote Device Information Detail

```
Local Port      : A3
ChassisType     : mac-address
ChassisId       : 00 16 35 ff 2d 40
PortType        : local
PortId          : 23
SysName         : ProCurve Switch 2510-24
System Descr    : ProCurve J9019A Switch 2510-24, revision
Q.10.XX, ROM Q.1...
PortDescr       : 23
```

```
System Capabilities Supported : bridge
System Capabilities Enabled   : bridge
```

```
Remote Management Address
Type      : ipv4
Address   : 10.0.102.198
```

Poe Plus Information Detail

```
Poe Device Type      : Type2 PD
Power Source         : Only PSE
Power Priority        : low
PD Requested Power Value : 20 Watts
PSE Actual Power Value : 20 Watts
```

Figure 68. Example of Remote Device Power Information

Enhancements

Version W.14.49 Enhancements

See the chapter “Power over Ethernet (PoE/PoE+) Operation” in the *Management and Configuration Guide* for your switch for more information about PoE.

Software Fixes

Software fixes are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each new software version includes all the software fixes added in all previous versions.

W.14.03 is the first software version for the HP ProCurve 2910al switches.

Version W.14.03

Status: Released and fully supported and posted on the Web.

Version W.14.04 through W.14.07

Status: Never released.

Version W.14.08 through W.14.10

Status: Never built.

Version W.14.11 through W.14.13

Status: Never released.

Version W.14.14

Status: Never built.

Version W.14.15

Status: Never released.

The following problems were resolved in software version W.14.15.

- **Enhancement (PR_0000010201)** — Support was added for SNMP client authentication. For more information, see [“SNMP Client Authentication” on page 10](#).
- **PoE (PR_0000016644)** — If the power supply fails, the switch may still indicate that it is delivering PoE power to the ports, when it is not.
- **Crash (PR_0000016665)** — If a transceiver is hot-swapped into the switch during switch initialization, the switch may reboot or restart a bank of ports.
- **sFlow (PR_0000016875)** — Packets sampled by sFlow are being forwarded twice by the switch.

- **Crash (PR_0000017018)** — The switch may reboot unexpectedly in response to an SNMP walk, depending on the specific switch configuration. The crash message may be similar to the following.

```
Software exception at ipamBttfSNetRoutes.c:339 -- in 'mIpAdmUpCt',  
task ID = 0x61d9e00
```

- **Crash (PR_0000017075)** — The switch may reboot unexpectedly after GVRP is disabled from a switch, displaying a message similar to the following.

```
Restricted Memory Exception number: 0xdead0100 HW Addr=0xe59ff094  
IP=0x10569748 Task='mGvrpCtrl'
```

- **Flow Control (PR_0000015824)** — Fiber ports do not notify the link partner of changes to the flow control configuration, resulting in a potential mismatch of flow control settings on each side of the link.

- **Rate-Limiting (PR_0000016255)** — The switch will not accept a Maximum Ingress Bandwidth value of zero.

- **Crash (PR_0000016124)** — The switch may reboot unexpectedly during a continuous SNMP MIB walk while SSH sessions are being created and ended.

- **Crash (PR_0000017015)** — When the switch is loading a configuration with the maximum number of IPv4 and IPv6 addresses and ACLs, the switch may reboot unexpectedly with an NMI event.

- **Crash (PR_0000017277)** — Configuration of a loopback address using a setmib may cause the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at ipamMGhsApi.c:522 - in 'eRouteCtrl', task ID  
= 0xa965dc0
```

- **IPv6 (PR_0000017078)** — A valid IPv4 loopback address is required, at a minimum, for IPv6 addresses to be configured. This fix notifies the user of this caveat during configuration.

- **IGMP (PR_0000009415)** — The switch may intermittently fail to forward a multicast stream.

- **Crash (PR_0000016652)** — Disabling routing from the CLI using the command **no ip routing** may trigger an unexpected reboot (NMI event) on a switch with a large config.

- **Port Communication (PR_0000004568)** — An Intel NIC using the 82566DM chipset may send out-of-spec packets to the switch which results in the loss of communication on that port, regardless of a continuous connection. Symptoms may include one or more of the following behaviors.

- Rx Bytes counter does not increment
- CRC/alignment errors

- Duplex mismatch
- Collisions, runts
- Giants
- Other physical layer errors

Although this fix improves or resolves the switch response to the problem traffic, the trigger for the switch symptoms is resolved through updated NIC firmware and drivers, when they are available from the device manufacturer.

- **Spanning Tree (PR_0000017820)** — Path costs are not appropriately updated after addition or removal of distributed trunks from the configuration.
- **QoS (PR_0000009724)** — QoS Priority settings are not present in routed packets.
- **Crash (PR_0000015746)** — A very busy switch with a large configuration may experience multiple module resets, displaying event log messages similar to the following.

```
Lost Communications detected - Heart Beat Lost(51)
Msg loss detected - no ack for seq # 15803
Msg loss detected - no ack for seq # 16654
Msg loss detected - no ack for seq # 17472
Msg loss detected - no ack for seq # 19015
Lost Communications detected - Source Message System(48)
Lost Communications detected - Source Message System(50)
Lost Communications detected - Source Message System(55)
```

- **Loop Protection (PR_0000037759)** — Loop-Protect may detect a loop and report that the port is shut down when it is not. This allows the loop-protect packets to flood the network and potentially starve spanning-tree and other protocols.

Version W.14.16

Status: Never released.

The following problems were resolved in software version W.14.16.

- **10-GbE (PR_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link.
- **Crash (PR_0000017435)** — Configuring a switch using the CLI command **include-credentials** may cause an unexpected reboot, if the switch has never had the feature previously enabled. The crash message may vary.

Version W.14.17 through W.14.25

Status: Never built.

Version W.14.26

Status: Released and fully supported and posted on the Web.

The following problems were resolved in software version W.14.26.

- **LLDP (PR_0000038230)** — The length of a CDP packet may prevent the switch from accepting the packet.
- **Proxy-ARP (PR_0000038934/0000038938)** — The switch may provide proxy-ARP replies to gratuitous-ARPs, which could be interpreted as a “duplicate IP address” by the original sending host.
- **Proxy-ARP (PR_0000038935)** — The switch may provide proxy-ARP replies to ARPs from a source IP address that is not within scope of the switch’s IP address/subnet mask.
- **DHCP-Snooping (PR_0000019155)** — DHCP-Snooping does not correctly identify fragmented packets, and drops UDP Fragments if a hex value of 44 (68 Decimal) is present in the payload where the header is usually located (in a non-fragment).

Version W.14.27

Status: Released and fully supported and posted on the Web.

The following problems were resolved in software version W.14.27.

- **Egress Memory Allocation (PR_0000039439)** — The egress priority queues were programmed with equal maximum sizes, rather than allowing the normal priority queue a larger size than the others, potentially impairing switch performance. A problem with enabling or disabling flow control on a port was also fixed.
- **ACL/QoS (PR_0000017975)** — When an ACL permit statement specifies a TCP or UDP port number or range, non-initial fragments of these TCP or UDP packets may not be acted upon in the same manner as the initial fragment, potentially causing some inappropriate drops.

Version W.14.28

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.28.

- **Crash (PR_0000038523)** — Hot-swapping transceivers too quickly may cause the switch to reboot unexpectedly with a software exception. Best practice tip: Each time a transceiver is inserted into the switch, allow it to fully initialize prior to removing it. The crash message may be similar to the following, though it may vary.

Software exception in ISR at svc_timers.c:472

- **Crash (PR_0000037527)** — The switch may reboot unexpectedly when loading an extensive configuration. The crash message may be similar to the following.

