



## Release Notes: Version K.14.33 Software *for the HP ProCurve Series 6600 Switches*

---

These release notes include information on the following:

- K.14.33 is supported on the following switches:
    - HP ProCurve 3500-24 Switch (J9470A)
    - HP ProCurve 3500-24-PoE Switch (J9471A)
    - HP ProCurve 3500-48 Switch (J9472A)
    - HP ProCurve 3500-48-PoE Switch (J9473A)
    - HP ProCurve Switch 6600-24G (J9263A)
    - HP ProCurve Switch 6600-24G-4XG (J9264A)
    - HP ProCurve Switch 6600-24XG (J9265A)
    - HP ProCurve Switch 6600-48G (J9451A)
    - HP ProCurve Switch 6600-48G-4XG (J9452A)
  - Download switch software and documentation from the Web ([page 1](#))
  - Support Notes and Known Issues in releases K.14.03 through K.14.33 ([page 13](#))
  - A listing of software enhancements in recent releases K.14.03 through K.14.33 ([page 15](#))
  - A listing of software fixes included in releases K.14.03 through K.14.33 ([page 59](#))
-

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

## Publication Number

5992-6005  
June 2009

## Applicable Products

HP ProCurve 3500-24 Switch	(J9470A)
HP ProCurve 3500-24-PoE Switch	(J9471A)
HP ProCurve 3500-48 Switch	(J9472A)
HP ProCurve 3500-48-PoE Switch	(J9473A)
HP ProCurve Switch 6600-24G	(J9263A)
HP ProCurve Switch 6600-24G-4XG	(J9264A)
HP ProCurve Switch 6600-24XG	(J9265A)
HP ProCurve Switch 6600-48G	(J9451A)
HP ProCurve Switch 6600-48G-4XG	(J9452A)

## 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

[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

[www.openssl.org](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)

Hewlett-Packard Company  
8000 Foothills Boulevard, m/s 5551  
Roseville, California 95747-5551  
[www.procurve.com](http://www.procurve.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.

# 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
TFTP Download from a Server .....	2
Xmodem Download From a PC or Unix Workstation .....	3
Using USB to Download Switch Software .....	4
Saving Configurations While Using the CLI .....	5
ProCurve Switch, Routing Switch, and Router Software Keys .....	6
OS/Web/Java Compatibility Table .....	7
Minimum Software Versions .....	7
<b>Clarifications</b> .....	<b>10</b>
<b>Known Issues</b> .....	<b>13</b>
Release K.14.09 .....	13
Release K.14.03 .....	13
<b>Enhancements</b> .....	<b>15</b>
Release K.14.03 Enhancements .....	15
Release K.14.04 through K.14.08 Enhancements .....	15
Release K.14.09 Enhancements .....	15
Release K.14.10 Enhancements .....	16
Locator LED Status via CLI .....	16
Increase in Number of Trunk Groups .....	16
SNTP—Client Authentication .....	17
Show VLANs Custom .....	24
Release K.14.11 through K.14.13 Enhancements .....	27
Release K.14.14 Enhancements .....	27
Release K.14.15 Enhancements .....	27
Release K.14.16 through K.14.19 Enhancements .....	27

Release K.14.20 through K.14.23 Enhancements	27
Release K.14.24 Enhancements	27
Release K.14.25	27
Release K.14.26 Enhancements	27
Release K.14.27 through K.14.29 Enhancements	28
Release K.14.30 Enhancements	28
Release K.14.31 Enhancements	28
Single Source IP Identity	28
Increase MAC Lockout to 64	35
LACP and Link Traps Global Disable	35
Clear Statistics Without Reboot	36
RADIUS Server Groups	37
SSH Secure to RADIUS	42
MAC-Auth Failure HTTP Redirect Option	44
Optional Eavesdrop Prevention	48
USB Port Config via CLI and SNMP	50
MAC Authentication Global Password	56
Release K.14.32 Enhancements	58
Release K.14.33 Enhancements	58
<b>Software Fixes</b>	<b>59</b>
Release K.14.03	59
Release K.14.04 through K.14.08	61
Release K.14.09	61
Release K.14.10	63
Release K.14.11 through K.14.13	63
Release K.14.14	63
Release K.14.15	64
Release K.14.16 through K.14.19	64
Release K.14.20 through K.14.23	64
Release K.14.24	64
Release K.14.25	65
Release K.14.26	65

Release K.14.27 through K.14.29 .....	66
Release K.14.30 .....	66
Release K.14.31 .....	66
Release K.14.32 .....	67
Release K.14.33 .....	69

# Software Management

---

## Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various HP 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 (page 4).
- 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 `K_14_xx.swi` from a TFTP server with the IP address of `10.28.227.103`:

1. Execute the copy command as shown below:

```
ProCurve # copy tftp flash 10.28.227.103 K_14_xx.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message

```
Validating and Writing System Software to FLASH...
```

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
  - a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
  - b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

**Syntax:** `boot system flash [ < primary | secondary > ]`

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the `Software revision` field.

## Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the *Installation and Getting Started Guide* for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the Send File option in the Transfer drop-down menu.)

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

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

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 115200 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 115200, execute this command:

```
ProCurve(config)# console baud-rate 115200
```

(If you use this option, be sure to set your terminal emulator to the same baud rate.)

Changing the console baud-rate requires saving to the Startup Config with the “write memory” command. Alternatively, you can logout of the switch and change your terminal emulator speed and allow the switch to AutoDetect your new higher baud rate (i.e. 115200 bps).

2. Execute the following command in the CLI:

```
ProCurve # copy xmodem flash primary
The primary OS image will be deleted. continue [y/n]? Y
Press 'Enter' and start XMODEM on your host...
```

3. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
  - a. Click on **Transfer**, then **Send File**.
  - b. Type the file path and name in the **Filename** field.
  - c. In the Protocol field, select **Xmodem**.
  - d. Click on the **Send** button.

The download can take several minutes, depending on the baud rate used in the transfer.

4. If you increased the baud rate on the switch ([step 1](#)), use the same command to return it to its previous setting. (ProCurve recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)
5. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
6. Reboot the switch from the flash area that holds the new software (primary or secondary).  
After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

## Using USB to Download Switch Software

To use the USB port on the switch to download a software version from a USB flash drive:

- The software version must be stored on the USB flash drive, and you must know the file name (such as K\_14\_09.swi).
- The USB flash drive must be properly installed in the USB port on the switch.

---

### Note

Some USB flash drives may not be supported on your switch. For information on USB device compatibility, refer to the HP ProCurve support Website:  
<http://www.hp.com/rnd/support/faqs/index.htm>.

---

**Syntax:** `copy usb flash <filename> [ < primary | secondary > ]`

For example, to download a software file named K\_14\_09.swi from a USB flash drive:

1. Execute the copy command as shown below:

```
ProCurve # copy usb flash K_14_09.swi secondary
The secondary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message  

```
Validating and Writing System Software to FLASH...
```
3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
  - a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)

## Software Management

### Saving Configurations While Using the CLI

- b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

**Syntax:** boot system flash [ < primary | secondary > ]

After the switch reboots, it displays the CLI or Main Menu, depending on the **Logon Default** setting last configured in the menu's Switch Setup screen.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the `Software revision` field.

---

## 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 **Y**es) 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>	Secure Router 7000dl Series (7102dl and 7203dl)
<b>K</b>	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
<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
<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>Software Letter</b>	<b>ProCurve Networking Products</b>
<i>numeric</i>	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.)

## OS/Web/Java Compatibility Table

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

<b>Operating System</b>	<b>Internet Explorer</b>	<b>Java</b>
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
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: – Version 1.5.0_11, Version 1.6.0
Windows Server SE 2003 SP2		
Windows Vista		

## Minimum Software Versions

**For ProCurve Series 3500, 3500yl, 6200yl, 5400zl, 6600, and 8212zl Switches and Hardware Features**

<b>ProCurve Device</b>	<b>Product Number</b>	<b>Minimum Supported Software Version</b>
HP ProCurve 10-GbE SFP+ 1m Cable	J9281B	K.14.32
HP ProCurve 10-GbE SFP+ 3m Cable	J9283B	K.14.32
HP ProCurve 10-GbE SFP+ 7m Cable	J9285B	K.14.32
HP ProCurve 3500-24 Switch	J9470A	K.14.31
HP ProCurve 3500-24-PoE Switch	J9471A	K.14.31
HP ProCurve 3500-48 Switch	J9472A	K.14.31

<b>ProCurve Device</b>	<b>Product Number</b>	<b>Minimum Supported Software Version</b>
HP ProCurve 3500-48-PoE Switch	J9473A	K.14.31
HP ProCurve Switch 6600-48G	J9263A	K.14.24
HP ProCurve Switch 6600-48G-4XG	J9452A	K.14.24
HP ProCurve 10-GbE SFP+ 1m Cable	J9281A	K.14.03
HP ProCurve 10-GbE SFP+ 3m Cable	J9283A	K.14.03
HP ProCurve 10-GbE SFP+ 7m Cable	J9285A	K.14.03
HP ProCurve 10-GbE SFP+ SR Transceiver	J9150A	K.14.03
HP ProCurve 10-GbE SFP+ LR Transceiver	J9151A	K.14.03
HP ProCurve 10-GbE SFP+ LRM Transceiver	J9152A	K.14.03
HP ProCurve Switch 6600 Premium License	J9305A	K.14.09
HP ProCurve Switch 6600-24G	J9263A	K.14.03
HP ProCurve Switch 6600-24G-4XG	J9264A	K.14.03
HP ProCurve Switch 6600-24XG	J9265A	K.14.03
ProCurve ONE Services zl Module	J9154A	K.13.51
ProCurve 100-BX-D SFP-LC Transceiver	J9099B	K.13.45
ProCurve 100-BX-U SFP-LC Transceiver	J9100B	K.13.45
ProCurve 1000-BX-D SFP-LC Mini-GBIC	J9142B	K.13.45
ProCurve 1000-BX-U SFP-LC Mini-GBIC	J9143B	K.13.45
ProCurve 10-GbE X2-SC LRM Optic	J9144A	K.13.20
ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module	J9051A and J9052A	K.12.43
Switch 8212zl Base System	J8715A	K.12.31
100-FX SFP-LC Transceiver	J9054B	K.12.01
Premium Features on Series 3500zl and 5400zl Switches	J8993A and J8994A	K.11.33
Switch 5400zl 24p Mini-GBIC Module	J8706A	K.11.33
Switch 5400zl 4p 10-GbE CX4 Module	J8708A	K.11.33

**Software Management**  
Minimum Software Versions

<b>ProCurve Device</b>	<b>Product Number</b>	<b>Minimum Supported Software Version</b>
Switch 6200yl-24G-mGBIC	J8992A	K.11.33
Switch 3500yl 2p 10GbE X2 + 2p CX4 Module	J8694A	K.11.17

# Clarifications

---

The following clarification or updates apply to documentation for the ProCurve Series 3500yl, 6200yl, 5400zl, and 8212zl Switches as of July 2008.

