

## Release Notes: Version W.14.38 Software

*for the HP ProCurve Series 2910al Switches*

---

These release notes include information on the following:

- W.14.38 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 in releases W.14.03 through W.14.38 ([page 9](#))
- A listing of software enhancements in recent releases ([page 11](#))
- A listing of software fixes included in releases W.14.03 through W.14.38 ([page 50](#))

© Copyright 2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

## Publication Number

5900-0244  
December 2009

## 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.procurve.com](http://www.procurve.com)

# Contents

<b>Software Management</b>	<b>1</b>
Software Updates	1
Download Switch Documentation and Software from the Web	1
View or Download the Software Manual Set	1
Downloading Software to the Switch	1
Downloading Software to the Switch	2
TFTP Download from a Server	3
Xmodem Download From a PC or Unix Workstation	3
Saving Configurations While Using the CLI	5
ProCurve Switch, Routing Switch, and Router Software Keys	6
Minimum Software Versions for Series 2910al Switch Features	7
OS/Web/Java Compatibility Table	8
<b>Clarifications</b>	<b>9</b>
Virtual Stacking/Management VLANs	9
<b>Known Issues</b>	<b>9</b>
Release W.14.30	9
Release W.14.03	9
<b>Enhancements</b>	<b>11</b>
Release W.14.03 Enhancements	11
Release W.14.04 through W.14.07 Enhancements	11
Release W.14.08 through W.14.10 Enhancements	11
Release W.14.11 through W.14.13 Enhancements	11
Release W.14.14 Enhancements	11
Release W.14.15 Enhancements	11
SNTP-Client Authentication	11
Release W.14.16 Enhancements	19
Release W.14.17 through W.14.25 Enhancements	19
Release W.14.26 Enhancements	19

Release W.14.27 Enhancements .....	19
Release W.14.28 Enhancements .....	20
Release W.14.29 Enhancements .....	28
Release W.14.30 Enhancements .....	28
Release W.14.31 Enhancements .....	28
Release W.14.32 through W.14.34 Enhancements .....	30
Release W.14.35 Enhancements .....	30
Release W.14.36 Enhancements .....	30
Release W.14.37 Enhancements .....	47
Release W.14.38 Enhancements .....	48
<b>Software Fixes .....</b>	<b>50</b>
Release W.14.03 .....	50
Release W.14.04 through W.14.07 .....	50
Release W.14.08 through W.14.10 .....	50
Release W.14.11 through W.14.13 .....	50
Release W.14.14 .....	50
Release W.14.15 .....	50
Release W.14.16 .....	52
Release W.14.17 through W.14.25 .....	52
Release W.14.26 .....	53
Release W.14.27 .....	53
Release W.14.28 .....	53
Release W.14.29 .....	55
Release W.14.30 .....	56
Release W.14.31 .....	58
Release W.14.32 through W.14.34 .....	58
Release W.14.35 .....	59
Release W.14.36 .....	59
Release W.14.37 .....	60
Release W.14.38 .....	61

# Software Management

---

---

## Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various ProCurve switches you may have in your network.

---

## Download Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from the ProCurve Networking Web site as described below.

### View or Download the Software Manual Set

Go to: [www.procurve.com/manuals](http://www.procurve.com/manuals)

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

You can also register on the My ProCurve portal to receive a set of ProCurve switch manuals on CD-ROM. To register and request a CD, go to [www.procurve.com](http://www.procurve.com) and click on **My ProCurve Sign In**. After registering and entering the portal, click on **My Manuals**.

### Downloading Software to the Switch

ProCurve Networking periodically provides switch software updates through the ProCurve Networking Web site ([www.procurve.com](http://www.procurve.com)). After you acquire the new software file, you can use one of the following methods for downloading it to 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 3).
- 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.

---

This section describes how to use the 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.

---

## Downloading Software to the Switch

ProCurve Networking periodically provides switch software updates through the ProCurve Networking Web site ([www.procurve.com](http://www.procurve.com)). After you acquire the new software file, you can use one of the following methods for downloading it to the switch:

- For a TFTP transfer from a server, do either of the following:
  - Click on **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:
  - Click on **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 3).
- 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.

---

This section describes how to use the 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.