```
No msg buffer on at alloc_free.c:439 -- in 'mIpCtrl',
task ID = 0xa96bb80
```

- **CLI Wizard (PR_0000038179)** — The Management Interface Setup Wizard (invoked using the CLI command **setup mgmt-interfaces**) provides a generic error message of inconsistent value when an attempt is made to save a configuration with an invalid value.
- **SNMP (PR_0000038253)** — There are duplicate entries in the hpicfTC.mib for the 10-GbE SFP+ Direct Attach Cables.
- **10-GbE SFP+ DAC Transceiver (PR_0000038570)** — When a port that contains an SFP+ Direct Attach Cable is disabled, the switch stops sending traffic to the port but the transceiver on the other end of the cable is not aware of the link loss. This could be particularly problematic if the port is part of a static HP Trunk.
- **SNTP Authentication (PR_0000037553)** — The switch CLI does not allow configuration of the maximum key-value string of 32 characters for SNTP Authentication.
- **Crash (PR_0000038615)** — The switch may reboot unexpectedly with a message similar to the following.

```
Software exception at ipamSApi.c:66 -- in 'mIpAdMUpCt'
```

- **Flow Control (PR_0000038851)** — When flow control is disabled on one or more interfaces via the CLI, execution of the **show int brief** CLI command reveals that the change in flow control status does not take effect unless the switch is reloaded.
- **Crash (PR_0000039470)** — A very heavily utilized switch configured with jumbo frames, DHCP-snooping, QoS priority assignment, and Web-based authentication may reboot unexpectedly with a software exception. The crash message may vary.
- **Authentication (PR_0000011138)** — If the Radius server becomes unavailable, the **eap-radius authorized** option allows the switch to authenticate devices. If the response time of the RADIUS subsystem is greater than the server-timeout value on the switch or the device supplicant then switch will not be able to authenticate devices, and no warning of this failure will be displayed. This fix triggers the display of the following CLI message.

```
The RADIUS connection timeout must be less than the authentication
server timeout for the switch to authenticate automatically when the
RADIUS server is unavailable.
```

- **FFI (PR_0000039989)** — If an FFI event is triggered, and then the link is brought down and back up again, the same FFI event will be triggered again in about 20 seconds even if the trigger condition isn't met.

- **RADIUS Accounting (PR_0000012487)** — The switch doesn't send an accounting-stop when a switch **reload** closes the session.
- **CLI (PR_0000018670)** — Execution of the CLI command **show tech all** on a switch may trigger the switch to become unresponsive and require a power-cycle to recover.
- **CLI (PR_0000018594)** — Attempts to utilize the CLI interface configuration command **mdix-mode mdix** yields an error setting value mdix for port <port number>.
- **Authentication (PR_0000016211)** — If no RADIUS server is accessible during a re-authentication attempt, the clients will remain connected to an **auth-vid** even if an unauth-vid was defined.
- **10-GbE SFP+ DAC Transceiver (PR_0000039363)** — The “A” version of the J9281A HP ProCurve 10-GbE SFP+ 1m Cable, J9283A HP ProCurve 10-GbE SFP+ 3m Cable, and J9285A HP ProCurve 10-GbE SFP+ 7m Cable does not comply with the January 2009 version of the Multi-Source Agreement (MSA), SFF-8472 Rev 10.4. The result is interoperability problems that may prevent a link from becoming established. This fix adds support for the “B” version Direct Attach Cables (DACs): J9281B, J9283B, and J9285B. The “B” version DACs are compliant with MSA SFF-8472 Rev 10.4. Additionally, the “B” version DACs interoperate with the Intel NIC (Intel 10 Gigabit AF DA Dual Port Server Adapter).
- **Switch Hang (PR_0000014307)** — A switch with 802.1X configured may stop passing AAA requests and routed traffic. Over time this issue manifests itself in the form of lost TELNET and SSH access, and eventually even console access to its management is lost. Clients that attempt to authenticate will get a “domain not available” message. The switch must be reloaded to recover from this state.
- **Appletalk ARP (PR_0000015652)** — Appletalk ARP (AARP) packets are not traversing the Protocol VLAN, which makes file sharing and print services unavailable.
- **802.1X (PR_0000010850)** — If an **unauth-vid** is configured, and the client limit is reached on a switch port, a properly credentialed re-authentication following an improperly credentialed authentication attempt (for example, incorrect password) will leave the 802.1x client in the unauthorized VLAN instead of applying the appropriate authorized VLAN.
- **Web/FFI (PR_0000040095)** — The Web Management Interface Alert Log messages do not match the FFI event log messages.

Version W.14.29

Status: Released and fully supported and posted on the Web.
The following problems were resolved in software version W.14.29.

- **10-GbE (PR_0000041336)** — A switch with a 10-GbE transceiver installed may experience packet problems on any port due to egress packet memory misconfiguration.

- **Web Authentication (PR_0000041695)** — Web authentication for port-access does not function on software version W.14.29.
- **CLI (PR_0000038243)** — When task-monitor is enabled, the CLI output from the command **show cpu** is inconsistent with the cumulative sub-task averages, and higher than it should be. This behavior does not change after disabling task-monitor.

Version W.14.30

Status: Released and fully supported and posted on the Web.

The following problems were resolved in software version W.14.30.

- **Port Connectivity/Crash (PR_0000041622)** — If port 20 of the HP ProCurve 2910al-48 or 2910al-48-PoE+ switches is configured away from its auto default for speed-duplex or MDI/MDI-X, the switch will either reboot with a software exception message like the one below, or port 20 will go down and stay down.

```
Software exception at samba_chassis_slot_sm.c:2014 -- in 'eChassMgr',  
task ID = 0x1a4cbc40  
-> (B8): Co-Processor Crash detected - Available 0
```

- **Trunking (PR_0000041907)** — The Menu and Web Management Interfaces will allow a trunk to be given an invalid group name - “mesh”. A trunk named “mesh” will not be displayed properly in the startup or running configuration, despite the fact that the configuration is in place. Note that meshing is not supported in the 2910al series switches.
- **CLI (PR_0000042136)** — Output from various commands (or SNMP queries) of CPU utilization is not consistent. While the values reported by the CLI command **show cpu** is correct; **show sys** does not yield an accurate value. In addition, SNMP query of the CPU utilization, Menu navigation to CPU utilization, and Web Management Interface report of the CPU utilization is inaccurate.
- **Management (PR_0000016016)** — SSH and ping times to the switch are sluggish.
- **Crash (PR_0000016958)** — The switch may reboot unexpectedly when a second SSH session is established with the switch management while the switch is transferring a **show tech custom** file to a TFTP server. The crash message will be similar to the following.

```
Software exception at exception.c:501 -- in 'mSess3', task ID =  
0x8280a60 -> Memory system error at 0x60 - memPartFree
```
- **Crash (PR_0000041168)** — Running or copying the output from the CLI command **show tech** causes a memory leak that will eventually result in memory depletion and switch reboot. The crash messages vary widely, and may include PPC errors, NMI errors, and “Out of resources: no token found” errors.

- **Crash (PR_0000041586)** — Entry or upload of multi-line CLI config commands may cause the switch to reboot unexpectedly with a message similar to the following.