- **Maximum Number of VLANs Supported in Hardware for PIM-S** — Page 4-5 in the *Multicast and Routing Guide* dated January 2008 for switches running version K software incorrectly states that up to 2048 flows are supported in hardware across a maximum of 512 VLANs. Up to 2048 flows are supported across a maximum of 128 VLANs.
- **Maximum Number of Flows in the MRT** — Page 4-41 in the *Multicast and Routing Guide* dated January 2008 for switches running version K software incorrectly states that up to 1023 flows are supported. Up to 2048 flows are supported.

- **Enabling Jumbo Frames and Flow Control:**

The Series 3500yl, 6200yl, 5400zl, and 8212zl switches support simultaneous use of Jumbo Frames and Flow Control. (An earlier version of the *Management and Configuration Guide* had incorrectly stated that these features could not be enabled at the same time.)

- **Clarification for the Number of IP addresses and maximum VLANs that can be configured on the switch:**

You can configure a maximum of 512 routed VLANs per switch. A VLAN can be configured with up to 32 IP addresses. However, the maximum number of IP addresses that can be configured on the switch is 2048, so it is not possible to configure up to the maximum number of routed VLANs (512) with 32 IP addresses each. For example, if you wanted to use all available IP addresses for the switch and utilize all 512 possible routed VLANs with as many assigned IP addresses as possible, the configuration is calculated as follows:

512 routed VLANs x 4 IP addresses per VLAN = 2048 total IP addresses.

Refer to the *Advanced Traffic Management Guide* for further details.

- **TACACS+ Encryption Key Exclusion from TFTP Copies**

When using the copy command to transfer a configuration to a TFTP server, any server-specific or global encryption keys in the TACACS+ configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ user name/password information.

- **RIP and OSPF Redistribution:**

RIP operation supports static, connected, and OSPF route redistribution. OSPF operation supports static, connected, and RIP route redistribution. (The earlier version of the *Advanced Traffic Management Guide* omitted RIP and OSPF route redistribution.)

■ **Maximum UDP Broadcast Forwarding Entries:**

The number of UDP broadcast entries and IP helper addresses combined can be up to 16 per VLAN, with an overall maximum of 2048 on the switch. An earlier version of the *Multicast and Routing Guide* (page 5-142) had incorrectly stated that the overall maximum is 256.

■ **Reload Command Description**

Syntax: **Reload**

This command boots the switch from the currently active flash image and startup-config file. Because reload bypasses some subsystem self-tests, the switch boots faster than if you use a boot command. Note: To identify the currently active startup-config file, use the **show config files** command. (This is a clarification of *Syntax: Reload* (page 6.33) in the *Management and Configuration Guide*.)

Using Reload

The **reload** command reboots the switch from the flash image on which you are currently booted (primary or secondary) or the flash image that was set either by the **boot set-default** command or by the last executed **boot system flash <primary | secondary>** command. Because **reload** bypasses some subsystem self-tests, the switch reboots faster than when you use either of the **boot** command options. If you are using redundant management and redundancy is enabled when using **reload**, the switch will failover to the other management module. (This is a clarification of *Using Reload* (page 6.24) in the *Management and Configuration Guide*.)

■ **MSTP mCheck:**

Unlike other MSTP parameters, 'mCheck' is not a configurable option. It is a flag that tells MSTP to initiate transmission of RST/MST BPDUs for a MigrateTime (3 secs) period, to test whether all STP Bridges on the attached LAN have been removed and the Port can migrate to the native MSTP mode and use RST/MST BPDUs for transmission. The 'mCheck' is always cleared (set FALSE) prior to port initialization. Some of the earlier ProCurve MSTP implementations allowed the 'mCheck' option to be a configurable parameter. It was stored in the config. That was corrected beginning with version K.12.04.

■ **Virus-Throttling (Connection-rate filtering):**

As of release K.12.01, this feature enables notification of worm-like behavior detected on all inbound IP traffic. (The Advanced Traffic Management Guide retains some incorrect references to filtering on IP routed traffic only.)

■ **Menu Interface Configuration Limit:**

The menu interface allows the user to perform VLAN port assignment for up to 32 VLANs. CLI or Web Management Interface should be used for VLAN port assignment beyond 32 VLANs.

The following clarifications apply to documentation as of June 2009.

■ **Virtual Stacking (3500yl/6200yl Series switches only)/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.

- **Out of Band Management (OOBM) on 6600 Series switches/IPv6:**  
IPv6 configuration of the OOBM interface is not supported; only IPv4 addresses are supported.

# Known Issues

---

## Release K.14.09

The following problems are known issues as of release K.14.09.

- **10-GbE (PR\_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link, and 10-GbE X2 transceivers may fail to initialize entirely or they may initialize only after a long delay.

## Release K.14.03

The following problems are known issues as of release K.14.03.

- **CLI (PR\_0000008236)** — The **enable** CLI command is listed in enable-mode help.
- **Config (PR\_0000014381)** — Switches running K.14.03 or newer software may be unable to upload a valid config file to the switch, if it is set with the parameter, speed-duplex 1000-full, and on a dual personality port with a mini-GBIC inserted. The switch will display a message similar to the following. (The example below contained the speed-duplex value in line 8 of the config, and the value was applied to port 47.)

```
line: 8. Value 1000-full is not applicable to port 47.  
Corrupted download file.
```

- **Config (PR\_0000014818)** — Although the switch CLI provides an appropriate error message when the user tries to add more MAC addresses than a port is configured to allow, it seems to save the excess MAC addresses and display them in the configuration.
- **Syslog (PR\_0000008241)** — Event log messages with a severity of "E" (error) are not always supported by default on syslog servers. The fix will update the **show logging** help text to clarify the dependency. In order to modify the syslog configuration file on a Linux server in order to receive error messages, complete the following steps.

1. # vim /etc/syslog.conf
2. Add the following line in the syslog.conf file:

```
*.* /var/log/messages
```
3. # /etc/init.d/syslog restart

- **Syslog (PR\_0000012167)** — Syslog messages longer than 119 characters get truncated.

- **VRRP (PR\_0000016192)** — In a VRRP topology with only VRRP Backups configured (i.e. there is no Master/Owner present in the setup), initializing the VRID(s) on both Backups at exactly the same time (e.g. after loss and restoration of power to all switches at once) can lead to a situation where both Backups will enter a continuous sequence of failovers.
- **IGMP (PR\_0000009415)** — The switch may intermittently fail to forward a multicast stream.

## Enhancements

---

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

Release K.14.03 is the first production software release for the HP ProCurve 6600 switches.

### Release K.14.03 Enhancements

The following enhancements, present in K.13.40 and newer K.13 versions, are NOT present in K.14.03:

**Enhancement (PR\_0000003127)** — Link Trap and LACP Global Enable/Disable.

**Enhancement (PR\_0000003128)** — The ability to clear statistics was added.

**Enhancement (PR\_0000003718)** — The MAC Lockout limit was increased to 64.

**Enhancement (PR\_0000007388)** — The ability to configure logging via SNMP was added.

The following enhancement, present in K.13.43 and newer K.13 versions, is NOT present in K.14.03:

**Enhancement (PR\_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added.

The following enhancements, present in K.13.51 and newer K.13 versions, are NOT present in K.14.03.

**Enhancement (PR\_0000003144)** — Support was added for multiple RADIUS groups.

**Enhancement (PR\_0000003141)** — Support was added for SSH Secure to RADIUS authentication.

**Enhancement (PR\_0000000083)** — Support was added for a MAC-Auth failure HTTP Redirect option.

The following enhancements, present in K.13.52 and newer K.13 versions, are NOT present in K.14.03.

**Enhancement (PR\_0000013786)** — Support was added for source IP identification.

**Enhancement (PR\_0000008243)** — Support was added for an eavesdrop prevention option.

### Release K.14.04 through K.14.08 Enhancements

*No new enhancements, software never built.*

### Release K.14.09 Enhancements

Release K.14.09 includes the following enhancements.

- **Enhancement (0000017065)** — Support was added for the HP ProCurve 6600 Switch Premium License (J9305A) features.

## Release K.14.10 Enhancements

Release K.14.10 includes the following enhancements.

- **Enhancement (PR\_0000011224)** — Support was added for chassis locator LED status with the CLI.

### Locator LED Status via CLI

The **chassislocate** parameter provides a way to check the status of the blue Locator LED with a CLI command. The status will be displayed, and if the status is ON or BLINK, the amount of time the LED will continue to be on or to blink is displayed. .

**Syntax:** show system chassislocate

*Displays the chassis Locator LED status. Possible values are On, Off, or Blink. When the status is On or Blink, the number of minutes that the Locator LED will continue to be on or to blink is displayed.*

```
ProCurve(config)# show system chassislocate
Chassis Locator LED: ON 5 minutes 5 seconds

ProCurve(config)# show system chassislocate
Chassis Locator LED: BLINK 10 minutes 6 seconds

ProCurve(config)# show system chassislocate
Chassis Locator LED: OFF
```

**Figure 1. Example of Command Results for show system chassislocate Command**

- **Enhancement (PR\_0000011601)** — Support was added for an increased number of LACP trunk groups.

### Increase in Number of Trunk Groups

The number of trunk groups per switch is increased from 60 trunk groups to 144 trunk groups. The maximum number of ports per trunk remains at eight. The trunks do not have to be the same size, for example 100 two-port trunks and 11 eight-port trunks are supported.

- **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. See “Configuring Unicast and Broadcast Mode” on page 20.
- 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 2. 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 value is configured as “trusted”, the authentication succeeds. Only trusted key-id value information is used for SNTP authentication. See “Configuring Unicast and Broadcast Mode” on page 20 for information about configuring these modes.

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 3. 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 4. 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 5. 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 6. Example of SNTP Authentication Statistical Information**

### Saving Configuration Files and the Include-Credentials Command

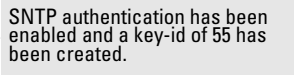
You can use the **include-credentials** command to store security information in the running-config file. This allows you to upload the file to a TFTP server and then later download the file to the ProCurve switches on which you want to use the same settings. For more information about the **include-credentials** 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
.
.
.
```



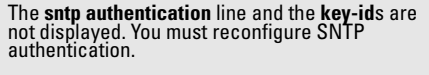
**Figure 7. Example of Configuration File with SNTP Authentication Information**

In [Figure 7](#), 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 8](#).

