



Release Notes:

Version K.15.03.0007 Software

for the HP Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches

These release notes include information on the following:

- K.15.03.0007 is supported on the following switches

HP ProCurve Switch 3500-24 (J9470A)
HP ProCurve Switch 3500-24-PoE (J9471A)
HP ProCurve Switch 3500-48 (J9472A)
HP ProCurve Switch 3500-48-PoE (J9473A)
HP ProCurve Switch 3500yl-24G-PWR Intelligent Edge (J8692A)
HP ProCurve Switch 3500yl-48G-PWR Intelligent Edge (J8693A)
HP ProCurve 3500yl-24G-PoE+ Switch (J9310A)
HP ProCurve 3500yl-48G-PoE+ Switch (J9311A)
HP ProCurve Switch 5406zl Intelligent Edge (J8697A)
E5406 zl Switch with Premium SW (J9642A)
HP ProCurve Switch 5412zl Intelligent Edge (J8698A)
E5412 zl Switch with Premium SW (J9643A)
HP ProCurve Switch 5406zl-48G Intelligent Edge (J8699A)
HP ProCurve Switch 5412zl-96G Intelligent Edge (J8700A)
HP ProCurve 5406zl-48G-PoE+ Switch (J9447A)
HP ProCurve 5412zl-96G-PoE+ Switch (J9448A)
HP ProCurve Switch 6200yl-24G-mGBIC (J8992A)
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)
HP ProCurve Switch 8206zl (J9475A)
E8206 v2 zl Switch with Premium SW (J9640A)
HP ProCurve Switch 8212zl (J8715A, J8715B)
E8212 v2 zl Switch with Premium SW (J9641A)

- Downloading switch software and documentation from the Web ([page 2](#))
- Best practices for software updates with major feature changes, including contingency procedures for rolling back to previous software versions and configurations. **Please read before updating software versions.** ([page 6](#)).
- Required BootROM updates ([page 16](#))
- Clarifications for selected software features ([page 20](#))
- Support Notes and Known Issues ([page 26](#))
- A listing of software enhancements ([page 28](#))
- A listing of software fixes ([page 94](#))

Manual Part Number

5998-1186
February 2011

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.

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.

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

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

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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

Warranty

See the *Software End User License Agreement and Hardware Limited Warranty* booklet, available through www.hp.com/networking/support.

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

Software Management

Premium License for Selected Switch Features	1
General Procedure	1
Download Switch Documentation and Software from the Web	2
Viewing or Downloading the Software Manual Set	2
Downloading Software Updates for Your Switch	3
TFTP Download from a Server	3
Xmodem Download From a PC or Unix Workstation	4
Using USB to Download Switch Software	4
Saving Configurations While Using the CLI	5
Important: Best Practices for Software Updates	6
Updating the Switch: Overview	6
Updating the Switch: Detailed Steps	7
Rolling Back Switch Software	9
Viewing or Transferring Alternate Configuration Files	11
HP Switch, Routing Switch, and Router Products Software Keys	12
Operating System and Web Browser Compatibility Table	13
Minimum Software Versions	14
ROM Updates Required!	16

Support Notes

What's New	17
Summary of New Features	17
Additional Features	18

Clarifications

HP Security Policy and Release Notes	20
Version K.15.01.0031 Clarifications	20
Delays During Configuration Changes to Physical Ports	20
Nonstop Switching (5400zl and 8200zl Switches)	20
Password Length and Special Character Issues	21
IPv4 Loopback Address Not Required for IPv6 Address Configuration	22
Version K.15.02.0004 Clarifications	22
Rate-Limiting on the Entire Packet	22
Change to Default Setting for Detecting and Powering Pre-802.3af Devices	23
Compatibility Mode for v2 zl and zl Modules	23
Authorized IP Managers Precedence	24
Minimum Guaranteed Bandwidth Issue	24
Version K.15.03.0005 Clarification	25
Loss of Event Log on Upgrade/Downgrade	25

Known Issues

Version K.15.01.0031	26
Version K.15.02.0004	26
Version K.15.03.0005	27

Enhancements

Version K.15.01.0031 Enhancements	28
Flapping Transceiver Mitigation	28
Module Reload (5400zl and 8200zl switches)	30
Version K.15.01.0032 Enhancements	32
Username and Password Size Increase	32
Version K.15.02.0004 Enhancements	33
Multicast ARP Support	33
Display Configuration of Selected Interface	34
Post-logon Banner Enhancement	40
Support for the Tilde (~) Character in TACACS+ and RADIUS Keys	42
Web Auth Deny Message	45
Port Security Per-Port MAC Increase	49
PoE with LLDP	49
Increase MAC Auth Client Limit to 256	52
Categorize CLI Return Messages	53
Energy Efficient Ethernet (EEE)	56
Version K.15.03.0003 Enhancements	60
Custom Default Configuration	60
SNMP Trap Upon Port Addition or Deletion of MAC Addresses	66
Log Message When Startup Config Updated	69
Show MAC with VLAN	70
Outbound Queue Monitor	71
Show OSPF Neighbor Timers	72
IP Enable/Disable for All VLANs	73
Logging for Routing ACLs	74
Trunk Load Balancing Using L4 Ports	79
Wake-on-LAN Support Across VLANs	81
Syslog via TCP	85
SNMP Trap on Running Configuration Changes	86
Static Summary Route to RIP	89
Dynamic Port Access Auth via RADIUS	90

Software Fixes

Version K.15.01.0031	94
Version K.15.01.0032	102
Version K.15.01.0033	102
Version K.15.02.0004	103
Version K.15.02.0005	107

Version K.15.03.0003 107

Version K.15.03.0004 110

Version K.15.03.0005 110

Version K.15.03.0006 110

Version K.15.03.0007 110

Software Management

Premium License for Selected Switch Features

Switch software licensing enables advanced features in selected HP switches. For software version K.15.01.0031 and later, the following table shows the software licenses available for supported switches:

License Type	Premium* Supports advanced routing features, including: <ul style="list-style-type: none"> – OSPF v2, OSPF v3 – PIM – sparse mode, PIM – dense mode – VRRP – QinQ (IEEE 802.1ad) 			
Switch Family	3500 and 3500yl	5400zl	6600	8200zl
License Product	J8993A	J8994A	J9305A	J9474A
* Notes: <ul style="list-style-type: none"> • Legacy HP ProCurve 8212zl switch (J8715A) included advanced features, a Premium License upgrade is not required. • HP ProCurve 6200yl switch included advanced features, a Premium License upgrade is not required. • A previously installed license can be removed from a switch and transferred to another switch within the same product series. 				