```
PPC Data Storage (Bus Error) exception 0x300: esf=0x082e6058  
addr=0x942201fc ip=0x001c7910 Task='mSess1' tid=0x82e6b20
```

- **10-GbE (PR_0000043292)** — Some J8438A HP ProCurve 10-GbE X2-SC ER Optics (a subset of those with serial number containing the letters DM in the middle) do not turn on the laser after the switch reboots.

- **CLI (PR_0000018556)** — The switch fails to copy a customized show tech file onto the switch, causing an error, No SHOW-TECH file found, when the **show tech custom** command is issued at the CLI.

- **Config (PR_0000041803)** — The config lines for **aaa authentication** and **aaa accounting** appear in the wrong order in the running-config; these configuration parameters are dependent upon the **radius-server** and **aaa server-group**, and therefore need to follow those settings in the configuration.

- **SNMP (PR_0000014902)** — SNMP traps contain the wrong instance number for the event Description (the eventDescription is one instance number too low).

- **Event Log (PR_0000038339)** — The switch records an event log message when a specific user's ACL/ACE cannot be added, but does not give any indication if all the switch ACE resources have been consumed

Original log message: 00700 idm: Unable to add ACL entry, ace index
3, client mac <MAC address>, port <number>

New log message: 00055 ACL: unable to apply ACL <client MAC address>,
failed to add entry 23, max ACE limit reached

- **10-GbE (PR_0000040368)** — Support is added for a future transceiver.
- **CLI (PR_0000015982)** — Using the port-security feature, attempts to enter more than the configured MAC address limit on a port result in an ambiguous error message: Inconsistent value. This fix triggers a more appropriate error message: Warning: Number of configured addresses on port <port number> exceeds address-limit.
- **Config (PR_0000018749)** — If MSTP instance port settings (port priority or path cost) are configured prior to link aggregation, once a trunk group is configured, the MSTP instance configuration lines reference the individual ports (errant behavior) and not the trunk group (expected behavior). As a consequence, the switch will not be able to reload the configuration because the MSTP instance port settings are invalid.
- **MAC Authentication (PR_0000015520)** — Traffic from unauthenticated clients may be allowed during the process of authenticating clients under heavy loads.

- **SSH (PR_0000040877)** — When an exit from a switch management SSH session is initiated from an SSH client, the termination values from the switch are incorrect, triggering the following erroneous message to be displayed at client, “SSH connection is closed by remote host”.
- **Crash (PR_0000002449/0000002511)** — The switch may reboot unexpectedly with a software exception when MSTP is configured.
- **Crash (PR_0000039155)** — A group of ports may reboot and report a crash message similar to the following when IPv6 ACLs or policies are applied at either the CLI or through IDM.

```
Software exception at aqTcamSlaveHwBttfClone.c:1332 -- in 'mAsicUpd',  
task ID = 0x61e7140
```

- **CLI (PR_0000016116)** — When the **include** parameter is used with a **show** command, and the switch finds a matching regular expression, the console output contains all-zeros byte.
- **Routing (PR_0000040696)** — CPU-generated packets may have the wrong next-hop MAC address; they are sent out of the appropriate IP interface and VLAN but this may cause SNTP, ping, and other host applications to fail.
- **Crash (PR_0000038937)** — Configuring an IPV6 address followed by a routed ACL with a UDP port range applied to a VLAN may cause the modules to reset.

Version W.14.31

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.31.

- **CLI (PR_0000044241)** — The switch does not recognize the valid CLI command **show module**; when the command is executed, the switch returns an error: `invalid input`.
- **10-GbE (PR_0000041859)** — Output from the switch CLI command **show vlan 1** may indicate that the 10-GbE SFP+ ports are up, even when they are not connected.
- **Web Management (PR_0000041910)** — The status of 10-GbE SFP+ ports is not displayed in the switch Web Management interface (Configuration tab -> Device View).
- **Enhancement (PR_0000018513)** — Banner enhancements were made. For more information, see [“Banner Enhancements” on page 27](#).
- **Enhancement (PR_0000040721)** — Extended ping and traceroute are now available.
- **Enhancement (PR_0000042579)** — Error messages returned from ping were updated to include a relevant VLAN reference.

Software Fixes

Version W.14.32 through W.14.34

- **Enhancement (PR_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation. For more information, see [“TELNET Negotiate About Window Size \(NAWS\) Initiation Enhancement” on page 28](#).

Version W.14.32 through W.14.34

Status: Never built.

Version W.14.35

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.35.

- **Enhancement (PR_0000044737)** — Support is added for the following new product.
J9443A - HP ProCurve 630 Redundant / External Power Supply
- **Crash (PR_0000041509)** — A group of ports (1-24 or 25-48) on the switch may reset unexpectedly when a module containing a mirror port is removed.
- **LED (PR-0000043752)** — When PoE controller failure occurs in the switch, the Chassis Fault LED, Self-Test Status LED, and PoE Mode LED on the switch do not blink amber to indicate a fault. The LEDs for the affected ports do blink amber as they should, however, and the self-test failure is accurately reported in the switch event log.

Version W.14.36

Status: Never released.

The following problems were resolved in software version W.14.36.

- **IP Communication (PR_0000044004)** — Switches running software versions W.14.31-W.14.35 may experience a self-limiting resource leak in ICMP.
- **DHCP Snooping (PR_0000040580)** — Configuration of trust status for DHCP-snooping on ports participating in a dynamic trunk yields undesirable results when the ports of the trunk are removed. This configuration should not be allowed on dynamic trunks (e.g. **dhcp-snooping trust Dyn1**) and this fix enforces that limitation at the CLI with an error message.
- **ACLs (PR_0000045003)** — Updated IPv6 rules for IDM ACLs.
- **GVRP (PR_0000040238)** — After a dynamically-learned VLAN is converted to a static port-based VLAN, and an interface is made a static member of that VLAN, disabling GVRP causes the port to lose the VLAN membership. The running-config, startup-config and the SNMP egress static member list for the VLAN show the port as member of the VLAN. All other data shows the port is no longer a member of the VLAN. VLAN communication over the affected

interface is no longer possible until one of the two following workarounds is executed.
Workarounds: Either re-issue the tag and untag commands for VLAN port assignment or reload the system.

- **QoS (PR_0000042343)** — QoS on Ports may not behave correctly when trunks are involved, e.g., if QoS is configured on a port that is a member of a trunk, the CLI command **no qos** does not disable the feature as it should.
- **ACL/QoS (PR_0000045616)** — ACL/QOS Error return definitions as measured by the hardware layer are out-of-synch with SNMP values.
- **RADIUS Accounting (PR_0000042522)** — The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.
- **Management (PR_0000016049)** — If a console or telnet session to the switch is used to execute a CLI command (e.g. execution of the **show tech** command) and then the management session is abandoned before the task is completed (e.g. the window is closed), that session becomes unresponsive. If, at that point, another management session is established and the CLI command **kill** is executed to end the initial, now unresponsive session, the new management session will become unresponsive as well, until all sessions are in use and unresponsive.
- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see [“Accounting Services” on page 29](#).
- **UDLD (PR_0000043071)** — UDLD transmits a burst of packets when any port on the switch goes down (1 packet is sent for each port that goes down), falsely triggering a failure state.
- **Command Authorization (PR_0000043525)** — HP-Command-String authorization does not work as expected.
- **PoE (PR_0000045766)** — There are intermittent issues in the support of some pre-standard PoE phones; sometimes phones will boot and sometimes they don't. Grouping four or more phones together in consecutive ports may trigger this issue more often.
- **GVRP (PR_0000012224)** — Changing the GVRP **unknown-vlan** state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **GVRP (PR_0000040758)** — Switches do not use multiple GVRP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs).

Version W.14.37

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.37.

- **Crash (PR_0000046506)** — Execution of the CLI command **console local-terminal none** may cause the switch to reboot unexpectedly, logging a message similar to the following. Note that this problem was found and fixed on a special debug version of software; symptoms in released software, if any, may vary.