```
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
.
.
.
```



**Figure 8. Example of a Retrieved Configuration File When Include Credentials is not Configured**

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

```
ProCurve(config)# show config

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

The diagram shows two callout boxes with arrows pointing to specific lines in the configuration output. The first callout box, labeled 'Include-credentials is configured.', points to the 'include-credentials' line. The second callout box, labeled 'All of the SNTP authentication information displays in the configuration file, including the key-values.', points to the 'sntp authentication' lines.

**Figure 9. Example of Saved SNTP Authentication Information when include-credentials is Configured**

- **Enhancement (PR\_0000013247)** — Support was added for the **show VLANs custom** CLI commands.

## Show VLANs Custom

The **show vlans custom** command allows you to customize the information displayed when executing the **show vlans** command.

**Syntax:** show vlans custom [port <port-list>] column-list

*Select the information that you want to display in the order you want to display it for the **show vlans** command. You can display information for one port or range of ports. If <port-list> isn't specified, then all ports display.*

Fields that can be included in the customized display are shown in the table below.

Field	Display	Example	Default
id	VLAN Id	5	6
name	VLAN Name	Vlan55	32
status	Status	Port-based	10
voice	Voice enabled	No	5

**Enhancements**  
Release K.14.10 Enhancements

Field	Display	Example	Default
jumbo	Jumbos enabled	No	5
ipconfig	How the ip address was configured	Manual Disabled DHCP/BootP	10
ipaddr (IPv4) ipaddr (IPv6)	the IP address(es)	10.10.10.3 fe80::212:79ff:fe8d:8000	15 for IPv4 46 for IPv6
ipmask	The subnet mask(s)	255.255.255.6 /64 (prefix for IPv6 is in format "/XX")	15
proxyarp	Whether proxy arp is configured	No	5
localproxyarp	Whether local proxy arp is configured	No	9
state	"Up" if at least one port is up	Up	5

The example in [Figure 10](#) displays **id** at its default width, and will show up to 20 characters of the VLAN **name**. The columns selected for display are separated by spaces.

```

ProCurve(config)# show vlan custom A1-A3 id name:20 ipaddr state

Status and Counters - VLAN Information - Custom view

VLANID  VLAN name                IP Addr                        State
-----  -
1        DEFAULT_VLAN                15.255.134.74                 Up
33       Vlan33                      10.10.10.01                   Up
44       Vlan44                      15.255.164.13                 Up
55       Vlan55                      15.255.178.2                  Down
                    15.255.178.3
                    15.255.178.4
60       Vlan60                      fe80::212:79ff:fe8d:8000%vlan60 Up

```

**Figure 10. Example of show vlan custom Command**

If the width of the column requested is smaller than the header name of the column, the display of the header name is truncated.

```

ProCurve(config)# show vlan custom id
Status and Counters - VLAN Information - Custom view

VLANID
-----
1
33
44

ProCurve(config)# show vlan custom id:2
Status and Counters - VLAN Information - Custom view

VL
--
1
33
44

```

**Figure 11. Example of Column Headers**

The total output will wrap if it is longer than the terminal width (for example, 80 characters). It is not truncated.

### Creating an Alias for Show VLAN Commands

You can create an alias for a frequently used **show vlans custom** command to avoid entering the selected columns each time you use the command.

```

ProCurve(config)# alias showvlanstatus = "show vlan custom A1-A3 id name:20
status"

ProCurve(config)# showvlanstatus
Status and Counters - VLAN Information - Custom view

VLANID VLAN name                Status
-----
1      DEFAULT_VLAN                Port-based
33     Vlan33                        Port-based

```

**Figure 12. Example of the alias Command**

### Note on Using Pattern Matching with the “Show VLANs Custom” Command

If you have included a pattern matching command to search for a field in the output of the **show vlan custom** command and the **show vlans custom** command produces an error, the error message may not be visible and the output is empty. For example, if you enter a command that produces an error (vlan is misspelled) with the pattern matching **include** option:

## Enhancements

Release K.14.11 through K.14.13 Enhancements

```
ProCurve(config)# show vlans custom 1-3 name vlun | include vlan1
```

the output may be empty. It is advisable to try the **show vlans custom** command first to ensure there is output, and then enter the command again with the pattern matching option.

## Release K.14.11 through K.14.13 Enhancements

*No new enhancements, software never built.*

## Release K.14.14 Enhancements

*No new enhancements, software fixes only. (Never released)*

## Release K.14.15 Enhancements

*No new enhancements, software fixes only.*

## Release K.14.16 through K.14.19 Enhancements

*Software never built.*

## Release K.14.20 through K.14.23 Enhancements

*Software never released.*

## Release K.14.24 Enhancements

- **Enhancement (PR\_0000041097)** — Support was added for the HP ProCurve 6600-48G (J9451A) and HP ProCurve 6600-48G-4XG (J9452A) Switches.

## Release K.14.25

*Software never built.*

## Release K.14.26 Enhancements

*No new enhancements, software fixes only.*

## Release K.14.27 through K.14.29 Enhancements

*Software never built.*

## Release K.14.30 Enhancements

*Software never released.*

## Release K.14.31 Enhancements

- **Enhancement (PR\_0000013786)** — Support is added for source IP identification.

### Single Source IP Identity

#### Overview

This enhancement applies to the following software applications:

- TACACS
- RADIUS
- System Logging applications

The above IP-based software applications use a client-server communication model, that is, the client's source IP address is used for unique client identification. The source IP address is determined by the system and is usually the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces due to load balancing or routing redundancy, and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses, which creates a client identification problem on the server site. For example, there is no way to designate a fixed IP address for outgoing packets for RADIUS or TACACS, so it is necessary to configure in the RADIUS or TACACS database all possible IP addresses that are configured on the switch as valid clients. When using system logging, it can be difficult to interpret the logging and accounting data on the server site as the same client can be logged with different IP addresses.

To decrease the amount of administrative work involved, a configuration model is provided that allows the selection of an IP address to use as the source address for all outgoing traffic generated by a specified software application on the switch. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server.

## Specifying the Source IP Address

The CLI command **ip source-interface** is used to specify the source IP address for an application. Different source IP addresses can be used for different software applications, but only one source IP address can be specified for each application.

**Syntax:** [no] ip source-interface <radius | tacacs | logging | all> <loopback <id> | vlan <vlan-id> address <ip-address>>

*Determines the source IP address used by the specified software application when transmitting IP packets. The **all** parameter can be used to set one IP address for all the listed applications, in this case, RADIUS, TACACS, and System Logging.*

*The **no** version of the command cancels the configuration and the application reverts to its default behavior. The system determines the source IP address of outgoing application-specific IP packets at packet transmission time.*

*loopback <id>: Specifies that the IP address of the loopback interface is used as the source IP address in outgoing packets. If the loopback interface has no IP address, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

*vlan <vlan-id>: Specifies that the IP address of the indicated VLAN interface is used as the source IP address of outgoing packets. If the specified VLAN interface has no IP address configured, or is down, then the application reverts to the default behavior. If more than one IP address is configured, then the lowest IP address is used.*

*address <ip-address>: Specifies the IP address that should be used as the source IP address of outgoing packets. The IP address must be a valid IP address configured on one of the switch's VLAN or loopback interfaces. If the interface is down, then the application reverts to the default behavior.*

## The Source IP Selection Policy

The source IP address selection for the application protocols is defined through assignment of one of the following policies:

- **Outgoing Interface**—the IP address of the outgoing IP interface is used as the source IP address. This is the default policy and the default behavior of applications.
- **Configured IP Address**—the specific IP address that is used as the source IP address. This address is configured on one of the switch's IP interfaces, either a VLAN interface or a Loopback interface.
- **Configured IP Interface**—the IP address from the specific IP interface (VLAN or Loopback) is used as the source IP address. If there are multiple IP addresses assigned (multinetting, for example), the lowest IP address is used.

If the selection policy cannot be executed because the interface does not have an IP address configured, does not exist, or is down, the application protocol uses the default Outgoing Interface policy. A warning message is displayed, but the configuration changes are accepted. When using the **show ip source-interface status** command to display information about the source IP address selection policy, the administratively-assigned source IP selection policy and the actual (operational) source IP selection policy in effect are displayed. The operational source IP selection policy may be different from the assigned source selection policy if the IP interface does not exist or is down. In this case, the default of Outgoing Interface appears as the operational policy. See [Figure 13](#).

```
ProCurve (config)# show ip source-interface detail

Source-IP Detailed Information

Protocol : Tacacs
Admin Policy           : Configured IP Interface
Oper Policy            : Outgoing Interface
Source IP Interface    : Vlan 22
Source IP Address      : 10.10.10.4
Source Interface State : Down
```

The Admin Policy differs from the Oper Policy because the Source Interface State is Down. The default Outgoing Interface policy is actually in effect.

**Figure 13. Example of the Administratively-assigned Source IP Selection Policy Differing From the Operational Policy**

The **no** form of the **ip source-interface** command reverts the application protocols to the default behavior. The Outgoing Interface policy is used.

[Figure 14](#) is an example of assigning a specific source IP address for a RADIUS application. The administrative policy is Configured IP Address.

```
ProCurve(config)# ip source-interface radius address 10.10.10.2

ProCurve(config)# show ip source-interface radius

Source-IP Configuration Information

Protocol | Admin Selection Policy | IP Interface | IP Address
-----+-----
```

Protocol	Admin Selection Policy	IP Interface	IP Address
Radius	Configured IP Address	vlan 3	10.10.10.2

**Figure 14. Example of a Specific IP Address Assigned for the RADIUS Application Protocol**

In [Figure 15](#), a VLAN interface (VLAN 22) is specified as the source IP address for TACACS. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface tacacs vlan 22
ProCurve(config)# show ip source-interface tacacs

Source-IP Configuration Information

Protocol | Admin Selection Policy | IP Interface | IP Address
-----+-----
Tacacs   | Configured IP Interface | vlan 22     | 10.10.10.4
```

**Figure 15. Example of Using a VLAN Interface as the Source IP Address for TACACS**

[Figure 16](#) shows a VLAN interface being specified as the source IP address for logging. The administrative policy is Configured IP Interface.