For more information on features enabled through a Premium License, see the data sheets and software documentation for your switch.

Each Premium License product provides license-to-use for a single switch. To install a license, see the documentation provided with the license product. For an overview, see [“General Procedure”](#) below.

Note	When updating to software version K.15.01.0031 or later, a Premium License upgrade is not required for supported switches that already contain a premium license.
-------------	---

General Procedure

The general procedure for installing a software license involves several different numbers:

- **registration ID** — This number comes with the license you purchase, and represents your right to install the particular type of license on a particular type of switch.
- **hardware ID** — This number is provided by the switch that you are licensing, and includes the switch’s serial number and an identifier for the feature that you are licensing.
- **license key** — This number is generated by the My ProCurve portal, based on the registration ID and the hardware ID that you provide. When you install this number into the switch, it enables the feature that you are licensing.

The procedure for installing a licensed feature into a switch is:

1. **Locate the registration ID.** When you purchase a software license, you receive a folded license registration card. The registration ID is located on the inside of the card, typically in the upper left corner.
2. **Get the switch’s hardware ID.** Establish a console connection to the switch CLI and enter Manager level, using the **enable** command if necessary and the switch password if required. For example:

Software Management

Download Switch Documentation and Software from the Web

```
ProCurve> enable
ProCurve#
```

From the Manager level, issue the **licenses hardware-id <license_type>** command. For example:

```
ProCurve# licenses hardware-id premium
```

The CLI returns a hardware ID number. Copy the hardware ID number from the screen (using Ctrl-C) or write it down. (Copying the number is easier and more accurate.) You will enter the number on the My ProCurve portal in the next step.

3. **Get the license key.** Point your Web browser at the My ProCurve portal (<http://my.procurve.com>) and sign in. Click the My Licenses tab, enter the registration ID, and then enter the hardware ID. At the end of the procedure a license key is displayed. (It is also e-mailed to you.) Copy the license key from the screen (using Ctrl-C) or write it down.
4. **Enter the license key into the switch.** On the CLI console, save the configuration of the switch (**write memory**). Then, from a Manager-level prompt, issue a **licenses install premium <license-key>** command. (The license key number is not case sensitive.) For example:

```
ProCurve# licenses install premium AA000GG000-A-0123ABC-ABCD123-0A2B3C4-0123ABC
```

5. Reboot the switch. For example:

```
ProCurve# boot
or:
ProCurve# reload
```

The licensed features should now be active on the switch.

HP ProCurve Manager (PCM) or ProCurve Manager Plus can be used to simplify the process of adding licenses. Just provide the registration ID from the Premium License and use PCM to identify which switch to install the license. PCM will communicate with the My ProCurve Portal directly and add the license to the switch without user intervention.

Download Switch Documentation and Software from the Web

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

Viewing or Downloading the Software Manual Set

Go to: www.hp.com/networking/support

Downloading Software Updates for Your Switch

HP periodically provides switch software updates through the HP networking web site (www.hp.com/networking/support). 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 4).
- Use the USB port to download a software file from a USB flash drive (page 4).
- Use the download utility in ProCurve Manager Plus management software.

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, to archive 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_15_01_0031.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_15_01_0031.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 your switch *Installation and Getting Started Guide* for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with most Windows systems, the Send File option in the Transfer drop-down menu supports the Xmodem protocol.)

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. (A baud rate of 9600 bits per second is recommended for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)
5. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
6. Reboot the switch from the flash area 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_15_01_0031.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 networking support FAQ web pages, www.hp.com/go/procurve/faqs, and select FAQs for your switch.

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

For example, to download a software file named K_15_01_0031.swi from a USB flash drive:

1. Execute the copy command as shown below:

```
ProCurve # copy usb flash K_15_01_0031.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)
- 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 Yes) when you see the “save configuration” prompt:

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

Important: Best Practices for Software Updates

Note

With version K.15.01.0031 and later software, you will notice a slight change in the versioning system. For more information, see [“What’s New” on page 17](#).

Software updates that contain significant new features and enhancements may be designated by an increment to both the major and minor release version numbers. That is, K.15.01.0031 represents a major update to software version(s) K.14.xx, and K.14.xx represents a major update to K.13.xx, and so forth. In addition, a future version (such as K.15.02.xxxx) may represent a minor release to version K.15.01.xxxx, but may still contain significant changes. To mitigate against potential migration issues when performing such updates, this section documents best practices for updating the switch, including contingency procedures for rolling back to previous software versions and saved configurations.

Updating the Switch: Overview

Caution

Before you update the switch software to a new version:

- We strongly recommend that you save a copy of your config file to an external location.
- We advise against rolling back (going from a newer software version to an older software version) without copying a backup config file to the device.

If you do choose to downgrade software using your existing config file, unpredictable changes in the config file and switch behavior may occur. If booting a K.15.01.0031 or later config file into a K.14.xx or earlier versions of software, the following commands may be removed from your config file:

- Any commands that are present in K.15.01.0031 (or later) but are not present in earlier versions of software
 - logging
 - snmp-server
 - mirror-session
 - auto-tftp
 - filter source-port
 - fault-finder
 - interface loopback
-

To perform an update to your switch software, follow the steps below (see page 7 for detailed steps):

1. Download the image to your TFTP server.
2. Save your current configuration (Config1) to a backup configuration file (Config2).
3. Save your current configuration to an external tftp server.
4. Backup your current running image (Primary) to the secondary image.
5. Set your secondary image to boot with Config2.
6. Download the new image to the switch’s primary image.
7. Verify that your images and configuration are set correctly.
8. Reload the switch.

After following these steps, you should end up with the following results:

- Primary image will hold the new software image you want to install (for example, K.15.01.0031)
-

- Secondary image will hold the image you are currently running (for example, K.14.47)
- Primary image will boot with Config1 (config file corresponding to new software version—in this example, K.15.01.0031)
- Secondary image will boot with Config2* (config file corresponding to previous software version—in this example, K.14.47)

* The current config file must be copied to Config2, or you will be unable to revert if the need arises.

Note

You might opt to use a different methodology in which the new software will be installed as the secondary and not the primary image, in which case you would use the commands **boot system flash secondary**, and/or **boot set-default flash secondary** to change the location of the default boot. However, since you will still need to take precautions to allow you to revert to your previous configuration, We strongly recommend that you follow the methods that are proposed in our update process. This will ensure that you can use our proposed roll back procedures should the need arise.

Updating the Switch: Detailed Steps

The following detailed steps shows how to update the switch software from an existing version to a significant new version (in the example provided here, from version K.14.47 to version K.15.01.0031).

1. Download the latest software image to your TFTP server from the HP networking web site.:
www.hp.com/networking/support
2. Save your current configuration (Config1) to backup configuration file (Config2).
 - a. Before copying the config, verify the current state of your system using the **show version**, **show flash**, and **show config files** commands. For example:

```
Switch1# show version
Image stamp:      /sw/code/build/btm(t4a)
                  Nov  6 2009 13:20:26
                  K.14.47
                  188
Boot Image:       Primary

Switch1# show flash
Image             Size(Bytes)   Date   Version
-----
Primary Image    : 9839140      11/06/09 K.14.47
Secondary Image  : 0
Boot Rom Version: K.12.20
Default Boot     : Primary

Switch1# show config files

Configuration files:

id | act pri sec | name
---+-----+-----+-----
 1 | *   *   *   | config1
 2 |           |
 3 |           |
```

- b. Create a backup configuration file and verify the change.

```
Switch1# copy config config1 config config2
```

```
Switch1# show config files
```

```
Configuration files:
```

id	act	pri	sec	name
1	*	*	*	config1
2				config2
3				

3. Save the current config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60 Switch1_config_K_14_47.cfg
```

Note

This step is necessary because HP switches do not support roll back (going from a newer software version to an older software version) without the ability to copy a backup config file onto the device.

4. Backup your current running image (primary) to the secondary image.

```
Switch1# copy flash flash secondary
```

```
Switch1# show flash
```

```
Image                Size(Bytes)    Date    Version
-----
Primary Image       : 9839140    11/06/09 K.14.47
Secondary Image     : 9839140    11/06/09 K.14.47
Boot Rom Version: K.12.20
Default Boot       : Primary
```

5. Set your secondary image to boot with Config2.

```
Switch1# startup-default secondary config config2
```

```
Switch1# show config files
```

```
Configuration files:
```

id	act	pri	sec	name
1	*	*		config1
2			*	config2
3				

Note

Step 5 will enable you to revert from K.15.01.xxxx to your previous image with your previous configuration just by invoking the command **boot system flash secondary**.

6. Download the new primary image.

```
Switch1# copy tftp flash 192.168.1.60 K_15_01_0031.swi primary
```

```
The Primary OS Image will be deleted, continue [y/n]?
```

At the prompt, enter **y** for yes, and the new image will be downloaded and written to the File system. Once tftp download has been completed you will see the following message:

```
Validating and Writing System Software to the Filesystem ...
```

7. Verify that your images and configuration are set correctly. For example, if you updated from K.14.47 to K.15.01.0031, you should see the following outputs from the switch show commands:

```
Switch1# show version
Image stamp:      /sw/code/build/btm(t4a)
                  Nov  6 2009 13:20:26
                  K.14.47
                  188
Boot Image:       Primary
```

```
Switch1# show flash
Image             Size(Bytes)   Date   Version
-----
Primary Image    : 11537788     04/23/10 K.15.01.0031
Secondary Image  :  9839140     11/06/09 K.14.47
Boot Rom Version: K.15.09
Default Boot     : Primary
```

```
Switch1# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		config1
2			*	config2
3				

8. Reload the new switch image.

```
Switch1# reload
System will be rebooted from primary image. Do you want to continue [y/n]? y
```

At the prompt, enter **y**, for yes, and the switch will boot with the new image.

Note

As an additional step, we recommend saving the startup-config to a tftp server using the **copy tftp** command. For example:

```
Switch1# copy startup-config tftp 10.1.1.60 Switch1_config_K_15_01_0031.cfg
```

Rolling Back Switch Software

If you have followed the update procedures documented in the previous section, you should be able to revert to your previous configuration and software version using the steps below.

Caution

Long Usernames and Passwords. Software versions K.15.01.0032 and later support the longer usernames and passwords introduced in K.14.59.

Before downgrading to a software version that does not support long usernames and passwords, use one of the following procedures:

- Using the **password** CLI command or the Web browser interface, change usernames or passwords to be no more than 16 characters in length, and without any special characters. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear the values using the **no password all** CLI command. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear password values by using the "Clear" button on the switch. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

Note: The procedures above should be used only when downgrading from a software version that supports long usernames and passwords to a version that does not.

To roll back your switch from K.15.01.0031 to K.14.47, for example, follow the steps below:

1. Verify that your images and configuration are set correctly using the **show version**, **show flash**, and **show config files** commands.

```
Switch1# show version
Image stamp:      /sw/code/build/btm(t5a)
                  Apr 23 2010 05:43:42
                  K.15.01.0031
                  67
Boot Image:      Primary

Switch1# show flash
Image            Size(Bytes)   Date    Version
-----
Primary Image   : 11537788    04/23/10 K.15.01.0031
Secondary Image :  9839140    11/06/09 K.14.47
Boot Rom Version: K.15.09
Default Boot    : Primary
```

```
Switch1# show config files
```

Configuration files:

id	act	pri	sec	name
1	*	*		config1
2			*	config2
3				

2. Boot the switch using the secondary image (with config2).