```
Software exception at parser.c:2373 -- in 'mSess1', task ID =  
0xa931000 -> ASSERT: failed
```

Version W.14.38

Status: Released and fully supported and posted on the Web.
The following problems were resolved in software version W.14.38.

- **Terminal Display (PR_0000008239)** — When a switch telnet session is opened from a Unix/Linux terminal, the line wrap of the terminal is not preserved after logout.
- **TFTP (PR_0000040441)** — When an attempt is made to download a configuration file from the TFTP server, there is an invalid error being logged if the config file does not exist on the TFTP server: tftp: RCVD error:0, msg:.. Changes have been implemented so that the error message accurately indicates the cause of the file transfer failure.
- **Banner MOTD (PR_0000042871)** — The message returned by the CLI in response to the banner MOTD configuration command erroneously states that a banner of up to 3071 characters is supported; the actual maximum number of characters is 3070.
- **RADIUS (PR_0000046154)** — When RADIUS Server Groups are configured, MAC Based RADIUS Sessions go unauthenticated even if cached reauth is enabled.
- **CLI Help (PR_0000046320)** — AAA command in-line help lists the "cached-reauth" option even after it has already been typed into that command. For example:

```
ProCurveSwitch(config)# aaa authentication port-access chap-radius  
server-group pat cached-reauth ?  
  
none          Do not use backup authentication methods.  
authorized    Allow access without authentication.  
cached-reauth Grant access in case of reauthentication retaining  
               the current session attributes.  
  
<cr>
```

The “cached-reauth” option should not be displayed, since it has already been typed in the command line.

- **Crash (PR_0000044298)** — When RADIUS accounting is enabled, entering a command with too many characters entered at the CLI will crash the switch and record an error similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x00000000 IP=0x00002680 Task='mftTask' Task ID=0xa941c80
fp: 0x30442030 sp:0x042333b
```

- **Enhancement (PR_0000038652/0000045335)** — Unauthenticated VLAN Access (Guest VLAN Access). For more information, see [“Unauthenticated VLAN Access \(Guest VLAN Access\) Enhancement” on page 47](#).

Version W.14.39

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.39.

- **802.1X (PR_0000037816)** — 802.1X does not allow for authentication of new clients when the client-limit is reached; unauthenticated clients contribute to the client-limit. This fix gives authenticated users precedence over unauthenticated users. In addition, the relevant **'show'** commands are updated to display clients in the unauthenticated state so the administrators will have the ability to see unintended users on a port.
- **802.1X (PR_0000044041)** — When a large number of 802.1X supplicants log off a single port simultaneously, the switch may reboot unexpectedly, logging a crash message similar to the following.

```
Software exception at aaa8021x_util.c:2265 -- in 'm8021xCtrl', task
ID = 0x84c1a10
```
- **802.1X (PR_0000047025)** — After the switch reboots and before IP communication is initialized, the switch accepts authentication requests from 802.1X clients. Because the switch cannot communicate with the RADIUS server yet, it sends EAP-Failure notifications to the client, which causes client authentication to fail.
- **Authentication (PR_0000017371)** — Unknown 802.1X, Web-, and MAC-Authentication clients take too long to connect, causing very slow DHCP addressing.
- **Authentication (PR_0000045833)** — Some EAP requests are not properly handled by the switch.
- **Authentication (PR_0000046171)** — When a client is authenticated on a port with one authentication method, if the client is moved to a different port with a different authentication method, the switch correctly lists the client as being authenticated on the second port, but does not remove the client from the first port.

- **BPDU Protection (PR_0000047748)** — This fix corrects the output of an SNMP query. Before the fix, the switch might incorrectly respond that BPDU protection is disabled on a port, when in fact it is enabled and functioning properly.
- **CLI (PR_0000008145)** — Counters for the following commands do not increment correctly when a TCP port is blocked by a NAS filter in a RADIUS-assigned ACL.

```
show port-access authenticator clients <PORT-LIST> detailed
show port-access mac-based clients <PORT-LIST> detailed
show port-access web-based clients <PORT-LIST> detailed
```
- **CLI (PR_0000012407)** — Output from the CLI command **show port-access authenticator <port number> client details** shows the Frames In and Frames Out for each client to be exactly the same and it does not increment as it should. Workaround: Output from the CLI command **show port-access authenticator <port> session-counters** shows the Frames In and Frames Out incrementing correctly.
- **CLI (PR_0000040869)** — A QoS policy that is applied to a switch interface cannot be removed with the CLI.
- **CLI (PR_0000043334)** — When the CLI config command **aaa port-access authenticator** is issued for a port that is part of a trunk, the error message is generic and does not let the user know the problem. This fix introduces a more specific error message.
- **CLI (PR_0000047545)** — The CLI command **no telnet-server** is not saved in the config file.
- **CLI (PR_0000049955)** — The output of **show tech route** does not include all the information it is intended to provide.
- **CLI Help (PR_0000048102)** — The debug help text (when the user types **debug ?**) offers some invalid parameters.
- **Config (PR_0000037570)** — After using the CLI to assign a port in a VLAN number higher than 32, the configuration cannot be saved via the Menu interface.
- **Config (PR_0000040782)** — When an HP ProCurve 1000Base-T Mini-GBIC (J8177C) is configured with the speed-duplex auto-100 setting, that configuration is lost from both running and startup configurations after a switch reload.
- **Config (PR_0000043984)** — The switch allows an inherent configuration conflict; the **rate-limit** and **service-policy** parameters should not be allowed concurrently on an interface.
- **Console (PR_0000001136)** — Rarely, the switch console may hang after a software image transfer to the switch. Workaround: **<Ctrl-C>** will restore the command prompt.
- **CoS (PR_0000046599)** — The switch reports incorrect Class Of Service (CoS) information in the output of the command **show port-access auth <port>** when the default CoS (value 255) is in effect.

- **Counters (PR_0000048657)** — When a switch port is supplying more than 9.9 Watts of power to a port, the **show power brief** output truncates the displayed value. For example, the switch displays 10... instead of 10.3 W.
- **Crash (PR_0000017707)**— The configuration of Web Authentication and connection of a PC into a switch port followed by an attempt to browse the Web will trigger a switch to reboot unexpectedly with a software exception.
- **Crash (PR_0000041445)**— When Web Authentication is in use, the switch may experience conditions that cause it to reboot unexpectedly with a crash message similar to the following.

```
Software exception at buffers.c:2231 -- in 'tHttpd', task ID =
0x80d25b0
```

- **Crash (PR_0000043167)**—When using TFTP with “octet” mode to upload the switch's configuration file, the switch may reboot unexpectedly with a message similar to the following.
- **Crash (PR_0000043188)**— Rarely, downloading a config file from a TFTP server to the switch may cause the switch to reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at hwBp.c:156 -- in 'tDcacheUpd', task ID =
0xa9835c0
```

- **Crash (PR_0000043538)**— When multiple 802.1X users try to authenticate simultaneously, the module or port bank may reset unexpectedly with messages similar to the following.

```
chassis: Slot B: Msg loss detected - no ack for seq #
```

```
chassis: Slot B: Lost Communications detected - Source Message
System(50)
```

```
chassis: Slot B Slave ROM Tombstone: 0x13000601
```

```
Software exception at interrupts_bts.c:294 -- in 'tMsgCount', task
ID = 0x4489bb1c
```

- **Crash (PR_0000043740)** — When switch ports are configured for both 802.1X authenticator and MAC-authentication, with different authenticated VLAN IDs for each, the switch may reboot unexpectedly with a software exception as they try to authenticate a client using both methods simultaneously. One of the following messages may be recorded by the switch crash log.