```
ProCurve(config)# ip source-interface syslog vlan 10
ProCurve(config)# show ip source-interface syslog

Source-IP Configuration Information

Protocol | Admin Selection Policy | IP Interface | IP Address
-----+-----
Syslog   | Configured IP Interface | vlan 10     | 10.10.10.10
```

**Figure 16. Example of Using a VLAN Interface as the Source IP Address for Logging (Syslog)**

## Displaying the Source IP Interface Information

There are several **show** commands that can be used to display information about the source IP interface status.

**Syntax:** show ip source-interface status [radius | tacacs | syslog]

*Displays the operational status information for the source IP address selection policy. Both the administratively-assigned source IP selection policy and the operational source IP selection policy are displayed.*

*When no parameters are specified, policy information for all protocols is displayed.*

```
ProCurve(config)# show ip source-interface status

Source-IP Status Information

Protocol | Admin Selection Policy  Oper Selection Policy
-----+-----
Tacacs   | Configured IP Interface Configured IP Interface
Radius   | Configured IP Address   Configured IP Address
Syslog   | Configured IP Interface Outgoing Interface
```

**Figure 17. Example of the Data Displayed for Source IP Interface Status**

When executing the **show ip source-interface** command without parameters, the configured IP interfaces (VLANs) and IP addresses are displayed for each protocol.

```
ProCurve(config)# show ip source-interface

Source-IP Configuration Information

Protocol | Admin Selection Policy  IP Interface  IP Address
-----+-----
Tacacs   | Configured IP Interface vlan 22          10.10.10.4
Radius   | Configured IP Address   vlan 3         10.10.10.2
Syslog   | Configured IP Interface vlan 10          10.10.10.10
```

**Figure 18. Example of show ip source-interface Command Output**

The **show ip source-interface detail** command displays detailed information about the configured policies, source IP address, and interface state for each protocol.

**Syntax:** show ip source-interface detail [radius | tacacs | syslog]

*Displays detailed operational status information for the source IP address selection policy. Information about the configured policies, source IP address and interface state are displayed.*

*When no parameters are specified, policy information for all protocols is displayed.*

```
ProCurve(config)# show ip source-interface detail

Source-IP Detailed Information

Protocol : Tacacs
Admin Policy      : Configured IP Interface
Oper Policy      : Configured IP Interface
Source IP Interface : vlan 22
Source IP Address  : 10.10.10.4
Source Interface State : Up

Protocol : Radius
Admin Policy      : Configured IP Address
Oper Policy      : Configured IP Address
Source IP Interface : vlan 3
Source IP Address  : 10.10.10.2
Source Interface State : Up

Protocol : Syslog
Admin Policy      : Configured IP Interface
Oper Policy      : Configured IP Interface
Source IP Interface : vlan 10
Source IP Address  : 10.10.10.10
Source Interface State : Up
```

**Figure 19. Example of Detailed Information Displayed for Each Protocol**

The **show** command can also be used with the application to display the source IP address selection information in effect for the application protocol.

```
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

  Deadttime (min) : 0
  Timeout (secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :
  Dynamic Authorization UDP Port : 3799
  Source IP Selection : Configured IP address ← Source IP Selection for the specified
                                                application protocol is displayed.
```

**Figure 20. Example of show radius Command Displaying Source IP Selection Information**

```
ProCurve(config)# show tacacs

Status and Counters - TACACS Information

  Timeout : 5
  Source IP Selection : Configured IP Interface ← Source IP Selection for the specified
                                                application protocol is displayed.
  Encryption Key :
```

**Figure 21. Example of show tacacs Command Displaying Source IP Selection Information**

```
ProCurve(config)# show debug

Debug Logging

  Source IP Selection: Configured IP interface ← Source IP Selection for the specified
                                                application protocol is displayed.
  Destination:      None

  Enabled debug types:
  None are enabled.
```

**Figure 22. Example of show debug Command Displaying Source IP Selection Information for Syslog**

## Error Messages

The following error messages may appear when configuring source IP selection if the interface does not exist, is not configured for IP, or is down.

Error Message	Description
Warning: Specified IP address is not configured on any interface	The IP address specified has not been assigned to any interface on the switch.
Warning: Specified IP interface is not configured	The IP interface has not been configured.
Warning: Specified IP interface is not configured for IP	An IP address has not been assigned to this interface.
Warning: Specified IP interface is down.	The interface on the switch associated with this IP address is down.
Warning: Specified IP interface is configured for DHCP	The IP address has not been configured specifically (manually) for this interface and may change.

- **Enhancement (PR\_0000003718)** — The MAC Lockout limit was increased to 64.

### Increase MAC Lockout to 64

The MAC lockout feature allows all traffic to or from a given MAC address to be dropped by the switch. A MAC address can exist on many different VLANs, so a lockout MAC address must be added to the MAC table as a drop. As this can quickly fill the MAC table, restrictions are placed on the number of lockout MAC addresses based on the number of VLANs configured. The restriction for the range of 17-256 VLANs is being increased to allow up to 64 lockout MAC addresses.

VLANs Configured	Number of MAC Lockout Addresses	Total Number of MAC Addresses
1-8	200	1,600
9-16	100	1,600
<b>17-256</b>	<b>64</b>	<b>16,384</b>
257-1024	16	16,384
1025-2048	8	16,384

- **Enhancement (PR\_0000003127)** — Link Trap and LACP Global Enable/Disable.

### LACP and Link Traps Global Disable

Two SNMP commands are added to allow disabling of LACP and link traps on multiple ports at one time. The new commands operate in the same manner as the CLI commands **no int all lacp** and **no snmp-server enable traps link-change all**.

The new SNMP OIDs are:

```
hpSwitchLACPConfig OBJECT IDENTIFIER ::= { hpSwitchConfig 28 }
```

```
hpSwitchLACPAllPortsStatus OBJECT-TYPE
    SYNTAX INTEGER {
        disabled (1),
        active (2),
        passive (3)
    }

    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "Used to set administrative status of LACP on all the
        ports. A Port can have one of the three
        administrative status of LACP.
        Active/Passive/Disabled are the three states."
    ::= { hpSwitchLACPConfig 1 }

hpSwitchLinkUpDownTrapAllPortsStatus OBJECT-TYPE
    SYNTAX INTEGER {
        enable (1),
        disable (2)
    }

    ACCESS read-write
    STATUS current
    DESCRIPTION "Used to either enable/disable the Link Up/Link Down traps
        for all the ports."
    ::= { hpSwitchPortConfig 3 }
```

- **Enhancement (PR\_0000003128)** — The ability to clear statistics was added.

## Clear Statistics Without Reboot

It is useful to be able to clear all counters and statistics without rebooting the switch when troubleshooting network issues. The **clear statistics global** command clears all counters and statistics for all interfaces except SNMP. You can also clear the counters and statistics for an individual port using the **clear statistics <port-list>** command.

**Syntax:** clear statistics <<port-list> | global >

*When executed with the <port-list> option, clears the counters and statistics for an individual port. When executed with the global option, clears all counters and statistics for all interfaces except SNMP.*

The **show interfaces** [**<port-list>**] command displays the totals accumulated since the last boot or the last **clear statistics** command was executed. The menu and web pages also display these totals.

SNMP displays the counter and statistics totals accumulated since the last reboot; it is not affected by the **clear statistics global** command or the **clear statistics <port-list>** command. An SNMP trap is sent whenever the statistics are cleared.

---

## Note

The clearing of statistics cannot be uncleared.

---

- **Enhancement (PR\_0000016121)** — Support is added for multiple RADIUS groups

## RADIUS Server Groups

### Overview

The authentication and accounting features on the switch can use up to three RADIUS servers, a primary server and two backup servers. This feature allow the RADIUS servers to be put into a group. The same three RADIUS servers would continue to be used. Up to 5 groups of RADIUS servers can be configured. The authentication and accounting features can choose which RADIUS server group to communicate with. End-user authentication methods (802.1X, MAC-based and web-based) can authenticate with different RADIUS servers from the management interface authentication methods (console, telnet, ssh, web).

### Commands Used

Several commands are used to support the RADIUS server group feature. The RADIUS server must be configured before it can be added to a group. See “RADIUS Authentication and Accounting” in the *Access Security Guide* for your switch for more information on configuring RADIUS servers.

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

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration. You can configure up to three RADIUS server addresses. The switch uses the first server it successfully accesses.*

**Syntax:** aaa server-group radius <group-name> host <ip-addr>  
no aaa server-group radius <group-name> host <ip-addr>

*Associates a RADIUS server with a server group.*

*The **no** form of the command removes the RADIUS server with the indicated IP address from the server group. If that server was the last entry in the group, the group is removed.*

**radius <group-name>:** *The group name of the RADIUS server group. The name has a maximum length of 12 characters. Up to five groups can be configured with a maximum of three RADIUS servers in each group. The first group slot is used by the default group.*

**host <ip-addr>:** *The IP address of the RADIUS server to be used.*

## Enhanced Commands

The following commands have the **server-group** option. If no **server-group** is specified, the default RADIUS group is used. The server group must have already been configured.

---

### Note

The last RADIUS server in a server group cannot be deleted if an authentication or accounting method is using the server group.

---

**Syntax:** aaa authentication <console | telnet | ssh | web> <enable | login <local | radius [server-group <group-name> | local | none | authorized]>>

*Configures the primary password authentication method for console, Telnet, SSH, and/or the web browser interface.*

**<enable | login>:** *Primary authentication method. Default: local*

**<local | radius>:** *Use either the local switch user/password database or a RADIUS server for authentication.*

**<server-group <group-name> >:** *Specifies the server group to use.*

**[ local | none | authorized ]:** *Provides options for secondary authentication (default: none). Note that for console access, secondary authentication must be **local** if primary access is not **local**. This prevents you from being locked out of the switch in the event of a failure in other access methods.*

**Syntax:** aaa authentication <port-access <local leap-radius | chap-radius> | <mac-based | web-based <chap-radius | peap-mschapv2> [none | authorized | server-group <group-name>] >>

*Configures the primary authentication method for port-access, MAC-based, or web-based access.*

**mac-based | web-based <chap-radius | peap-mschapv2>:** *Password authentication for web-based or MAC-based port access to the switch. Use **peap-mschapv2** when you want password verification without requiring access to a plain text password; it is more secure. Default: **chap-radius***

**port-access <local leap-radius | chap-radius>:** *Configures **local**, **chap-radius** (MD5), or **eap-radius** as the primary password authentication method for port-access. The default primary authentication is **local**. (Refer to the documentation for your RADIUS server application.)*

**[none | authorized | server-group <group-name>]:**

**none:** *No backup authentication method is used.*

**authorized:** *Allow access without authentication*

**server-group <group-name>:** *Specifies the server group to use with RADIUS.*

■

**Syntax:** aaa accounting <exec | network | system | commands | <start-stop | stop-only>  
radius [server-group <group-name>]

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

**radius:** *Uses RADIUS protocol as accounting method.*

**server-group <group-name>:** *Specifies the server group to use with RADIUS.*

## Displaying the Server Group Information

The **show server-group radius** command displays the same information as the **show radius** command, but displays the servers in their server groups.