```
Switch1# boot system flash secondary
System will be rebooted from secondary image. Do you want to continue [y/n]? y
```

Enter **y** for yes, and the switch will boot from the secondary image (K.14.47, in this example) with the corresponding configuration for that software version (Config2).

Viewing or Transferring Alternate Configuration Files

Viewing or copying an alternate configuration saved to the switch will always be accomplished through the software currently running on the switch. This may result in a misleading portrayal of the configuration. For example, if a configuration is created on K.14.47 and saved as config2, and if it is then viewed or transferred while the switch is running K.15.01.0031, it will appear as though K.15.01.0031 has converted the configuration. However, the alternate configuration file, config2, will still be intact on the switch and load properly when the switch is booted into the same software version from which the configuration file originated.

When an enhancement introduces a feature that did not previously exist in the switch, it may present several challenges to the user.

Backwards compatibility of the configuration created with a version of software that supports a new feature or parameter is not guaranteed. Software versions that did not recognize or support a particular command or parameter will not be able to interpret that line in the configuration. For this reason, it is strongly recommended that network administrators always save their configuration *while still running the switch with the original software version*, and with a notation indicating the software version on which the configuration was saved. For example, a user might save a configuration for a switch running K.14.47 to a TFTP server with an IP address of 10.10.10.15 as follows:

```
ProCurve5406zl-onK1447# copy running-config tftp 10.10.10.15 5406onK1447
```

If, for example, the user deems it necessary to revert to the use of K.14.47, the user can boot into it and then restore the saved config from the TFTP server.

Viewing or copying an alternate configuration that is saved to the switch flash can be accomplished only with the software that is currently running on the switch.

Here, for example, a configuration is created on K.14.47 and then saved to flash:

```
ProCurve5406zl-onK1447# copy config config2 config K1447config <cr>
```

And later, the configuration that was created on K.14.47 is viewed while the switch is running K.15.01.0031:

```
ProCurve5406zl-onK1501# show config K1447config <cr>
```

The command output will show how the K.14.47 config would be interpreted *if it were to be used by the K.15.01.0031 software*. Copying the K1447config file to a TFTP server would similarly trigger an interpretation by the software performing the file transfer. Note, however, that this does not actually *change* the configuration. If the version is rolled back from K.15.01.0031 to K.14.47 with a command like the following (given that K.14.47 is stored in secondary flash), the K.14.xx formatted config is still intact and valid.

```
ProCurve5406zl# boot system flash secondary config K1447config
```

This “interpretation” during a TFTP or **show** command execution is inherent in the architecture of the switch. When switch features change significantly (such as the move from IPv4 support to IPv6 support), there may be configuration parameters from the previous config that cannot be translated by the switch for viewing while it is running the new software. This necessitates storing configurations for each version of software to an external location, if the user would like to view the stored config prior to reloading it.

HP Switch, Routing Switch, and Router Products Software Keys

Software Letter	HP Networking Products
A	Switch 2615-8-PoE and Switch 2915-8G-PoE
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	J.xx.xx.biz Secure Router 7000dl Series (7102dl and 7203dl)
J	J.xx.xx.swi Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1810G (1810G-8, 1810G-24)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
S	Switch 2520 Series (2520-8-PoE, 2520-24-PoE)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WM	ProCurve Access Point 10ag
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	ProCurve 6120G/XG and 6120XG Blade Switches
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Operating System and Web Browser Compatibility Table

The switch Web agent supports the following combinations of OS browsers:

Operating System	Tested Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Vista SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2003 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2008 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows 7	Internet Explorer 8 Firefox 3.0, 3.5
MAC OS	Firefox 3.0, 3.5

Minimum Software Versions

For HP Series 3500, 3500yl, 5400zl, 6200yl, 6600 and 8200zl Switches and Hardware Features

HP Device ^{Note 1}	Product Number	Minimum Supported Software Version
HP ProCurve 3500yl-24G-PoE+ Switch	J9310A	K.15.02.0004
HP ProCurve 3500yl-48-PoE+ Switch	J9311A	K.15.02.0004
HP ProCurve 2-Port SFP+/2-Port CX4 10GbE yl Module	J9312A	K.15.02.0004
HP ProCurve 24-port 10/100/1000 PoE+ v2 zl Module	J9534A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	J9535A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module	J9536A	K.15.02.0004
HP ProCurve 24-port SFP v2 zl Module	J9537A	K.15.02.0004
HP ProCurve 8-port 10-GbE SFP+ v2 zl Module	J9538A	K.15.02.0004
HP 24-port 10/100 PoE+ v2 zl Module	J9547A	K.15.02.0004
HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	J9548A	K.15.02.0004
HP 20-port Gig-T / 4-port SFP v2 zl Module	J9549A	K.15.02.0004
HP 24-port Gig-T v2 zl Module	J9550A	K.15.02.0004
HP 12-port Gig-T / 12-port SFP v2 zl Module	J9637A	K.15.02.0004
HP ProCurve 8206zl Switch Base System	J9475A	K.14.34
HP ProCurve 24-Port 10/100/1000 PoE+ zl Module	J9307A	K.14.34
HP ProCurve 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module	J9308A	K.14.34
HP ProCurve 24-port 10/100 PoE+ zl Module	J9478A	K.14.34
HP ProCurve 5406zl-48G-PoE+ Switch	J9447A	K.14.34
HP ProCurve 5412zl-96G-PoE+ Switch	J9448A	K.14.34
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
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 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
HP ProCurve ONE Services zl Module	J9154A	K.13.51
HP ProCurve Wireless Edge Services zl Module and the HP ProCurve Redundant Wireless Services zl Module	J9051A and J9052A	K.12.43
Premium Features on Series 3500yl and 5400zl Switches	J8993A and J8994A	K.11.33

HP Device ^{Note 1}	Product Number	Minimum Supported Software Version
HP ProCurve Switch 5400zl 24p Mini-GBIC Module	J8706A	K.11.33
HP ProCurve Switch 5400zl 4p 10-GbE CX4 Module	J8708A	K.11.33
HP ProCurve Switch 6200yl-24G-mGBIC	J8992A	K.11.33
HP ProCurve Switch 3500yl 2p 10GbE X2 + 2p CX4 Module	J8694A	K.11.17
HP ProCurve Switch 8212zl Base System	J8715A and J8715B	K.12.31
<p>Note 1 For minimum software requirements for supported transceivers, visit www.hp.com/networking/support.</p> <ul style="list-style-type: none"> – In the first textbox, type J4858 (for 100-Mb and Gigabit information), or J8436 (for 10-Gigabit information). – Select any of the products that display in the dropdown list. – Select Product support information. Then click on Manuals and find the Transceiver Support Matrix. 		

ROM Updates Required!

BootROM updates are needed to be able to boot specified switch software versions. In most cases, selected software versions are used to automatically update the BootROM. Therefore, to successfully update to K.15 software, you may have to update software in multiple steps, depending on your current software and BootROM versions. Please use the steps in the table below.

If your software version is:	Your next step should be:
K.12.31 through K.13.55 (BootROM K.12.12 - 12.14)	Update and reload into software version K.13.58 or K.13.68
K.13.58 or newer (BootROM K.12.17 or newer; use show flash command)	Update directly into software version K.15.03.0007 (BootROM K.15.11)

Caution

When updating to interim software versions, refer to the Release Notes supplied with those versions and observe any precautions noted.

If your switch is running a software version earlier than K.15, your BootROM will be updated when you upload K.15 software to your switch. During the software update, the switch will automatically boot **twice**, first to update the BootROM to the proper version, and then to load the system software. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. **Do not interrupt power to the switch during this important update.**

To confirm that the BootROM and system software have updated successfully following a reload into software version K.15.01.0031 or later, follow the process below at your switch CLI.