```
Software exception at portsecMaster_util.c:1088 -- in m8021xCtrl'
```

```
Software exception at portsecMaster_util.c:1093 -- in m8021xCtrl'
```

- **Crash (PR_0000043765)** — Switches performing port-access authentication may experience an unexpected reboot with a crash message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at radius_request.c:1472 -- in 'mRadius006', task  
ID = 0x8320
```

- **Crash (PR_0000043802)**— When GVRP is configured and the switch is learning GVRP VLANs through a trunk, if GVRP is disabled on the neighboring switch, or if the neighbor switch is reloaded, the switch will reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at vls_dyn_reconfig.c:2487 -- in 'mGarpCtrl',  
task ID = 0x83b9670
```

- **Crash (PR_0000044219)**— When the switch is configured for web-auth with client moves enabled using the CLI command **aaa port-access web-based <port-list> client-moves**, if a client is authenticated on one port and moves to another port (also configured for web-auth), the switch may reboot unexpectedly with a crash message similar to the following. Note that this problem was found and fixed on an internal software development build; symptoms in released software may vary.

```
Software exception at wma_client_sm.c:387 -- in 'mWebAuth', task ID  
= 0x8379a70
```

- **Crash (PR_0000044225)** — When multiple MAC-authentication clients attempt to log in to the switch with a RADIUS-assigned VLAN unknown to the switch, the switch may reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at radius_util.c:463 -- in 'mRadius006', task ID  
= 0x8306d60
```

- **Crash (PR_0000046643)** — With DHCP Snooping enabled on a VLAN, if a client requests a DHCP address and receives it from a trusted port, these changes can cause the switch to reboot unexpectedly:

- 1.The client port is disabled.
- 2.The trusted port configuration is changed to be untrusted.
- 3.The client port is re-enabled and the client requests a DHCP address, but the response comes from the now-untrusted port.

The switch logs a message similar to the following.

```
Software exception at pmgr_util.c:1283 -- in 'mIpPktRecv', task ID
= 0xa972cc0
```

- **Debug (PR_0000046165)**— With DHCP snooping enabled, debug messages display IP addresses in reverse order.
- **DHCP (PR_0000044256)**— The switch does not properly forward the DHCP response to clients.
- **DHCP Snooping (PR_0000046276)** — With DHCP snooping enabled, a MAC-Authenticat-ion client whose session times out cannot reauthenticate.
- **DHCP Snooping (PR_0000046831)** —The switch forwards DHCP Discovery packets out untrusted ports.
- **DHCP Snooping (PR_0000048426)** — With DHCP Snooping enabled, a client DHCP request is forwarded out untrusted ports.
- **Enhancement (PR_0000016657)** — Access Control Debug Logging changes have been made. For more information, see [“Access Control Debug Logging” on page 48](#).
- **Enhancement (PR_0000042147, PR_0000042840)**— Port-Based Debug Logging Enhancement. This enhancement provides debug logging with the ability to filter debug messages related to a specific set of configured ports. When the port filter is enabled for a debug type, only the messages that inherently refer to a specific port will be filtered. All other messages for that debug type will still be sent to debug logging. The CLI command for this enhancement is below.

```
Switch# debug <security> <port-access | port-security | user-
profile-mib> <optional detailed debug type> include port [PORT-LIST]
```

The following is used to remove all ports:

```
Switch# [no] debug <security> <port-access | port-security |
user-profile-mib> <optional detailed debug type> include port
```

- **Enhancement (PR_0000045680)**— Management Access Security enhancements. For more information, see [“Management Access Security Enhancements” on page 51](#).
- **Enhancement (PR_0000045711)** — Web authentication message enhancement. For more information, see [“Web Authentication Message Enhancement” on page 54](#).
- **Event Log (PR_0000043041)**— When the switch downgrades a port from Gigabit to 10/100 operation, the resulting event log "FFT" message is displayed twice.
- **IGMP (PR_0000018494)**—IGMP joins may cause multicast streams to flood, briefly, across the VLAN.

- **IP Communication (PR_0000042790)** — A very busy switch may cease all IP communication when the CLI command **show tech route** is executed. Messages similar to the following may be seen in the event log when this occurs.

```
W <date> <time> 00436 NETINET: 1 route entry creation(s) failed.  
W <date> <time> 00075 system: Out of pkt buffers; miss count: 0
```

- **IP Communication (PR_0000043121)** — Execution and subsequent interruption of the CLI command **show tech route** during a vulnerability scan negatively affects IP communication.
- **IP Connectivity (PR_0000046280)**— After updating software, the hostname is removed from the configuration and the switch does not respond to SSH requests.
- **IPv6 (PR_0000042273)** — The switch responds to LLDP requests with the first IPv6 address defined internally, which may be the link-local address. With this fix, the switch will advertise an IPv6 address that can communicate to remote sites.
- **IPv6 (PR_0000045773)** —IPv6 duplicate address detection (DAD) does not work properly in some topologies.
- **Mini-GBIC (PR_0000044130)**— The HP ProCurve Gigabit-SX-LC Mini-GBIC (J4858C) does not transmit after a switch reboot or hot-swap when it is used in a dual-personality port.
- **PoE (PR_0000043773)**— The "MPS absent" counter does not increment when a PoE-powered device (PD) is removed from a switch port.
- **Port Access (PR_0000017541)**— The switch allows an inherent configuration conflict; port-based 802.1X should not be allowed concurrently with Web and MAC authentication.
- **Port Access (PR_0000043432)** — CLI output from the command **show port-access authenticator** does not update the authenticated client list for local authentication clients.
- **Port Authentication (PR_0000042402)**— Configuration of 802.1X after MAC-Authentication will override the MAC-Auth logoff-period value. A previous fix (PR_0000010737) allowed the network administrator to see that all logoff timers on a port (802.1X, MacAuth, WebAuth) are functionally identical; i.e. writing a value to one will automatically write them all. This fix allows different timers to be used for different authentication methods.
- **Port Communication (PR_0000043048)** — The switch will not allow a port to link if the MDIX-MODE is set to **MDI** or **MDIX** (only the **auto-MDIX** setting will allow link).
- **Port Connectivity (PR_0000038601)** — The time between a port coming up and that port being online and passing traffic varies, and at times, may be extended to over a minute.
- **QoS (PR_0000039751)** — Strict outbound queuing is being enforced on trunk ports; when traffic is egressing (sent out of) a trunk port on multiple queues, the higher priority queues will starve out lower priority queues when oversubscribed.

- **RADIUS (PR_0000043940)** — With the Single Source IP Identity feature enabled, the “Radius-NAS-IP Attribute” sent by the switch is using the outgoing interface as the source address instead of the address defined in the **ip source-interface** configuration.
- **RADIUS Accounting (PR_0000043555)**— When the switch is configured for RADIUS accounting of commands (**aaa accounting commands stop-only radius**), and a user has logged on to the switch via telnet, the switch sends the incorrect calling-station-id AVP in the radius-accounting-request packet. The calling-station-id AVP is supposed to list the IP address of the host from which the user has connected to the switch.
- **sFlow (PR_0000015656)**—Outbound sampling using sFlow is not functioning.
- **SNMP (PR_0000045869)**— When a large number of SNMPSET commands (on the order of 100 commands) are sent to the switch, at some point the switch runs out of room to store those entries. When the switch's memory limit is reached it gives this error message:

```
snmp: event 1997; events file too big; record not written.
```

This fix increases the available memory to allow the switch to accept up to 380 SNMPSET commands.
- **SNMP (PR_0000046735)**— Event log messages of type “Info” are sent as traps even after applying the configuration command **snmp-server host <IPaddress> <community> not-info**.
- **SNTP (PR_0000048717)**— The switch does not ensure the VLAN is up before sending SNTP requests, which can result in SNTP timeouts.
- **SNTP Authentication (PR_0000048588)**— With SNTP authentication disabled, the switch sends extra, unnecessary authentication information in the SNTP request packet.
- **SSH (PR_0000045158)** — SSH login to the switch might fail.
- **SSH (PR_0000046259)** — The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB).
- **SSH (PR_0000046860)**— After a client public key is copied to the switch via TFTP, if the user uses SSH to connect to the switch, when the SSH session is closed the switch reboots unexpectedly with a software exception message.
- **STP (PR_0000017189)**— When the switch is running in RSTP-mode (through the use of the CLI configuration command **spanning-tree force-version rstp-operation**) and MSTI settings are still present in the switch, a TCN is triggered when the MSTI settings are modified or removed.
- **TFTP (PR_0000046063)**— When the management VLAN is changed from the default (VLAN 1), the switch does not respond to TFTP requests.