```
ProCurve(config)# show server-group radius
```

```
Status and Counters - AAA Server Groups
```

```
Group Name: radius
```

Server IP Addr	Auth Port	Acct Port	DM/ CoA	Time Window	Encryption Key
192.168.1.3	1812	1813	No	300	default_key
192.168.3.3	1812	1813	No	300	grp2_key
192.172.4.5	1812	1813	No	300	grp2_key
192.173.6.7	1812	1813	No	300	grp2_key
192.168.30.3	1812	1813	No	300	grp3_key
192.172.40.5	1812	1813	No	300	grp3_key
192.173.60.7	1812	1813	No	300	grp3_key

```
Group Name: group2
```

Server IP Addr	Auth Port	Acct Port	DM/ CoA	Time Window	Encryption Key
192.168.3.3	1812	1813	No	300	grp2_key
192.172.4.5	1812	1813	No	300	grp2_key
192.173.6.7	1812	1813	No	300	grp2_key

```
Group Name: group3
```

Server IP Addr	Auth Port	Acct Port	DM/ CoA	Time Window	Encryption Key
192.168.30.3	1812	1813	No	300	grp3_key
192.172.40.5	1812	1813	No	300	grp3_key
192.173.60.7	1812	1813	No	300	grp3_key

**Figure 1. Example of Output from show server-group radius Command**

```
ProCurve(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

Server group information
├── Login
│   ├── Primary
│   ├── Server Group
│   ├── Login Secondary
│   ├── Enable Primary
│   └── Server Enable Group
└── Enable Secondary

Access Task | Login Primary | Server Group | Login Secondary | Enable Primary | Server Enable Group | Enable Secondary
-----+-----+-----+-----+-----+-----+-----
Console | Local | radius | None | Local | radius | None
Telnet | Local | radius | None | Radius | group2 | None
Port-Access | Local | | None | | | |
Webui | Local | | None | Local | | None
SSH | Local | | None | Local | | None
Web-Auth | ChapRadius | group3 | None | | | |
MAC-Auth | ChapRadius | group3 | None | | | |
```

**Figure 2. Example of Output from show authentication Command**

```
ProCurve(config)# show accounting

Status and Counters - Accounting Information

Interval(min) : 0
Suppress Empty User : No

Server group information
├── Method
├── Mode
└── Server Group

Type | Method | Mode | Server Group
-----+-----+-----+-----
Network | None | | |
Exec | Radius | Start-Stop | group2
System | Radius | Stop-Only | group2
Commands | Radius | Start-Stop | radius
```

**Figure 3. Example of Output from show accounting Command**

- **Enhancement (PR\_0000003141)** — Support is added for SSH Secure to RADIUS authentication.

## SSH Secure to RADIUS

It is desirable to have an additional method for authentication that allows the storage of passwords in a secure manner rather than as plain text. The MS-CHAPV2 authentication method allows password verification without requiring access to a plain text password. This method is provided for these types of authentication:

- telnet
- SSH
- console

MS-CHAPv2 is currently supported for web authentication and MAC authentication on the switch.

The **aaa authentication** command is modified to provide the MS-CHAPv2 authentication method to the above options. After selecting one of these options, you can choose the authentication method, either **radius** (the default) or the more secure **peap-mschapv2** authentication method.

**Syntax:** aaa authentication [console | telnet] [enable | login] [radius | peap-mschapv2 | tacacs | local]  
aaa authentication web [enable | login] [radius | peap-mschapv2 | local]  
aaa authentication ssh [enable | login] [radius | peap-mschapv2 | tacacs | local | public-key]

*Select the authentication method, **radius** (ChapRadius) or the more secure **peap-mschapv2** (PeapRadius).*

**Default:** ChapRadius

---

### Note

An authentication type of “radius” is interpreted as “ChapRadius”.

---

```
ProCurve(config)# aaa authentication ssh peap-mschapv2
```

**Figure 4. Example Command with peap-mschapv2 Option Selected**

The show authentication command will display which authentication method has been configured.

```
ProCurve(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

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

**Figure 5. Example of show authentication Command Displaying Different Authentication Types**

## MIB Support

The hpicfAuth.mib will be as follows:

```
hpSwitchAuthenEnablePrimary OBJECT-TYPE
    SYNTAX      INTEGER {
                    local (1),
                    tacacs (2),
                    radius (3),
                    sshPubkey (6),
                    radiusPeapMSChapv2 (7)
                }
    MAX-ACCESS  read-write
    STATUS      current

    DESCRIPTION "Indicates the primary authentication mechanism,
                 i.e. whether TACACs+/RADIUS/local will be tried
                 first for a change of a privilege level of session."
 ::= { hpSwitchAuthenEntry 4 }
```

- **Enhancement (PR\_000000083)** — Support is added for a MAC-Auth failure HTTP Redirect option.

## MAC-Auth Failure HTTP Redirect Option

### Overview

When a client's MAC address is checked by the RADIUS server against the known list of MAC addresses, and the MAC address is not found, the client needs a way to quickly become registered through a web registration process. The HTTP Redirect feature provides a way for a client who has failed MAC authentication to become registered through a web/registration server. Only a web browser is required for this authentication process.

---

### Notes

The HTTP redirect feature cannot be enabled if web authentication is enabled on any port, and conversely, if HTTP redirect is enabled, web authentication cannot be enabled on any port.

The web/registration server software is not included with this feature.

---

### How HTTP Redirect Works

The **unauth-redirect** option must be configured with the registration server's URL as a parameter before HTTP redirect operations can begin. The full URL must be used, for example:

`http://14.29.16.192:80/myServer.html`

or

`https://company.com/myServer.html`

**Syntax:** [no] aaa port-access mac-based unauth-redirect

*Configure the HTTP redirect registration server feature.*

*<redirect-URL-st>*

*Enable HTTP redirect registration server feature by configuring the URL of the registration page. An entry can have either an IP address or a DNS name. Only one server can be configured.*

**Note:** *The entire URL must be used, including the "http://" or "https://" portion.*

[restrictive-filter]

*Enable the redirect server to only return a Warning or Information page.*

[timeout <seconds>]

*The time (in seconds) before a client in an unauthorized redirection state is removed from the state tables.*

*Range: <30-10800> seconds*

*Default: 1800 seconds*

---

## **Caution**

Rogue clients can attempt to access any web pages on the web/registration server via interface ports configured for MAC authentication.

---

The following steps are involved in HTTP registration.

1. When the redirect feature is enabled, a client that fails MAC authentication is moved into the unauthorized MAC authentication redirection state.
2. A client in the redirect state (having failed MAC authentication) with a web browser open sends a DHCP request. The switch responds with a DHCP lease for an address in the switch's configurable DHCP address range. Additionally, the switch's IP address becomes the client's default gateway. All ARP/DNS requests are handled by the switch and all requests are directed to the switch. The switch replies to these requests with its own address.
3. The client requests a web page. The switch takes this request and responds to the client browser with an HTTP redirect to the configured URL. The client MAC address and interface port are appended as HTTP parameters.
4. Before returning the initial registration page to the client, the switch enables NAT so that all subsequent requests will go to the web server directly. The initial HTML page is returned to the switch and then proxied to the client.
5. After the registration process completes, the registration server updates the RADIUS server with the client's username, password, and profile.
6. The client remains in the redirect state until the client's time exceeds the configured timeout or the switch receives an SNMP deauthentication request from the registration server.
7. The registration server sends an SNMP request to the switch with the MAC identification and interface port to reauthenticate or deauthenticate the client.
8. The switch moves the client out of the special Web/MAC auth redirect state and the client becomes unknown to the switch again. This sets the stage for a new MAC authentication cycle.