```
ProCurve_Switch# show flash
```

```
Image           Size(Bytes)   Date    Version
-----
Primary Image   : 11537788   04/23/10 K.15.01.0031 <--Indicates that system software is updated
Secondary Image :  9839140   11/06/09 K.14.47
Boot Rom Version: K.15.09 <-- Indicates the BootROM is updated
Default Boot    : Primary
```

Support Notes

What's New

Summary of New Features

Starting with software version K.15.01.0031, some key new features are summarized below. To access or use these new features, see the software documentation for your switch.

New Features in K.15.01.0031 (or later)	Description:
Nonstop Switching for 8200zl series switches	Provides high-availability support for business-critical and real-time applications. <ul style="list-style-type: none"> Allows layer 2 switching to continue during Management Module switchover. Transition from the Active Management Module to the Standby Management Module is quick and seamless, and does not require a reboot. Both Management Modules support identical features and configuration files
IPv6 Layer 3 support	<ul style="list-style-type: none"> K.13 provided IPv6 foundation services: <ul style="list-style-type: none"> IPv6 Host Dual stack (IPv4/IPv6) MLD snooping K.14 provided additional security and control: <ul style="list-style-type: none"> IPv6 ACL IPv6 QoS K.15 provides Layer 3 support services: <ul style="list-style-type: none"> OSPFv3 Static routing DHCPv6 Relay Other features, including Port-based ACLs, Auto tftp, syslog, SSH Server, SNMP server (v1, v2, v3), SNTTP client, Web server, IP Auth Manager.
New Web Agent	The Web browser interface provides a new look and feel for simplified configuration. Java services and other client software are no longer needed.
Additional feature enhancements	<ul style="list-style-type: none"> VRRP enhancements, including: <ul style="list-style-type: none"> Simplified troubleshooting of VRRP configurations Physical IP is no longer identical with Virtual IP Route Maps enhancements for route management QoS and Mirroring Policies enhancements, allowing them to be applied dynamically show mesh, show class and show policy command enhancements
New software version designation	VVV.UU.BB.FFFaaaaa software code designations, where: <ul style="list-style-type: none"> VVV is a switch platform identifier (for example, 'K'). UU is a major version number (for example, "15"), to specify significant changes in features or functions. BB is a minor version number for versions that may include significant changes in features or functions, including support of new hardware or enhancements. If the major number is incremented, the minor version number will reset to '01'. FFF specifies a unique build number. It may be used to identify a specific bug-fix release that may, or may not, carry over to a subsequent build. aaaaa is a character string suffix to identify a type of build, for example, a special feature build (such as 'spcl') or a maintenance build (such as "m"). This is an optional string. Non-maintenance releases will not have a suffix.

Additional Features

Event Log Capacity

Beginning with Version K.15.01.0031 the capacity of the event log has been increased. In prior versions, the event log was stored as ASCII text strings on the switch; the maximum number of event log messages that could be stored was 2000 messages. With Version K.15.01.0031, the event log is now stored in a compressed form rather than ASCII text. Since compression can be variable, the new capacity of the event log will also be variable. Typically, the new capacity will be between 3,000 and 5,000 entries.

Due to the new method of storing the event log, event log entries created in K.15.01.0031 and later versions cannot be read by K.14.xx and earlier versions, and vice-versa. When booting from K.15.01.0031 (or later) into K.14.xx or earlier versions, the K.15 event log stored in memory will be erased. When booting from K.14.xx into K.15.01.0031 (or later), the K.14 event log stored in memory will also be erased.

Event Log for Nonstop Switching (5400zl and 8200zl Switches)

With the introduction of Nonstop Switching, both Active and Standby management modules can create event log entries. To identify the slot and status of the management module creating the entry, the following tags are now used:

- AM1 - Active Management Module in Slot 1
- AM2 - Active Management Module in Slot 2
- SM1 - Standby Management Module in Slot 1
- SM2 - Standby Management Module in Slot 2

Example:

```
ProCurve Switch 8212zl(config)# show log -r
Keys:   W=Warning   I=Information
        M=Major     D=Debug E=Error
---- Reverse event Log listing: Events Since Boot ----
I 03/16/10 18:03:29 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/15/10 15:34:00 00077 ports: AM1: port B1 is now off-line
I 03/15/10 15:34:00 00435 ports: AM1: port B1 is Blocked by STP
I 03/14/10 18:03:28 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/14/10 07:48:56 00077 ports: AM1: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: AM1: port B1 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: AM1: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: AM1: port B2 is Blocked by STP
```

By default, only log entries from the Active management module will be shown.

To see all management module entries use the "-s" option.

Example:

```
ProCurve Switch 8212zl(config)# show log -r -s
Keys:   W=Warning   I=Information
        M=Major     D=Debug E=Error
---- Reverse event Log listing: Events Since Boot ----
I 03/16/10 18:03:29 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subne t mask
I 03/15/10 15:34:00 00077 ports: SM2: port B1 is now off-line
I 03/15/10 15:34:00 00077 ports: AM1: port B1 is now off-line
I 03/15/10 15:34:00 00435 ports: SM2: port B1 is Blocked by STP
I 03/15/10 15:34:00 00435 ports: AM1: port B1 is Blocked by STP
I 03/14/10 18:03:28 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/14/10 07:48:55 00077 ports: SM2: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: SM2: port B1 is Blocked by STP
I 03/14/10 07:48:56 00077 ports: AM1: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: AM1: port B1 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: SM2: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: SM2: port B2 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: AM1: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: AM1: port B2 is Blocked by STP
```

Typically, the need to view both Active and Standby event messages would be limited (for example, troubleshooting a failover or a failure of the Standby module). Because the Standby module is in a "hot standby" mode, it still executes many of the same operations that the Active module does, which is why duplicate event log messages from the Standby module would be displayed.

Clarifications

HP Security Policy and Release Notes

Per HP policy, a Security Bulletin must be the first published notification of a security defect. Fixes to security defects are not documented in release notes, also by HP policy.

The official communication for security defect fixes will always be through HP Security Bulletins. For more information on security bulletins, and information on how to subscribe to them, please see http://www.procurve.com/docs/security/ProCurve_Finding_SecurityNote&Bulletins_US.pdf.

Visit the ProCurve Web site for more information on security and ProCurve products:
<http://www.procurve.com/customercare/support/security/index.aspx>.

Note	Version K.15.01.0031 is a major software release, and was developed from Version K.14.41. Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.
-------------	--

This section provides clarifications of software features starting with Version K.15.01.0031. For prior software versions, see the Release Notes provided with those versions.

Version K.15.01.0031 Clarifications

Delays During Configuration Changes to Physical Ports

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

Nonstop Switching (5400zl and 8200zl Switches)

For more information on Nonstop switching, see the “Chassis Redundancy” chapter in the *Management and Configuration Guide* for your switch.

Unsupported zl Modules

ZL modules/controllers that do not support the Nonstop switching feature include the following:

- HP ProCurve ONE Services zl Module (J9289A)
- HP ProCurve Threat Management Services zl Module (J9155A)
- HP ProCurve Threat Management Services zl Module with 1-year IDS/IPS subscription (J9156A)
- HP ProCurve Wireless Edge Services zl Module (J9051A) and Redundant Wireless Services zl Module (J9052A)

■ HP ProCurve MSM765zl Mobility Controller (J9370A)

During a Nonstop switching failover, unsupported modules will not failover seamlessly to the Standby module. A Nonstop switching failover will cause a forced reboot on these modules. After rebooting, these modules will then sync with the newly active management module and begin operation again. Module traffic will be disconnected until the module completes the reboot process.

Hot Swapping of Management Modules

Use the shutdown button on the front of the management module before removal. The shutdown button ensures that the management module will be shutdown properly. If Nonstop Switching is enabled, using the shutdown button prior to removal will ensure failover to the Standby module will be successful.

Rapid Routing Switchover and Stale Timer

With K.15.01.0031, Nonstop switching only supports Layer 2 functions on the switch. During a failover, traffic routed through the switch at Layer 3 will see an interruption. When a failover from Active to Standby occurs, the routing table is "frozen". All routes that existed at the time of the failover are marked as "stale". While dynamic routing protocols running at the time may act as if the routing protocol has been restarted and rebuilds the table, the switch on which the failover occurred will continue to rout traffic using the 'stale routes'.

The "Stale timer" begins counting when the switchover occurs. When the "Stale timer" expires, any routes that are still marked as stale are purged from the routing table. Due to the nature of Rapid Routing switchover, if there are multiple simultaneous failures, network loops could occur or traffic could flow through unpredictable paths.

Caution should be taken if setting the "rapid-switchover" timer higher than the default. To disable "Rapid Routing Switchover" and to ensure that all routing is based on the most current routing protocol information, set the "rapid-switchover" timer to 0.

Password Length and Special Character Issues

K.15.01.0031 does not support the longer usernames and passwords introduced in K.14.59. Use caution when upgrading or downgrading between software versions that do not support these features.

Before downgrading to a software version that does not include this feature, use one of the following procedures:

- Using the **password** CLI command or the Web browser interface, change usernames or passwords to be no more than 16 characters in length, and without any special characters. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear the values using the **no password all** CLI command. This clears all the passwords. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear password values by using the "Clear" button on the switch. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

Note

These procedures should be used only when downgrading from a software version that supports long usernames and passwords to a version that does not.

If a switch with long usernames/passwords is inadvertently booted into K.15.01.0031, you will not be able to gain access to the switch. To regain access to the switch:

1. Get access to the serial console on the switch.
2. Reboot the switch.
3. Interrupt the boot process when you see the following text:

Boot Profiles:

0. Monitor ROM Console
1. Primary Software Image
2. Secondary Software Image

Select profile (secondary):

4. Boot the software image that does support long usernames and passwords. For example, if your Primary image is K.15.01.0031 installed and your Secondary image is K.14.xx, boot your Secondary image.
5. After the switch is booted, perform one of the three procedures described above.

Caution

If you inadvertently booted into K.15.01.0031 with a long username/password, **do not** attempt to change the password or clear the password while running K.15.01.0031 software. Attempting to do so may corrupt the switch configuration and cause the switch to be inaccessible, resulting in a service call.

IPv4 Loopback Address Not Required for IPv6 Address Configuration

On K.14.xx software, an IPv4 loopback address was required prior to configuring an IPv6 address. In K.15.01.0031 (or later), this is no longer a requirement.

However, before enabling OSPFv3 on K.15.01.0031 (or later), do one of the following:

- Configure a unique 32-bit router ID.
- Configure a unique IPv4 loopback address.

OSPFv3 requires a 32-bit router ID for operation. The 32-bit router ID can be derived from an IPv4 loopback address or it can be specifically set.

Version K.15.02.0004 Clarifications

Rate-Limiting on the Entire Packet

As of software version K.15.02.0004, ICMP rate-limiting and Classifier-based rate-limiting operates on the entire packet length instead of just the IP payload part of the packet. As a result, the effective metering rate is now the same as the configured rate. The rate-limiting applies to these modules.

HP Device	Product Number	Minimum Supported Software Version
HP ProCurve 24-port 10/100/1000 PoE+ v2 zl Module	J9534A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	J9535A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module	J9536A	K.15.02.0004
HP ProCurve 24-port SFP v2 zl Module	J9537A	K.15.02.0004
HP ProCurve 8-port 10-GbE SFP+ v2 zl Module	J9538A	K.15.02.0004
HP 24-port 10/100 PoE+ v2 zl Module	J9547A	K.15.02.0004
HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	J9548A	K.15.02.0004

HP Device	Product Number	Minimum Supported Software Version
HP 20-port Gig-T / 4-port SFP v2 zl Module	J9549A	K.15.02.0004
HP 24-port Gig-T v2 zl Module	J9550A	K.15.02.0004
HP 12-port Gig-T / 12-port SFP v2 zl Module	J9637A	K.15.02.0004

Change to Default Setting for Detecting and Powering Pre-802.3af Devices

- **PoE (PR_0000060319)** - The default setting for the **pre-std-detect** PoE parameter changed. In earlier software the default setting is "on". In K.15.02 and later software, the new default setting is "off".

Compatibility Mode for v2 zl and zl Modules

Note In the following context, v2 zl modules are the second version of the current zl modules. Both v2 zl and zl modules are supported in the 5400zl and 8200zl series chassis switches.

Compatibility Mode allows the inter-operation of v2 zl modules with zl modules in a chassis switch. When in Compatibility Mode, the switch accepts either v2 zl or zl modules. The default is Compatibility Mode enabled. If Compatibility Mode is disabled by executing the **no allow-v1-modules** command, the switch will only power up v2 zl modules.

Syntax: [no] allow-v1-modules

Enables Compatibility Mode for inter-operation of v2 zl and zl modules in the same chassis.

*The **no** form of the command disables Compatibility Mode. Only the v2 zl modules will be powered up.*

Default: Enabled.

The following table shows how the v2 zl and zl modules behave in various combinations and situations when Compatibility Mode is enabled and when it is disabled.

Modules	Compatibility Mode Enabled	Compatibility Mode Disabled
v2 zl modules only	Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities.	v2 zl modules are at full capacity. ZL modules are not allowed to power up.
Mixed v2 zl and zl modules	Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities. But if compatibility mode is disabled, the zl modules go down.	ZL modules are not allowed to power up.
ZL modules only	Same as exists already. If a v2 zl module is inserted, then it operates in the same mode as the zl module, but with performance increases.	The Management Module is the only module that powers up.

Modules	Compatibility Mode Enabled	Compatibility Mode Disabled
	In Compatibility Mode, no v2 zl features are allowed whether the modules are all v2 zl or not.	If Compatibility Mode is disabled, and then enabled, the startup config is erased and the chassis will reboot.