- **TFTP (PR_0000046863)**— The switch experiences a loss of free memory each time a software image is downloaded via TFTP.
- **Transceivers (PR_0000045482)** — Some J9152A SFP+ LRM transceivers do not turn on the laser after the switch reboots. Workaround: remove, then re-insert the transceiver.
- **UDLD (PR_0000047414)**— When UDLD is enabled, communication with the switch might be inconsistent, affecting the switch response to ping, telnet, 802.1X requests, SNMP requests, and SNMP packets.
- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

Best Practice Tip: 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if the first packet sent was not 802.1X, Web- or MAC-auth could be initiated before 802.1X places the user in the unauthenticated VLAN and when Web- or MAC-auth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

If a MAC- or Web-based configuration on a port is associated with an unauth-VID, and an attempt is made to configure an unauth-VID for 802.1X (**port-access authenticator**), the switch with this fix will reject the configuration change with a message similar to one of the following.

Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):

```
Configuration change denied for port <number>. Only Web or MAC
authenticator can have unauthenticated VLAN enabled if 802.1X
authenticator is enabled on the same port. Please disable Web and
MAC authentication on this port using the following commands:
```

```
no aaa port-access web-based <PORT-LIST> or
no aaa port-access mac-based <PORT-LIST>
```

Then you can enable 802.1X authentication with unauthenticated VLAN. You can re-enable Web and/or MAC authentication after you remove the unauthenticated VLAN from 802.1X. Note that you can set unauthenticated VLAN for Web or MAC authentication instead.

Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):

Configuration change denied for port <number>. Only Web or MAC authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please remove the unauthenticated VLAN from 802.1X authentication on this port using the following command:

no aaa port-access authenticator <PORT-LIST> unauth-vid

Note that you can set unauthenticated VLAN for Web or MAC authentication instead.

Message 3:

Configuration change denied for port <number>. Only Web or MAC authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please use unauthenticated VLAN for Web or MAC authentication instead.

Event log message when the configuration is changed:

mgr: Disabled unauthenticated VLAN on port <number> for the 802.1X. Unauthenticated VLAN cannot be simultaneously enabled on both 802.1X and Web or MAC authentication.

- **VRRP (PR_0000049259)** —In some situations the VRRP Virtual IP does not respond to ping.
- **Web Authentication (PR_0000016178)**— When a client connecting to the switch through Web Authentication enters the wrong credentials, the switch places the client in the unauth-vid and does not prompt for authentication retry. Once the port is in the unauthenticated state, only a reload of the switch allows for reauthentication.
- **Web Authentication (PR_0000017374)** — Following successful Web Authentication by a client, the browser redirect (to either the configured redirect URL or the client's home page) does not work.
- **Web Authentication (PR_0000017431)**— During Web Authentication login, the login progress pages are cached and the user is subjected to these cached pages when trying to navigate to other sites after successful authentication.
- **Web Authentication (PR_0000018047)**— A Web Authentication request may return a blank page.

- **Web Authentication (PR_0000018869)** — After redirection to the login page, and successful login using Web Authentication, the initial URL cannot be reached.
- **Web Authentication (PR_0000037786)** — Login progress pages provided during Web Authentication give the end-users an “Access Granted” page prior to completion of the network transition. Better dialogue with clearer instructions to end-users is implemented with this fix.
- **Web Authentication (PR_0000042390)** — The Web Authentication login page is no longer functional after there has been a configuration change in the DHCP range the switch uses for Web-auth.
- **Web Authentication (PR_0000043209)** — Following successful Web Authentication, the browser redirect does not work correctly; it omits the hostname from the redirect URL.
- **Web Authentication (PR_0000048491)** — The Web Authentication login page is not presented to Web Authentication clients.

Version W.14.40

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.40.

- **BootROM (PR_0000039743)** — When software containing a boot ROM update is copied to the primary flash of the switch and the switch is reloaded into the primary image, the boot ROM does not successfully update. Workaround: Copy software with boot ROM update to secondary, and execute the CLI command **boot system flash secondary** to load the secondary image.
- **Config (PR_0000046578)** — An IP BOOTP gateway configured on subnet zero is not displayed in the startup or running configuration file. The gateway is used correctly by the switch; this is a configuration display issue only.
- **Crash (PR_0000051910)** — SSH login to the switch might fail, and the switch may reboot unexpectedly with a message similar to the following.

```
NMI event SW:IP=0x00f64f88 MSR:0x02029200 LR:0x00f654dc
cr:0x20000000
sp:0x05337598 xer:0x00000000 Task='tTelnetOut2' Task ID=0xa903000
```
- **Crash Messaging (PR_0000049806)** — A coredump file is not generated when the switch crashes.
- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement. For more information, see [“Multicast ARP Support” on page 60](#).

- **File Transfer (PR_0000048178)** — While loading switch software via Secure Copy (SCP) or TFTP, the switch can be rebooted by the user before the software file load completes.
- **LLDP (PR_0000048124)** — The LLDP Port VLAN ID TLV is incorrectly advertised as 0 for Trunked ports.
- **SNMP (PR_0000046906)**—Responses to SNMP queries on a switch configured with trunk groups are slow, which can lead to SNMP polling failures.
- **TACACS (PR_0000047886)** — When a TACACS server is not available, the switch waits 40 seconds or more before the TACACS request is timed out and the configured secondary authentication method is tried. By default, the timeout should take 5 seconds.
- **Unauthenticated VLAN (PR_0000045072)**— An unauthenticated VLAN cannot be configured for 802.1X authentication, when another authentication method is also in use on a port. This fix also adds the **unauth-period** parameter for MAC authentication.

Version W.14.41

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.41.

- **Authentication (PR_0000043924)**— The switch responds with invalid PEAP packets when the RADIUS server request includes optional EAP TLVs, resulting in authentication failure.
- **CLI (PR_0000044704)** — The switch does not properly adjust terminal size display, if the user telnets to the switch and then changes the terminal size. This can cause the username to display when the password is requested, instead of a blank field.
- **Counters (PR_0000048734)**—After clearing counters on all ports with the command **clear statistics global**, if the counters on a single port are subsequently cleared, counters on other ports revert to their pre-cleared values.
- **Flow Control (PR_0000052789)** —When flow control is enabled on the switch, execution of the **show int brief** CLI command reveals that flow control is not actually enabled on gigabit or dual-personality ports.
- **LLDP-MED (PR_0000018681)** — LLDP-MED responses from a device connected to the switch are stored in the wrong order, which causes errors when the user uses “snmpwalk” to see the stored values on the switch.
- **LLDP-MED (PR_0000050798)** — In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.
- **UDLD (PR_0000050402)**— With UDLD enabled, a trunk that uses fiberoptic transceivers stops forwarding traffic after a switch reboot.