## Diagram of Registration Process

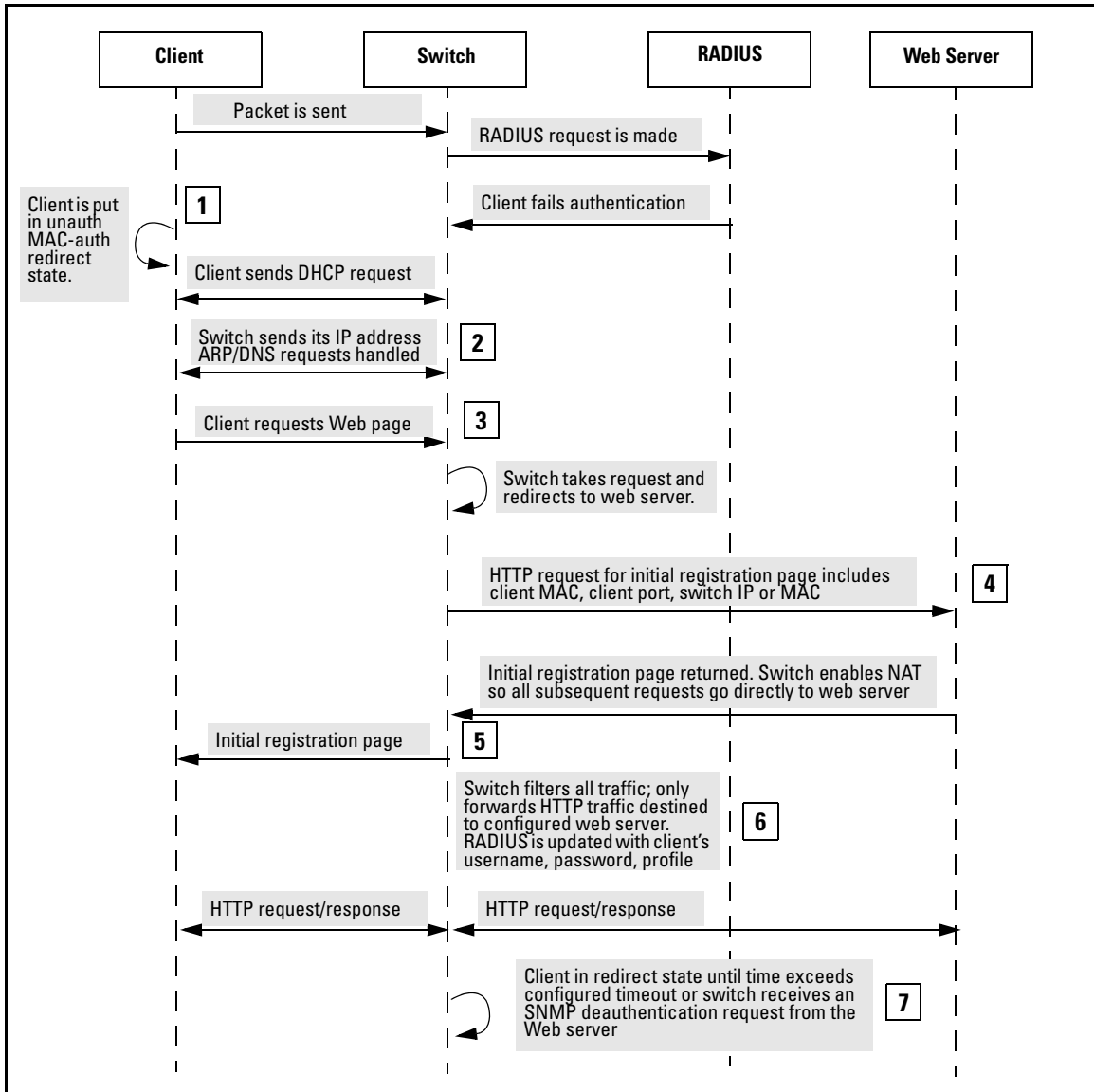


Figure 6. Example of Registration Process Using Redirection

## Using the Restrictive-Filter Option

The **restrictive-filter** option allows the switch to reply to all HTTP requests to the switch's IP address with an HTTP-redirect containing the URL of the registration server. It is used when there is no registration process and only a warning or informational page is displayed to the client.

If SSL is not configured, the switch verifies that the MAC address and interface port parameters are present. If SSL is enabled, the switch ensures that the HTTP request is to the registration server's destination IP address.

## Show Command Output

Figure 7 is an example of the **show** command that displays the HTTP redirect configuration.

```
ProCurve(config)# show port-access mac-based config
Port Access MAC-Based Configuration
MAC Address Format : no-delimiter
Unauth Redirect Configuration URL : http://14.29.16.192:80/myserver.html
Unauth Redirect Client Timeout (sec) : 1800
Unauth Redirect Restrictive Filter : Disabled
Total Unauth Redirect Client Count : 1
```

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-Auth Period	Unauth VLAN ID	Auth VLAN ID	Cntrl Dir
1	No	1	No	300	0	0	0	both
2	No	1	No	300	0	0	0	both
3	No	1	No	300	0	0	0	both
4	No	1	No	300	0	0	0	both

Figure 7. Example of HTTP Redirect Configuration

## Reauthenticating a MAC-Auth Client

### Using SNMP

The MIB variable `hpicfUsrAuthMacAuthClientReauthenticateEntry` in the `hpicfUsrAuthMIB` provides the capability to reauthenticate a specific MAC-auth client on a port. The MAC address and port are required for SNMP reauthentication.

### Using the CLI

To reauthenticate a client using the CLI, use this command:

```
ProCurve(config)# aaa port-access mac-based <single-port>  
                    reauthenticate mac-addr <MAC address>
```

The keyword **mac-addr** specifies single client reauthentication. If the **reauthenticate** parameter is entered without the **mac-addr** keyword and MAC address, the command is executed as port reauthentication—all clients on a port are reauthenticated.

### Configuring the Registration Server URL

To configure the registration server URL, the command is:

```
ProCurve(config)# aaa port-access mac-based unauth-redirect <URL>
```

For example:

```
ProCurve(config)# aaa port-access mac-based unauth-redirect  
                    https://serverA.com:124/registration server/reg.html
```

### Unconfiguring a MAC-Auth Registration Server

Each configured registration server's URL must be removed by specifying it exactly, for example:

```
ProCurve(config)# no aaa port-access mac-based unauth-redirect  
                    https://serverA.com:124/registration server/reg.html
```

### Operating Notes

- If the configured URL contains a domain name (as opposed to an IP address) the switch's DNS resolver must be configured:
- `ProCurve(config)# ip dns server-address priority 1 <ipv4-address>`
- The NAT does an IP route lookup before it sends the packet to the destination registration server. A VLAN must have been configured that allows the switch to access the registration server.
- The initial page, redirect server, and filter path configuration will be per-switch.

- **Enhancement (PR\_000008243)** — Support is added for an eavesdrop prevention option.

## Optional Eavesdrop Prevention

### Overview

Traffic with an unknown destination address is blocked when port security is configured and Eavesdrop Prevention is enabled. Eavesdrop Prevention is enable by default and could not be disabled.

This enhancement provides the ability to disable Eavesdrop Prevention on ports where it may cause problems, such as on ports that are configured to use limited-continuous learning mode.

## Feature Interactions

The following table explains the various interactions between learning modes and Eavesdrop Prevention when Eavesdrop Prevention is disabled.

---

### Note

When the learning mode is “port-access”, Eavesdrop Prevention will not be applied to the port. However, it can still be configured or disabled for the port.

---

Learn Mode	Effect
Static	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured and only a limited number of static MAC addresses are learned. A device <i>must</i> generate traffic before the MAC address is learned and traffic is forwarded to it.
Continuous	The default. The Eavesdrop Prevention option does not apply because port security is disabled. Ports forward traffic with unknown destination addresses normally.
Port-access	Disabling Eavesdrop Prevention is not applied to the port. There is no change.
Limited-continuous	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured; MAC addresses age normally. Eavesdrop Prevention may cause difficulties in learning MAC addresses (as with static MAC addresses) and cause serious traffic issues when a MAC ages out.
Configured	When Eavesdrop Prevention is disabled, the port transmits packets that have unknown destination addresses. The port is secured by a static MAC address. Eavesdrop Prevention should not cause any issues because all valid MAC addresses have been configured.

---

**Syntax** [no] port-security <port-list> eavesdrop-prevention

*When this option is enabled, the port is prevented from transmitting packets that have unknown destination addresses. Only devices attached to the port receive packets intended for them. This option does not apply to a learning mode of **port-access** or **continuous**.*

*Default: Enabled*

```

ProCurve(config)# show port-security

Port Security

Port  Learn Mode          Eavesdrop
-----+-----
A1   Continuous          Enabled
A2   Continuous          Disabled
A3   Continuous          Enabled
A4   Continuous          Disabled
A5   Continuous          Enabled
A6   Continuous          Enabled
A7   Continuous          Disabled
A8   Continuous          Disabled
A9   Continuous          Enabled

```

**Figure 8. Example of show port-security Command Displaying Eavesdrop Prevention**

### MIB Support

The following MIB support is provided for Eavesdrop Prevention.

```

hpSecPtPreventEavesdrop OBJECT-TYPE
    SYNTAX      INTEGER {
        enable (1),
        disable (2)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "If enabled on a switch, outbound unknown unicast
        packets will not be forwarded out this port. If
        enabled on a repeater, outbound unknown unicast
        packets for this port will be scrambled."
    ::= { hpSecurePortEntry 5 }

```

- **Enhancement (PR\_0000013992)** — The ability to disable 5V power to the USB port is added.

### USB Port Config via CLI and SNMP

#### CLI Implementation

This feature allows configuration of the USB port with either the CLI or SNMP.

To enable/disable the USB port with the CLI:

**Syntax:** usb-port  
no usb-port

*Enables the USB port. The **no** form of the command disables the USB port and any access to the device.*

To display the status of the USB port:

**Syntax:** show usb-port

*Displays the status of the USB port. It can be enabled, disabled, or not present.*

```
ProCurve(config)# show usb-port
USB port status: enabled
USB port power status: power on      (USB device detected in port)
USB port reseal status: USB reseal not required
```

**Figure 9. Example of show usb-port Command Output on version K.13.59 and later**

```
ProCurve(config)# show usb-port
USB port status: enabled
USB port power status: power on      (USB device detected in port)
```

**Figure 10. Example of show usb-port Command Output on version K.14.XX**

One of the following messages indicates the presence or absence of the USB device:

- Not able to sense device in USB port
- USB device detected in port
- no USB device detected in port

The reseal status messages can be one of the following (K.13.XX only):

- undetermined USB reseal requirement
- USB reseal not required
- USB device reseal required for USB autorun

The autorun feature only works when a USB device is inserted and the USB port is enabled.

## **Behavior of Autorun When USB Port is Disabled**

### **Software Versions K.13.XX Operation**

When using software version K.13.58, if the USB port is disabled (no usb-port command), the USB autorun function does not work in the USB port until the USB port is enabled, the config file is saved, and the switch is rebooted. The 5 volt power to the USB port remains on even after the USB port has been disabled.

For software versions after K.13.58, the 5 volt power applied to the USB port is synchronized with the enabling of the USB port, that is, when the USB port is enabled, the 5 volts are supplied; when the USB port is disabled, the 5 volts are not supplied. For previous software versions the power was supplied continuously. The autorun function does not require a switch reboot, but the USB device must be inserted at least once after the port is enabled so that the switch recognizes that the device is present. If the USB device is inserted and then the USB port is enabled, the switch does not recognize that a USB device is present.

### **Software Version K.14.XX Operation**

For software versions K.14.XX, the USB port can be disabled and enabled without affecting the autorun feature. When the USB port is enabled, the autorun feature activates if a USB device is already inserted in the USB port.

Power is synchronized with the enabling and disabling of USB ports as described above for K.13.59 and later K.13.XX software versions, and K.14.31 and later K.14.XX software versions.

## **SNMP Implementation**

The HP enterprise MIB hpicfUSBPort.mib allows configuration of the USB port with SNMP.

```
HP-ICF-USBPORT DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY
```

```
    FROM SNMPv2-SMI
```

```
    NOTIFICATION-GROUP, OBJECT-GROUP, MODULE-COMPLIANCE
```

```
    FROM SNMPv2-CONF
```

```
    hpSwitch
```

```
    FROM HP-ICF-OID;
```

```
hpicfUSBPortMIB MODULE-IDENTITY
```

```
    LAST-UPDATED "200812180000Z"
```

```
    ORGANIZATION "Hewlett-Packard Company,
```

```
        Workgroup Networks Division"
```

**Enhancements**  
Release K.14.31 Enhancements

CONTACT-INFO "Hewlett Packard Company  
8000 Foothills Blvd.  
Roseville, CA 95747"  
DESCRIPTION "This MIB module manages the USB Port."