## TFTP Download from a Server

**Syntax:** `copy tftp flash <ip-address> <remote-os-file> [ < primary / secondary > ]`

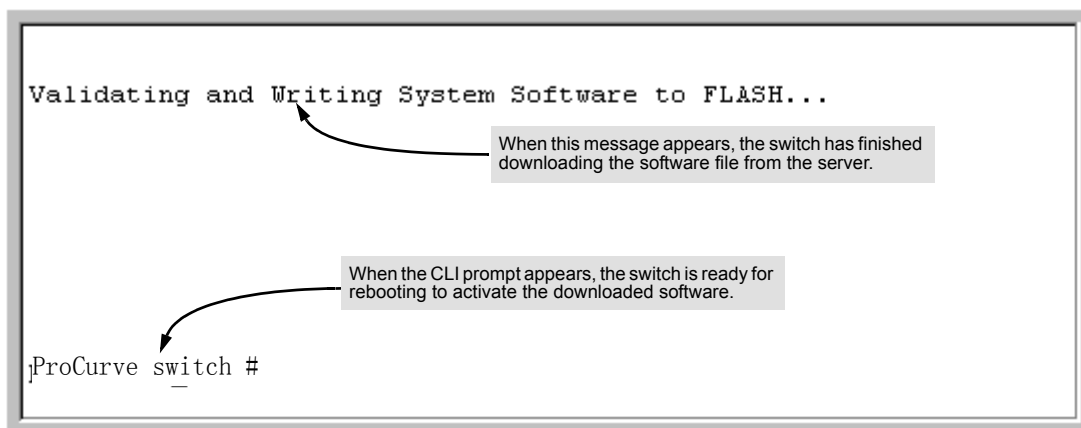
Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named W\_14\_03x.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 shown in [Figure 1](#). When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:



**Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software**

3. Reboot the switch.

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.

## 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 dropdown 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. Reboot the switch.

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
<b>C</b>	1600M, 2400M, 2424M, 4000M, and 8000M
<b>CY</b>	Switch 8100fl Series (8108fl and 8116fl)
<b>E</b>	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
<b>F</b>	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
<b>G</b>	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
<b>H</b>	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
<b>I</b>	Switch 2800 Series (2824 and 2848)
<b>J</b>	<b>J.xx.xx.biz</b> Secure Router 7000dl Series (7102dl and 7203dl)  <b>J.xx.xx.swi</b> Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
<b>K</b>	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).
<b>L</b>	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
<b>M</b>	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.
<b>N</b>	Switch 2810 Series (2810-24G and 2810-48G)
<b>PA/PB</b>	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
<b>Q</b>	Switch 2510 Series (2510-24)
<b>R</b>	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
<b>T</b>	Switch 2900 Series (2900-24G and 2900-48G)
<b>U</b>	Switch 2510-48
<b>W</b>	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
<b>VA/VB</b>	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
<b>WA</b>	ProCurve Access Point 530
<b>WS</b>	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module

Software Letter	ProCurve Networking Products
<b>WT</b>	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
<b>Y</b>	Switch 2510G Series (2510G-24 and 2510G-48)
<b>Z</b>	ProCurve 6120G/XG and 6120XG Blade Switches
<b>numeric</b>	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 ProCurve Networking Web site at [www.procurve.com](http://www.procurve.com).
2. Click on **Software updates**.
3. Click on **Minimum Software Version Required by Feature**.

### 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

## OS/Web/Java Compatibility Table

The switch Web agent supports the following combinations of OS browsers and Java Virtual Machines:

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: <ul style="list-style-type: none"><li>– Version 1.3.1.12</li><li>– Version 1.4.2.05</li></ul>
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, SP2 and 7.0	Sun Java 2 Runtime Environment: <ul style="list-style-type: none"><li>– Version 1.5.0_11, Version 1.6.0</li></ul>
Windows Server SE 2003 SP2		
Windows Vista		

# 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

---

### Release W.14.30

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

- **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.

### Release W.14.03

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

- **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

---

Enhancements are listed in chronological order, oldest to newest software release.

---

## Release W.14.03 Enhancements

*No new enhancements; Initial release.*

## Release W.14.04 through W.14.07 Enhancements

*No new enhancements, software never released.*

## Release W.14.08 through W.14.10 Enhancements

*No new enhancements, software never built.*

## Release W.14.11 through W.14.13 Enhancements

*No new enhancements, software never released.*

## Release W.14.14 Enhancements

*No new enhancements, software never built.*

## Release W.14.15 Enhancements

Release W.14.15 includes the following enhancements.

- **Enhancement (PR\_0000010201)** — Support was added for SNTP client authentication.