Version W.14.42

Status: Never released.

Version W.14.43

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.43.

- **Authentication (PR_0000054344)** — The request sent from switch to RADIUS server truncates the username to 16 characters, which causes authentication failure if the username is longer than 16 characters.
- **Authentication (PR_0000054384)** — In some situations an unauthenticated client can access the authenticated VLAN.
- **Management (PR_0000054089)** — Initiating a management session to the switch causes the switch's available memory to decrease.
- **SSH (PR_0000051551)** — If an SSH session is closed during a large file transfer, the session cannot be re-opened.
- **SSH (PR_0000052970)** — The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB). This improves the original fix in W.14.39 (PR_0000046259).
- **Stacking (PR_0000053271)** — The CLI command **no stack** does not disable stacking.

Version W.14.44

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.44.

- **802.1X (PR_0000038874)** — When using 802.1X in client mode, the command **aaa port-access authenticator 1 client-limit 2** should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.
- **CLI (PR_0000051739)** — The “alias” command configuration is removed from the config file upon reboot. Also, the output of **show alias** does not include the name of the alias.
- **Crash (PR_0000047202)** — If a large configuration or switch software file is downloaded to the switch when the DHCP lease timer expires, the transfer will fail and the switch might reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

```
Software exception at svc_timers.c:820 -- in 'mDHCP Clint', task ID  
= 0x5d79880
```

- **Crash (PR_0000048592)** — With meshing enabled, if the switch receives a packet destined to a MAC address with certain parameters the switch might reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

```
Software exception at btthHwUtil.c:798 -- in 'eDrvPoll', task ID =  
0x61fe800
```

- **Crash (PR_0000049154)** — In software versions W.14.39 - W.14.43, some situations related to IGMP-learned MAC addresses combined with a MAC address learned on an interface module can cause the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at btthSlaveLearn.c:1691 -- in 'mAdMUpCtrl'
```

- **Crash (PR_0000049919)** — A rare situation related to source port filtering can cause the switch to reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

```
Software exception at btthDma.c:410 -- in 'tDevPollTx', task ID =  
0xa9a1780
```

- **Crash (PR_0000050090)** — In some situations, attempting to delete a non-existent VLAN from the switch configuration might cause the switch to reboot unexpectedly with a message similar to the following. This problem was found and fixed on a special debug version of software. Symptoms in released software may vary.

```
Software exception at vls_util.c:1380 -- in 'mMTM', task ID =  
0xa967200
```

- **DHCP Snooping (PR_0000049563)** — The switch forwards DHCP packets when DHCP Snooping is configured globally but not on any VLANs.
- **DIPLD (PR_0000051983)** — A switch running Dynamic IP Lockdown (DIPLD) and DHCP Snooping has these two issues. If a port is part of multiple DHCP snooping-enabled VLANs and IP Lockdown is enabled on that port, removing that port from one VLAN disables IP Lockdown on all VLANs. Also, if a port is part of multiple DHCP snooping-enabled VLANs and IP Lockdown is enabled on that port, removing DHCP snooping on one VLAN disables IP Lockdown on all VLANs. This fix resolves both issues.
- **Enhancement (PR_0000045796)** — The ability to enable SNMP traps when MAC addresses are added to or deleted from a port. For more information, see [“SNTP Client Authentication” on page 10](#).

- **IGMP (PR_0000052737)** — With Forced Fast-Leave disabled (which is the default), upon receipt of a “leave” message from a client, the switch sends a Group Specific Query with a Max Response Time of zero seconds, which is not a valid value.
- **SNMP (PR_0000045943)** — When using SNMP to initiate a TFTP “get” of a file from the switch, if the requested file does not exist, the switch responds with a vague error message. This fix implements meaningful error messages in that situation.
- **SNMP (PR_0000050956)**— SNMP traps contain hexadecimal characters instead of valid event log messages.
- **TELNET (PR_0000047906)** — A telnet session to the switch is not dropped when the IP address to which the telnet session connected is removed from the interface.
- **TFTP (PR_0000049655)** — After enabling Secure Copy (SCP) which automatically disables TFTP, the switch continues to send information via TFTP.

Version W.14.45

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version W.14.45.

- **Banner MOTD (PR_0000054833)** — The switch experiences a loss of free memory when a login banner is configured.
- **CLI (PR_0000050756)** — When the user presses <Ctrl>c to cancel the output of a previously-issued command, in some cases the <Ctrl>c does not appear to have any effect, and the switch displays the remaining output of the previous command.
- **CLI (PR_0000052748)** — The switch does not allow a VLAN number higher than 4 to be configured as the primary VLAN.
- **File Transfer (PR_0000039190)** —A configuration file that has a QoS policy applied to a VLAN (**vlan <vlan-id> service-policy <policy-name> in**) cannot be downloaded to the switch.
- **IP Communication (PR_0000053603)**— The switch responds to an ARP request received on one VLAN but sent from a different VLAN. This situation can occur when a client's port is moved from one VLAN to another, and the client sends an ARP request from an IP address on the original VLAN.
- **IP Communication (PR_0000053861)**— The switch is unable to telnet or ping to super-netted IP addresses, and supernetted IP addresses cannot be configured on the switch.

Version W.14.46

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.46.

- **Crash (PR_0000052464)** — A switch that has a large number of ACLs applied by the Identity Driven Manager (IDM) application might reboot unexpectedly with a message similar to the following.


```
Software exception at enDecode.c:54 -- in 'midmCtrl', task ID =
0xa946380
-> out of memory!
```
- **DHCP (PR_0000054749)**— When the switch acts as a DHCP relay agent, it erroneously removes the “end” option (code 255) from DHCP packets.
- **DIPLD (PR_0000052518)** — With Dynamic IP Lockdown enabled, there is no communication between clients on the switch.
- **sFlow (PR_0000012123)**— The switch does not allow sFlow to be configured on a mirror port.
- **sFlow (PR_0000041583)**—The switch does not send VLAN tag information in sFlow data.
- **SNMP/Config (PR_0000039221)**— The switch can misinterpret the community name as if it were a trap level, in the **snmp-server host** command. This fix modifies the command with keywords **community** and **trap-level**. The new command syntax is as follows.


```
snmp-server host <ip addr> [community <community string>] [trap-level <none | all | not-info |
critical | debug>] [informs].
```

Version W.14.47

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.47.

- **CLI (PR_0000046858)**— The switch does not use the specified **startup-default** configuration file when the user types **reload**. If the user issues the **reload at** or **reload after** command, the specified **startup-default** file is correctly used. This fix also adds a warning message when the user issues the **startup-default** command.
- **CLI (PR_0000047495)** — With the same trap receiver configured for multiple SNMP community names, if the user attempts to delete that trap receiver from any of the SNMP community names with the CLI command **no snmp-server host <ip-address> <community-name>**, the trap receiver that is deleted is always the trap receiver for the first configured SNMP community.

- **CLI (PR_0000048578)**— The **<Ctrl-c>** break sequence does not work while the user is creating a custom login banner.
- **CLI (PR_0000050554)** — The **debug acl** command is not available.
- **Console (PR_0000042791)**— The output of **show interfaces** can be slightly different from switch to switch, depending on each switch's configuration. For example, for large values the counters might include commas in one case and not display commas in another case.
- **Counters (PR_0000048732)**— The output of **show interfaces <port> hc** does not display the counters in hexadecimal as it should.
- **Counters (PR_0000048733)**— The output of **show interfaces** has commas for large values in some, but not all fields. This fix makes the display consistent.
- **Crash (PR_0000038431)**— When the Web Management Interface is used for port security configuration of 44 or more ports concurrently (Security > Port Security > Select 44 ports > click on 'Set Security Policy for the Selected Ports') the switch will reboot unexpectedly with a message similar to the following.