--  
-- Revision History  
--

REVISION "200812180000Z" -- December 18, 2008  
DESCRIPTION "Add hpicfUSBPortZeroPowerStatus object "

REVISION "200809170000Z" -- September 17, 2008  
DESCRIPTION "Move NOTIFICATIONS OID from 3 to 0"

REVISION "200809100000Z" -- September 10, 2008  
DESCRIPTION "Added NOTIFICATIONS for enabled/disabled"

REVISION "200806250000Z" -- June 25, 2008  
DESCRIPTION "Original version"

::= { hpSwitch 53 }

-- USBPort Configuration

hpicfUSBPortConfig OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 1 }

hpicfUSBPortStatus OBJECT-TYPE

SYNTAX INTEGER {  
notPresent(0),  
enabled(1),  
disabled(2) }

MAX-ACCESS read-write

STATUS current

DESCRIPTION "hpicfUSBPortStatus control whether or not  
the USB port is enabled.  
notPresent(0) - USBPort is not present

```
        enabled(1) - USBPort Enabled.
        disabled(2) - USBPort Disabled.
    "
DEFVAL { enabled }
::= { hpicfUSBPortConfig 1 }

hpicfUSBPortZeroPowerStatus OBJECT-TYPE
SYNTAX  INTEGER {
    powerUnavailable(0),
    powerOff(1),
    powerOn(2) }

MAX-ACCESS read-only
STATUS    current
DESCRIPTION "hpicfUSBPortZeroPowerStatus indicates if
    the USB port zero power is on or off.
    powerUnavailable(0) - USBPort power reading is
        unavailable.
    powerOff(1) - USBPort power is off.
    powerOn(2) - USBPort power is on.
    "
DEFVAL { powerOn }
::= { hpicfUSBPortConfig 2 }

-- Notifications
hpicfUSBPortNotifications OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 0 }

hpicfUSBPortEnabled NOTIFICATION-TYPE
STATUS    current
DESCRIPTION
    "An hpicfUSBPortEnabled notification signifies that the
    SNMP entity, acting in an agent role, has detected that
    the hpicfUSBPortStatus object has transitioned into the
    'enabled' state."
::= { hpicfUSBPortNotifications 1 }

hpicfUSBPortDisabled NOTIFICATION-TYPE
STATUS    current
```

DESCRIPTION

"An hpicfUSBPortDisabled notification signifies that the SNMP entity, acting in an agent role, has detected that the hpicfUSBPortStatus object has transitioned into the 'disabled' state."

::= { hpicfUSBPortNotifications 2 }

-- USBPort conformance information

hpicfUSBPortConformance

OBJECT IDENTIFIER ::= { hpicfUSBPortMIB 2 }

hpicfUSBPortGroups

OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 1 }

hpicfUSBPortBaseGroup OBJECT-GROUP

OBJECTS {  
    hpicfUSBPortStatus,  
    hpicfUSBPortZeroPowerStatus  
}

STATUS current

DESCRIPTION "A mandatory group with an object to enable or disable the USB port."

::= { hpicfUSBPortGroups 1 }

hpicfUSBPortNotificationGroup NOTIFICATION-GROUP

NOTIFICATIONS {  
    hpicfUSBPortEnabled,  
    hpicfUSBPortDisabled  
}

STATUS current

DESCRIPTION "The hpicfUSBPort MIB Notification Group."

::= { hpicfUSBPortGroups 2 }

-- USBPort conformance statements

hpicfUSBPortCompliances

OBJECT IDENTIFIER ::= { hpicfUSBPortConformance 2 }

```
hpicfUSBPortCompliance MODULE-COMPLIANCE
STATUS    current
DESCRIPTION "Compliance statement for HP ICF USBPort
            configuration"
MODULE
  MANDATORY-GROUPS { hpicfUSBPortBaseGroup,
                    hpicfUSBPortNotificationGroup }
  ::= { hpicfUSBPortCompliances 1 }

END
```

- **Enhancement (PR\_0000016100)** — A Global MAC Auth Password is now supported.

## MAC Authentication Global Password

MAC authentication only requires that an entry is placed in the user database with the device's MAC address as both the username and the password, creating the opportunity for malicious device spoofing using the readily available MAC address. To make spoofing more difficult, the global password option allows a network administrator to configure a common MAC authentication password that is used for all MAC authentications sent to the RADIUS server.

### Configuring the Global MAC Authentication Password

When implementing the global MAC authentication password option, it is important that the user database on the RADIUS server has the MAC authentication password as the password for each device performing MAC authentication.

Use this command to configure the global MAC authentication password.

**Syntax:** [no] aaa port-access mac-based password <password-value>

*Specifies the global password to be used by all MAC authenticating devices.*

*The **no** form of the command disables the feature.*

```
ProCurve(config)# aaa port-access mac-based password secretMAC1

ProCurve(config)# show port-access mac-based config

Port Access MAC-Based Configuration

MAC Address Format : no-delimiter
Password           : secretMAC1

Unauth Redirect Configuration URL :

Unauth Redirect Client Timeout (sec) : 1800
Unauth Redirect Restrictive Filter : Disabled
Total Unauth Redirect Client Count : 0
```

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-Auth Period	Unauth VLAN ID	Auth VLAN ID	Cntrl Dir
1	No	1	No	300	0	0	0	both
2	No	1	No	300	0	0	0	both
3	No	1	No	300	0	0	0	both
4	No	1	No	300	0	0	0	both
5	No	1	No	300	0	0	0	both
6	No	1	No	300	0	0	0	both
7	No	1	No	300	0	0	0	both
8	No	1	No	300	0	0	0	both

**Figure 11. Example of Configuring a Global MAC Authentication Password**

---

**Note**

The password value will display in an exported config file when **include-credentials** is enabled.

---

- **Enhancement (PR\_0000040203)** — Support is added for the HP ProCurve 3500-24 (J9470A), 3500-24-PoE (J9471A), 3500-48 (J9472A), and 3500-48-PoE (J9473A) Switches.

## Release K.14.32 Enhancements

- **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 K.14.33 Enhancements

*No enhancements, software fixes only.*

## 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.

The first production software release for the 6600-24 switches is K.14.03. The first production software release for the 6600-48 switches is K.14.24.

### Release K.14.03

The following enhancements, present in K.13.40 and newer K.13 versions, are NOT present in K.14.03:

**Enhancement (PR\_0000003127)** — Link Trap and LACP Global Enable/Disable.

**Enhancement (PR\_0000003128)** — The ability to clear statistics was added.

**Enhancement (PR\_0000003718)** — The MAC Lockout limit was increased to 64.

**Enhancement (PR\_0000007388)** — The ability to configure logging via SNMP was added.

The following enhancement, present in K.13.43 and newer K.13 versions, is NOT present in K.14.03:

**Enhancement (PR\_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added.

The following enhancements, present in K.13.51 and newer K.13 versions, are NOT present in K.14.03.

**Enhancement (PR\_0000003144)** — Support was added for multiple RADIUS groups.

**Enhancement (PR\_0000003141)** — Support was added for SSH Secure to RADIUS authentication.

**Enhancement (PR\_0000000083)** — Support was added for a MAC-Auth failure HTTP Redirect option.

The following enhancements, present in K.13.52 and newer K.13 versions, are NOT present in K.14.03.

**Enhancement (PR\_0000013786)** — Support was added for source IP identification.

**Enhancement (PR\_0000008243)** — Support was added for an eavesdrop prevention option.

The following problems were resolved in release K.14.03.

- **Self Test (PR\_0000009650)** — In some cases, when a bank of ports fails on the yl switches, the failure status is not appropriately recognized and reported in the switch's event log.

- **CLI (PR\_000009868)** — Execution of a **show** command in one Telnet or console session prevents successful execution of a **show** command in a concurrent management (CLI) session.
- **TELNET (PR\_000008234)** — When a user Telnets from one switch's CLI to a second switch's CLI, and then logs out from the session on the second switch, the CLI message, "telnet connection reset by peer," is inappropriately displayed.
- **Console (PR\_000008235)** — The CLI command **console local-terminal** should affect only the session in which the command is issued, but instead it is persistent for any subsequent connections that use the same session number.
- **Crash (PR\_0000010915)** — Deletion of a VLAN or creation of a trunk group from the CLI during a Telnet session from another switch may cause an unexpected reboot with a message similar to one of the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x088bf120 HW Addr=0xc3d2e1f0 IP=0x008631c0  
Task='mSnpCtrl' Task ID =0x88bf6a0 fp: 0xc3d2e1f0  
  
Software exception at iputil_integrity.c:3054  
-- in 'mIpCtrl', task ID = 0x1a4a0640
```

- **Crash Messaging (PR\_0000015799)** — Important data may be truncated from the crash message.
  - **Crash (PR\_0000015286)** — A switch configured for routing and PIM-SM may reboot unexpectedly due to depletion of the message buffer. The switch would then report a message similar to the following.
- ```
Software exception at alloc_free.c:439 -- in 'mIpCtrl', task ID =  
0xa96da80 -> No msg buffer
```
- **IGMP (PR\_0000014293)** — When forced fast leave (FFL) is in use, a GMP leave sometimes terminates the stream before the appropriate timeout. Additionally, the FFL timeout value configured is not honored.
  - **Logging (PR\_0000003908)** — PIM errors may be inadequate for problem isolation and troubleshooting. This fix enhances the PIM error messages with more descriptive information.
  - **PIM-SM (PR\_0000011001)** — A Designated Router (DR) is a router directly connected to a multicast source in a PIM-SM domain. The DR notifies the Rendezvous Point (RP) of the attached multicast sources. In some cases, the DR does not notify the RP of a source, causing the multicast stream to become unavailable.

- **PIM-SM (PR\_0000011070)** — The Designated Router (DR) may not transition appropriately from a Rendezvous Point Tree (RPT) or shared tree to a Shortest Path Tree (SPT), even when the source-specific SPT had the preferred route in the unicast routing table.

## Software Fixes

Release K.14.04 through K.14.08

- **PIM-SM (PR\_0000010035)** — When a routing update is given to PIM as part of a group of several updates, only the first route is updated and the switch does not properly handle subsequent unicast routing changes.
- **PIM-SM (PR\_0000011801)** — PIM-SM fails to appropriately switch back to the Rendezvous Point Tree when there is a device failure on the Shortest Path Tree.
- **PIM-SM (PR\_0000004569)** — Configuration of **ip pim-sparse hello-interval** does not take affect until the switch is rebooted.
- **PIM-SM (PR\_0000013537)** — PIM-SM is not correctly forwarding some fragmented tunneled packets, which is causing multicast traffic to be dropped.
- **PIM-SM (PR\_0000006729)** — One or more of the following symptoms may occur.
  - There may be multicast stream failure from the Designated Router to the Rendezvous Point router.
  - A failure to move appropriately from Rendezvous Point Tree to Shortest Path Tree occurs, so that a less optimal route through the network is used.
  - A prune, immediately followed by a join, could be inappropriately sent.
  - The routing switch is not processing the last entry of a compound join.
  - Prunes or joins may intermittently be sent on the wrong interface.
  - In a many-to-many multicast topology, there may be stream failure on devices residing between the DR and the RP routers.
  - Joins may be incorrectly sent when all of the joins should have aged out.
  - Some receivers are not receiving a flow until the mroute table times out.
- **PIM-SM (PR\_0000011057)** — Per RFC4601, the Designated Router is supposed to send another Register message prior to expiration of the Register-Stop-Timer. This fix corrects the Register-Stop-Timer.

## Release K.14.04 through K.14.08

Software never built.

## Release K.14.09

The following problems were resolved in release K.14.09.

- **Enhancement (0000017065)** — Support was added for the HP ProCurve 6600 Switch Premium License (J9305A) features.

- **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'
```

- **IGMP (PR\_0000009415)** — The switch may intermittently fail to forward a multicast stream.
- **Port Communication (PR\_0000004568)** — An Intel NIC using the 82566DM chipset may send fragments to the switch which results in the loss of communication on that or another 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

Symptoms improve or resolve with updated NIC firmware/drivers, when they are available from the device manufacturer.