### 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](#).

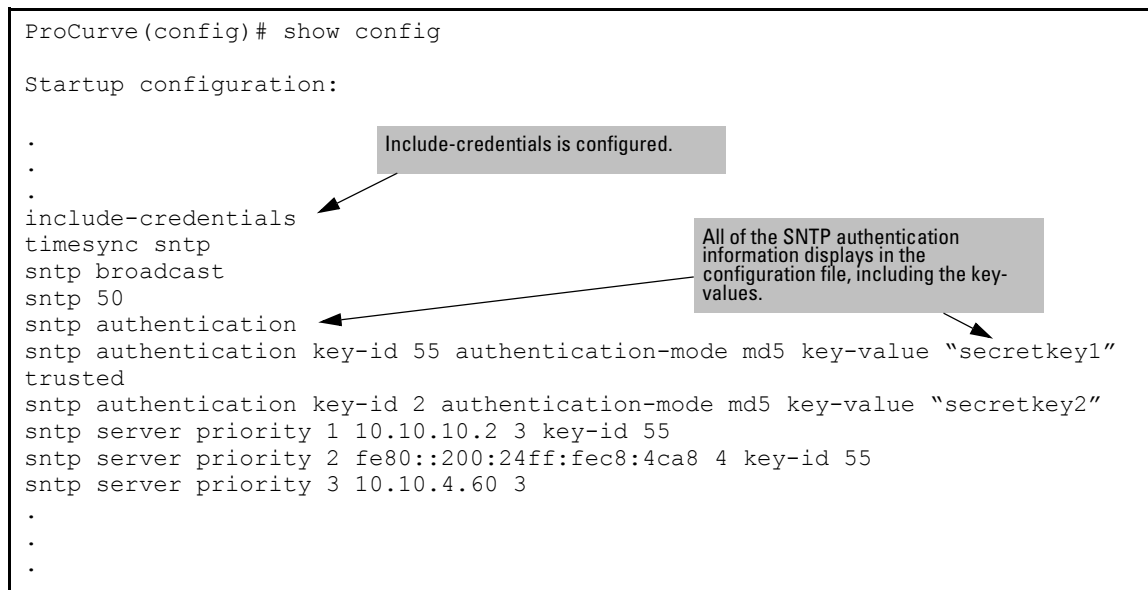
```
ProCurve(config)#copy tftp startup-config 10.2.3.44 config1
.
.
.
Switch reboots...

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.



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

## Release W.14.16 Enhancements

*No new enhancements, software not a public release.*

## Release W.14.17 through W.14.25 Enhancements

*No new enhancements, software never built.*

## Release W.14.26 Enhancements

*No new enhancements, software fixes only.*

## Release W.14.27 Enhancements

*No new enhancements, software fixes only.*

## Release W.14.28 Enhancements

Release 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>

*vlan-id*                Specifies a valid VLAN ID number to bind with the specified MAC and IP addresses on the port in the DHCP binding database.

*ip-address*           Specifies a valid client IP address to bind with a VLAN and MAC address on the port in the DHCP binding database.

*mac-address* Specifies a valid client MAC address to bind with a VLAN and IP address on the port in the DHCP binding database.

*port-number* Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.

---

## 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**

- **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

## Release W.14.29 Enhancements

*No new enhancements, software fixes only.*

## Release W.14.30 Enhancements

*No new enhancements, software fixes only.*

## Release W.14.31 Enhancements

Release W.14.31 includes the following enhancements. (Not a public release.)

- **Enhancement (PR\_0000018513)** — Banner enhancements were made.

### Banner Enhancements

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.

- **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.
- **Enhancement (PR\_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation.

### **TELNET Negotiate About Window Size (NAWS) Initiation Enhancement**

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.

## Release W.14.32 through W.14.34 Enhancements

*No new enhancements, software never built.*

## Release W.14.35 Enhancements

Release W.14.35 includes the following enhancements. (Not a public release.)

- **Enhancement (PR\_0000044737)** — Support is added for the following new product.

J9443A - HP ProCurve 630 Redundant / External Power Supply

## Release W.14.36 Enhancements

Release W.14.36 includes the following enhancement. (Not a public release.)

- **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-Output-Packets | • Service-Type       |
| • Acct-Status-Type     | • Acct-Input-Octets   | • NAS-IP-Address     |
| • Acct-Terminate-Cause | • Nas-Port            | • NAS-Identifier     |
| • Acct-Authentic       | • Acct-Output-Octets  | • Calling-Station-Id |
| • Acct-Delay-Time      | • Acct-Session-Time   |                      |
| • Acct-Input-Packets   | • User-Name           |                      |

- **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:

- |                        |                     |                      |
|------------------------|---------------------|----------------------|
| • Acct-Session-Id      | • Acct-Delay-Time   | • NAS-IP-Address     |
| • Acct-Status-Type     | • Acct-Session-Time | • NAS-Identifier     |
| • Acct-Terminate-Cause | • User-Name         | • Calling-Station-Id |
| • Acct-Authentic       | • Service-Type      |                      |

- **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 47.](#))
- 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 30.](#))

- 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 preceeding 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 <b>show ip</b> , which results in this accounting entry. Notice the session ID (003300000009) assigned to this accounting entry incrementally follows the preceeding 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 <b>logout</b> command. The session ID (00330000000A) assigned to this accounting entry incrementally follows the preceeding 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".	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
User "fred" then executes <b>show ip</b> , 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.	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
User "fred" executes the <b>logout</b> 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.	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
Terminate Exec Accounting Session "00330000000B"	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

**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 >	36
[acct-port < port-number >]	36
[key < key-string >]	36
[no] aaa accounting < exec   network   system > < start-stop   stop-only > radius	40
[no] aaa accounting commands < stop-only   interim-update > radius	
aaa accounting session-id < unique   common >	
[no] aaa accounting update	41
periodic < 1 - 525600 > (in minutes)	
[no] aaa accounting suppress null-username	41
show accounting	46
show accounting sessions	47
show radius accounting	46

---

### 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 32.)
    - **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 30)
      - network (page 30)
      - system (page 31)
      - commands (page 31)
    - **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 :
```