```
PPC Bus Error exception vector 0x300:  
Stack-frame=0x033ace80 HW Addr=0x37392c38 IP=0x0047ade0  
Task='tHttpd' Task ID=0x33ad408 fp: 0x0000001c sp:0x033acf40 lr:0x
```

- **Crash (PR_0000041777)** — If a configuration file with the entry **power-over-ethernet redundancy n+1** is downloaded to the switch, the switch will reboot unexpectedly with a message similar to the following.

```
PPC Data Storage (Bus Error) exception 0x300: esf=0x083a5570  
addr=0xc3d2e1f0 ip=0x00113424 Task='mftTask' tid=0x83a69d0  
fp=0x69696969 sp=0x083a5630 lr=0x001136
```

- **Crash (PR_0000056315)**—From the Web interface of a commander switch, if the user removes a stack member and then tries the close-up view, the switch might reboot unexpectedly with a message similar to the following.

```
Invalid Instruction Exception number: 0x00000004  
HW Addr=0x434f535c IP=0x434f535c Task='InetServer' Task ID=0xa6e2b80  
fp: 0x434f535f sp:0x03129058 lr:0x00f224
```

- **Enhancement (PR_0000040979)**— The **entry-count** parameter is added to these two commands: **show access-list** and **show policy**. When either of those commands is used with the **entry-count** parameter, the switch displays the number of configured class, policy, and ACL entries.
- **Event Log (PR_0000049520)** — For some event log entries, the VLAN ID (VID) is not properly displayed if the VID has more than one digit.

- **Event Log (PR_0000050999)** — If the CLI command is issued to download software to the switch, and during that download an SNMP request to download software is sent to the switch, the resulting error message is garbled.
- **Mirroring (PR_0000015825)**— Remote mirroring and certain source/destination IP address combinations do function properly; the remote destination switch does not copy the traffic to the mirror (exit) port.
- **MSTP (PR_0000045597)** —If the user configures the path cost for a port in an MSTP instance, and then configures a priority for that same port in that MSTP instance, the switch changes the path cost back to the default value (auto). Workaround: configure the priority first, then configure the path cost. This issue is seen with MSTP instances only; configuring path cost and priority for ports in the CIST works properly.
- **Routing (PR_0000052349)**— When a destination host does not respond, the switch sends the wrong ICMP message (“network unreachable” instead of “host unreachable”).
- **sFlow (PR_0000039269)** — When sFlow is enabled on a trunk port and one of the trunk ports is disabled, the switch does not consistently send port counter data to the sFlow server.
- **sFlow (PR_0000049710)** — During times of high traffic, the dropped samples counter displayed by **show sflow <port> sampling-polling** is not updated.
- **TACACS (PR_0000052495)** — If the switch is configured to use TACACS for telnet access and the TACACS timeout is configured for a value greater than 75 seconds, the switch waits much longer than 75 seconds before timing out the TACACS request.
- **Trunking (PR_0000050635)** — When 7-meter Direct Attach Cables (J9285B) are configured as a trunk between switches, if one of the switches is rebooted, the trunk ports might begin to toggle offline/online repeatedly.
- **Unauthenticated VLAN (PR_0000051515)** — Using SNMP, the switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. As with PR_0000010533, *this fix will alter existing configurations*. Please see the PR_0000010533 writeup (in W.14.39) for complete details.
- **Web Authentication (PR_0000042284)**— When an EWA server is used for Web authentication, authentication is successful but custom graphics are not displayed.
- **Web Management (PR_0000044397)**— Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access. Also, if both the commander and member are configured for SSL-only access, connection to the stack member fails.

Version W.14.48

Status: Released and fully supported, but not posted on the Web.

The following problems were resolved in software version W.14.48.

- **Banner MOTD (PR_0000053198)** — When using TACACS for telnet authentication, if a banner MOTD is longer than four lines, the first four lines of the banner are not visible on the screen.
- **Crash (PR_0000050103)** — The switch allows setMIB commands to create invalid configurations, which might cause the switch to reboot unexpectedly when the user issues the **show running-config** command, with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
Software exception at cli_xlate.c:5340 -- in 'mSess1', task ID = >
0xa924e00
```

- **Crash (PR_0000054005)** — If an SFP+ transceiver or cable is present in the switch and the menu interface is used to make port or trunk configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x3131393e IP=0x00002670 Task='mSess1' Task ID=0xa930640
fp: 0x05216200 sp:0x038ac7f0
```

- **File Transfer (PR_0000054790)** — Switch software cannot be updated via HTTPS.
- **LEDs (PR_0000048829)** — Although the event log reports an Unrecoverable fault on PoE controller, the switch LEDs do not indicate any problem.
- **PoE (PR_0000055223)** — In some cases the PoE controller fails self-test, after software attempts to update the controller firmware.
- **QoS (PR_0000054917)** — On a switch configured to use DSCP (command **qos type-of-service diff-services**), if one of the default DSCP policies is disabled and a lower-precedence QoS policy is applied (for example VLAN QoS), that new QoS policy is not used until the switch is rebooted. Workaround: disable DSCP on the switch so that the default policies are not used (command **no qos type-of-service diff-services**), or reboot the switch.

Version W.14.49

Status: Released and fully supported and posted on the Web.

The following problems were resolved in software version W.14.49.

- **Config (PR_0000054554)**—The command **copy config <config1 | config2 | config3> config CONFIG** either fails, or creates a CONFIG file with invalid parameters.
- **Config (PR_0000054730)** —For a switch with two configuration files that contain SSH keys, when the inactive config file is deleted by the user, in some cases the SSH keys are erroneously removed from the active config file.
- **Config (PR_0000057944)**—After a software update the TACACS and RADIUS keys are deleted from the configuration file.
- **Crash (PR_0000047343)**—If Spanning Tree Protocol is enabled when 256 VLANs are already configured on the switch, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at buffers.c:3323 -- in 'mGvrpCtrl', task ID = 0x5dace40
```

- **Crash (PR_0000056868)**—In some cases with DHCP snooping enabled globally and on a VLAN, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception at alloc_free.c:646 -- in 'tDevPollTx', task ID = 0xa9a1300  
-> buf already freed by 0x0A96BC00, op=0x00000000
```

- **DHCP Snooping (PR_0000056774)**—When DHCP snooping is enabled, valid PXE boot packets that have yiaddr = 0.0.0.0 are dropped by the switch.
- **Enhancement (PR_0000045685)**—Allows creation of a custom default configuration for the switch. For more information, see [“Custom Default Configuration” on page 65](#).
- **Enhancement (PR_0000046912)**—Adds support for LLDP PoE+. For more information, see [“LLDP PoE+ Enhancements” on page 72](#).
- **File Transfer (PR_0000057021)**—A remote client is unable to copy the switch's config file via SCP or SFTP.
- **File Transfer (PR_0000057616)**—In rare situations the switch might not correctly download a config file, reporting `invalid input errors`.
- **SNMP (PR_0000050869)**—An SNMP query for `hpChassisTemperature` always returns a value of 4 (indicating good), even when the output of **show system temperature** indicates the switch is overheated.



© 2010 Hewlett-Packard Development
Company, LP. The information contained
herein is subject to change without notice.

July 2010
Publication Number
5900-0244