- **Flow Control (PR\_0000015824)** — Fiber links may not communicate changes in flow control status appropriately to the link partner.
- **Bandwidth Limiting (PR\_0000016255)** — The switch will not access a valid value of 0 (zero) for the maximum ingress bandwidth on a port.
- **Configuration (PR\_0000017015)** — Configurations which utilize multiple switch features pushed to their maximum values may take an extended period to load, or cause an unexpected reboot with a message similar to the following.

```
NMI event HW:PC=0x10e8350c sp:0x12a8844c Suspects: eRouteCtrl[92]  
InetServer[6]
```

- **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.
- **Crash (PR\_0000017354)** — Disabling debug which had been previously logging to the switch buffer may cause the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at exception.c:621 -- in 'mDebugCtrl',  
task ID = 0x89ff620 -> Memory system error  
at 0x7c58450 - memPartFree
```

## Software Fixes

### Release K.14.10

- **CLI (PR\_0000014002)** — There are multiple problems with output from the CLI command `show ipv6 routers` which make the output either inaccurate or confusing.
- **Meshing (PR\_0000017406)** — A switch participating in meshing may run out of packet buffer space and stop communicating with the other switches in the network.
- **Spanning Tree (PR\_0000017820)** — Path costs are not appropriately updated after addition or removal of distributed trunks from the configuration.

## Release K.14.10

The following problems were resolved in release K.14.10. (Never released.)

- **Enhancement (PR\_0000011224)** — Support was added for chassis locator LED status with the CLI. For more information, see [“Release K.14.10 Enhancements” on page 16](#).
- **Enhancement (PR\_0000011601)** — Support was added for an increased number of LACP trunk groups. For more information, see [“Release K.14.10 Enhancements” on page 16](#).
- **Enhancement (PR\_0000010201)** — Support was added for SNMP client authentication. For more information, see [“Release K.14.10 Enhancements” on page 16](#).
- **Enhancement (PR\_0000013247)** — Support was added for the `show VLANs custom` CLI commands. For more information, see [“Release K.14.10 Enhancements” on page 16](#).

## Release K.14.11 through K.14.13

Versions K.14.11 through K.14.13 were never built.

## Release K.14.14

The following problems were resolved in release K.14.14. (Never released.)

- **Crash (PR\_0000015746)** — A very busy switch with a large configuration may experience multiple module resets, displaying event log messages similar to the following.

```
chassis: Slot A: Lost Communications detected - Heart Beat Lost(51)
chassis: Slot J: Msg loss detected - no ack for seq # 15803
chassis: Slot G: Msg loss detected - no ack for seq # 16654
chassis: Slot F: Msg loss detected - no ack for seq # 17472
chassis: Slot C: Msg loss detected - no ack for seq # 19015
chassis: Slot J: Lost Communications detected - Source Message
System(48)
chassis: Slot G: Lost Communications detected - Source Message
System(50)
```

```
chassis: Slot F: Lost Communications detected - Source Message  
System(55)
```

```
chassis: Slot C: Lost Communications detected - Source Message  
System(4B)
```

- **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 K.14.15

The following problems were resolved in release K.14.15.

- **10-GbE (PR\_0000038110/0000038298)** — 10-GbE SFP+ transceivers may fail to form a stable link, and 10-GbE X2 transceivers may fail to initialize entirely or initialize only after a long delay.

## Release K.14.16 through K.14.19

Software never built.

## Release K.14.20 through K.14.23

Software never released.

## Release K.14.24

The following problems were resolved in release K.14.24.

- **OSPF ECMP (PR\_0000039060)** — ECMP does not route correctly to a /32 route when there are two or more paths to the destination.
- **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.
- **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.

- **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
```

- **10-GbE (PR\_0000038110)** — 10-GbE SFP+ transceivers may fail to form a stable link.
- **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 on an HP ProCurve 6600 Series Switch 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.
- **SNMP (PR\_0000039064)** — The SNMP index for the ports on the 6600-48G switches, referenced in the `hpicfOid.mib`, is not correct.
- **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'
```

## Release K.14.25

Software never built.

## Release K.14.26

The following problems were resolved in release K.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 the 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 K.14.27 through K.14.29

Software never built.

## Release K.14.30

Software never released.

## Release K.14.31

The following problems were resolved in release K.14.31.

- **Flow Control (PR\_0000038853)** — When flow control is enabled on the switch, execution of the **show int brief** CLI command reveals that flow control is not actually enabled on gigabit or dual-personality ports.
- **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.
- **OSPF (PR\_0000038751)** — A switch configured for OSPF on both a VLAN and a loopback interface will report the following in the event/debug log, due to improper treatment of the loopback address.

```
OSPF: invalid packet: Packet with same router id as ours (28)
```

- **Crash (PR\_0000039470)** — A very busy switch configured with jumbo frames, OSPF routing, DHCP-snooping, QoS priority assignment, and Web-based authentication may reboot unexpectedly with a software exception. The crash message may vary.

## Software Fixes

### Release K.14.32

- **Virus Throttling/IGMP (PR\_0000040124)** — When a switch is configured for IP IGMP and Virus Throttling (connection-rate filtering), if the rate of joins sent by a host triggers a "block" by the Virus Throttling, the following software exceptions are seen in the switch event log. No other symptoms have been observed except the lines in the log. Multicast traffic still goes through. The port is not blocked as expected.

```
00805 connfilt: Unable to block 124.2.0.211 in hardware, <port>
sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID =
0xa977e40'
sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPkt-
Recv', task ID = 0xa977e40'
00805 connfilt: Unable to block 124.2.0.210 in hardware, <port>
sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID =
0xa977e40'
sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPkt-
Recv', task ID = 0xa977e40'
00805 connfilt: Unable to block 124.2.0.212 in hardware, <port>
sys: 'Software exception at vt.c:1065 -- in 'mIpPktRecv', task ID =
0xa977e40'
sys: 'Software exception at aqTcamInterface.c:829 -- in 'mIpPkt-
Recv', task ID = 0xa977e40'
```

## Release K.14.32

The following problems were resolved in release K.14.32.

- **Port Communication (PR\_0000018161)** — On some driver/firmware revisions, the Intel 82566DM and 82566DM-2 gigabit NIC chipsets may send an excessive number of corrupt packets. This traffic may affect communication on the port attached to the problem NIC, or on another port on the same module or port-bank. This fix helps to ensure continued communication by downgrading the port setting to auto-10/100, and logging an FFI message in the event log. The event log message will be similar to the following, and will indicate the port that is receiving the problem traffic. Please check with your PC vendor to see if there is an updated firmware version available for the affected NIC.

```
02671 FFI: Port <number> has been downgraded to 10/100.
See www.procurve.com/device\_help/nic\_update for details.
```

- **Authentication (PR\_0000011138)** — If the Radius server becomes unavailable, the **eap-radius authorized** option allows the switch to authenticate devices. If the response time of the RADIUS subsystem is greater than the server-timeout value on the switch or the device supplicant then the 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.
```

- **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.
- **Port Communication (PR\_0000017032/0000037992)** — Invalid/corrupt packets sent to the switch by a NIC operating at gigabit speed may trigger a loss of communication on a different port that shares the same ASIC. In that case, the port will retain its link and the Rx bytes, ifInDiscards, and the Discard Rx counters increment. Prior to this fix, communication on the port could only be reliably recovered by switch reload. This problem may also be associated with the following event log messages.

```
00374 chassis: Slot <x> Slave ROM Tombstone: 0x13000601
00374 chassis: Slot <x>: Lost Communications detected - Heart Beat
Lost
```

- **FFI/Config (PR\_0000039989)**
  - **FFI** - 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.
  - **Config** - Configuration changes made for PR\_0000018161 (see page 69) are not visible to the user; it appears that a port configured at both the NIC and the switch for auto-gig is operating at 100FDx for no reason (particularly if the associated event log message has scrolled out of the switch log). This fix makes the downgrade of the port to auto-10/100 visible in the running configuration. Note that this may trigger the switch to ask "Do you want to save current configuration?" upon logout or switch reload.
- **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.
- **VRRP (PR\_0000016626)** — VRRP may show failovers or near failovers without any apparent reason.
- **Port Communication (PR\_0000039476)** — Ports on zl switches configured for 10/100 may get into a state where connectivity is compromised. The network icon in the PC system tray shows limited or no connectivity. The PC does not get a DHCP address, and the switch Rx counters do not increment. If the PC is moved to another port the client PC comes up. The switch port is recoverable by configuring it down to 10-Mb operation, then back to 10/100.
- **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 message does not match the FFI log message for PR\_0000018161 on page [69](#).

## Release K.14.33

The following problems were resolved in release K.14.33.

- **Web Authentication (PR\_0000041695)** — Web authentication for port-access does not function on software version K.14.32.

- **CLI (PR\_0000038243)**— When task-monitor is enabled, the CLI output from the command **show cpu** is inconsistent with the sub-task averages, and higher than it should be. This behavior does not change after disabling task-monitor.



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

June 2009  
Manual Part Number  
5992-6005