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.

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

**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.*

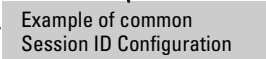
*For more on these options, refer to [“Acct-Session-ID Options in a Management Session” on page 31](#).*

```
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 38).

---

**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 38.*

**start-stop:** *Applies to exec, network, and system accounting service types. Refer to “Accounting Controls” on page 39.*

**stop-only:** *Applies to all accounting service types. Refer to “Accounting Controls” on page 39.*

**interim-update:** *Applies to the commands accounting service type. Refer to “Accounting Controls” on page 39*

**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 <b>reload</b> 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
```

Update Period

Suppress Unknown User

**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 35.](#))*

```
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 35.](#))*

```
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**

## Release W.14.37 Enhancements

*No new enhancements, software fixes only. (Not a public release.)*

## Release W.14.38 Enhancements

Release W.14.38 includes the following enhancement.

- **Enhancement (PR\_0000038652)** - Unauthenticated VLAN Access (Guest VLAN Access).

### **Unauthenticated VLAN Access (Guest VLAN Access) Enhancement**

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**

# Software Fixes

---

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

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

## Release W.14.03

*No software fixes; no new enhancements (Initial release).*

## Release W.14.04 through W.14.07

Versions W.14.08 through W.14.10 were never released.

## Release W.14.08 through W.14.10

Versions W.14.08 through W.14.10 were never built.

## Release W.14.11 through W.14.13

Versions W.14.11 through W.14.13 were never released.

## Release W.14.14

Version W.14.14 was never built.

## Release W.14.15

The following problems were resolved in release W.14.15. (Never released.)

- **Enhancement (PR\_0000010201)** — Support was added for SNMP client authentication. For more information, see [“Release W.14.15 Enhancements” on page 11](#).
- **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.

## Release W.14.16

The following problems were resolved in release W.14.16. (Not a public release.)

- **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.

## Release W.14.17 through W.14.25

Versions W.14.17 through W.14.25 were never built.



## Release W.14.26

The following problems were resolved in release 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).

## Release W.14.27

The following problems were resolved in release 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.

## Release W.14.28

The following problems were resolved in release 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 **cap-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.

## Release W.14.29

The following problems were resolved in release 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.14.28.

- **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.

## Release W.14.30

The following problems were resolved in release 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.
- **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.

## Release W.14.31

The following problems were resolved in release W.14.31. (Not a public release.)

- **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 28](#).
- **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.
- **Enhancement (PR\_0000038122)** — TELNET Negotiate About Window Size (NAWS) Initiation. For more information, see [“TELNET Negotiate About Window Size \(NAWS\) Initiation Enhancement” on page 29](#).

## Release W.14.32 through W.14.34

Versions W.14.32 through W.14.34 were never built.

## Release W.14.35

The following problems were resolved in release W.14.35. (Not a public release.)

- **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.

## Release W.14.36

The following problems were resolved in release W.14.36. (Never released.)

- **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 30](#).
- **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).

## Release W.14.37

The following problems were resolved in release W.14.37. (Not a public release.)

- **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
```



## Release W.14.38

The following problems were resolved in release 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 48](#).



© 2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

December 2009  
Manual Part Number  
5900-0244