```
ProCurve(config)# allow-v1-modules
This will erase the configuration and reboot the switch.
Continue [y/n]?
```

Figure 1. Example of Enabling Compatibility Mode

```
ProCurve(config)# no allow-v1-modules
All V1 modules will be disabled. Continue [y/n]?
```

Figure 2. Example of Disabling Compatibility Mode

Authorized IP Managers Precedence

Page 15-2 in the Access Security Guide dated June 2010 (and earlier versions) for switches running version K software incorrectly states that the Authorized IP Managers feature takes precedence over Port-Based Access Control (802.1X) and Port Security. The 802.1X and Port Security features are *network* authentication methods, and do not apply to authenticating clients to manage the switch itself. The first sentence in the second paragraph on page 15-2 should read as follows:

“Also, when configured in the switch, the Authorized IP Managers feature takes precedence over local passwords, TACACS+, and RADIUS.”

Minimum Guaranteed Bandwidth Issue

When 10 Mbps ports on an 8200zl or 5400zl switch are configured in QoS for eight outbound queues (the default), and the guaranteed minimum bandwidth is set for 5 Mbps or less for a given queue, then packets in the lower-priority queues may be discarded on ports that are oversubscribed for extended periods of time. If the oversubscription cannot be corrected, HP recommends reconfiguring the switch to operate with four outbound queues. The command to do this is:

```
HPswitch(config)# qos queue-config 4-queues
```

This issue applies to 8200zl and 5400zl switch operating with any of the following modules installed.

HP Device	Product Number	Minimum Supported Software Version
HP ProCurve 24-port 10/100/1000 PoE+v2 zl Module	J9534A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	J9535A	K.15.02.0004
HP ProCurve 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module	J9536A	K.15.02.0004
HP ProCurve 24-port SFP v2 zl Module	J9537A	K.15.02.0004
HP ProCurve 8-port 10-GbE SFP+ v2 zl Module	J9538A	K.15.02.0004
HP 24-port 10/100 PoE+ v2 zl Module	J9547A	K.15.02.0004
HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	J9548A	K.15.02.0004
HP 20-port Gig-T / 4-port SFP v2 zl Module	J9549A	K.15.02.0004
HP 24-port Gig-T v2 zl Module	J9550A	K.15.02.0004

HP Device	Product Number	Minimum Supported Software Version
HP 12-port Gig-T / 12-port SFP v2 zl Module	J9637A	K.15.02.0004

Version K.15.03.0005 Clarification

Loss of Event Log on Upgrade/Downgrade

As a result of the new method of storing the event log in switch memory, event log entries created in K.15.01 or K.15.02 software versions will be erased when upgrading to K.15.03 or later software. Also, event log entries created in K.15.03 and later software will be erased when back-revving to K.15.02 and earlier software versions.

Known Issues

Note	Version K.15.01.0031 is a major software release, and was developed from Version K.14.41. Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.
-------------	--

Known Issues are listed in chronological order of the software version, oldest to newest. For Known Issues in prior versions (K.14.*xxx* or earlier), see the Release Notes provided with those versions.

Version K.15.01.0031

- **OSPF (PR_0000054952)** — HP Switch does not accept Type 7 default route in a NSSA when announced by Cisco.
- **VRRP (PR_0000055742)** — VRRP Fast Failover fails for HA when advertisement interval is less than 1.
- **File Transfer (PR_0000048178)** — If a switch is rebooted through software (CLI, Web, or SNMP) after starting to transfer a new software image to the switch using Secure Copy or SSH File Transfer Protocol, it may abort the image transfer in progress, and reboot to the existing version of the switch software.
- **802.1X (PR_0000054821)** — Client with valid credentials is not able to reach authorized-vid when mixed mode and unauthorized-vid are set.

Expected Results: The client with invalid credentials should be sent to the unauthorized VLAN and the client with the valid credentials should be sent to the authorized VLAN and be able to ping that VLAN.

Current Results: The client with the valid credentials is correctly authenticated but it is not able to ping the auth-vid.
- **Crash (PR_0000055882)** — IPv4 loopback address which followed an IPv6 EUI-64 address in configuration would cause a crash.
- **OSPF (PR_0000046029)** — OSPF Virtual Links cause route flapping.
- **802.1X (PR_0000055580)** — Multiple auth users with different auth-vids placed on same vid
- **DAC (PR_0000050635)** — DAC port flaps after reboot.
- **SFLOW (PR_0000041583)** — Not sending vlan tag in sFlow data.

Version K.15.02.0004

- **PoE (PR_0000060884)** - When using TFTP to copy a pre-K.15 configuration file onto a switch running K.15 software, if the value of **pre-std-detect** was "disabled" in the pre-K.15 config file, the value of **pre-std-detect** will be "enabled" after the file transfer. Workaround: manually disable **pre-std-detect** after the file transfer.
- **Services Module (PR_0000053005)** - In some cases the Services Module will initially fail to boot, but will then recover. During the initial boot failure, the switch Fault LED and the slot LED on the System Support Module will be lit, as well as the module status LED on the Services Module. After the module boots successfully, the Services Module LEDs will correctly indicate that it is functioning properly, but the switch Fault LED and slot LED on the System Support Module will incorrectly remain lit.

- **SFTP (PR_0000060656)** - When connecting to a switch via SFTP, if the user enters the command **ls/cfg**, the switch may appear unresponsive for a period of time. The console will recover, but it might be unresponsive for one minute or more.
- **UDLD (PR_0000058636)** - UDLD can take up to 5 seconds to bring a port online, which may cause issues with VRRP.

Version K.15.03.0005

- **Event Log (PR_0000060511)** — When the switch experiences a brief power outage, the event log might give erroneous indications regarding the cause and the results. Specifically, the switch might report that a) the switch rebooted due to the reset button being pressed, and b) the switch booted from secondary flash because primary flash is corrupt. Both these indications are false. The output of **show version** confirms that the switch booted from primary flash and is running the software from primary flash.

Enhancements

Note

Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

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

Version K.15.01.0031 Enhancements

- **Enhancement (PR_0000011015)** — Cached Re-authentication (Hold State if Radius Server Unavailable). For more information, see the “RADIUS” chapter in the *Access Security Guide* for your switch.
- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link "flapping" rapidly between link-up and link-down states. A new fault event "link-flap" has been created to detect these events. Additionally, a new action, "warn-and-disable," has been created to report and disable the events. Together, these enhancements allow the errant condition to be detected, and the port in question optionally disabled. For more information, see [“Flapping Transceiver Mitigation”](#) below.

Flapping Transceiver Mitigation

In traditional HP switches, the state of a link is driven directly by the reported state of the port, which is required for rapid detection of link faults. However, the consequence of this is that a marginal transceiver, optical, or wire cabling, one which “flaps” up and down several times per second, can cause STP and other protocols to react poorly, resulting in a network outage. This enhancement expands the functionality of the existing Fault Finder function to include a “link-flap” event and a new action of "warn-and-disable". Together, these additions allow the errant condition to be detected, and the port in question can be optionally disabled.

Syntax: fault-finder <link-flap> sensitivity <low | medium | high> action <warn | warn-and-disable>

Default settings: Sensitivity = Medium; Action = Warn

Sensitivity thresholds are static. In a 10-second window, if more than the threshold number of link state transitions (up or down) is detected, the event is triggered. The 10-second window is statically determined, i.e. the counters are reset every 10 seconds, as opposed to being a sliding window. The counters are polled twice per second (every 500 milliseconds), and the event is triggered if the sensitivity threshold is crossed at that time.

The sensitivity thresholds are:

High = 3 transitions in 10 seconds
Medium = 6 transitions in 10 seconds
Low = 10 transitions in 10 seconds

Configuration of the link-flap event and corresponding action applies to all ports and port types (it is a global setting per FFI event type). Note that normal link transition protocols may prevent link state changes from occurring fast enough to trigger the event for some port types, configurations, and sensitivity settings.

When the link-flap threshold is met for a port configured for **warn** (for example, **fault-finder link-flap sensitivity medium action warn**), the following message will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

When the link-flap threshold is met for a port configured for **warn-and-disable** (for example, **fault-finder linkflap sensitivity medium action warn-and-disable**), the following messages will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

```
02673 FFI: port <number>-Port disabled by Fault-finder.
```

```
02674 FFI: port <number>-Administrator action required to re-enable.
```

The warn-and-disable action is available for all fault-finder events on an individual basis. It may be used, for example, to disable a port when excessive broadcasts are received. Because the fault-generated disabling of a port requires operator intervention to re-enable the port, such configuration should be used with care. For example, link-flap initiated disablement is not desired on ports that are at the client edge of the network, because link state changes there are frequent and expected.

Automatic disabling of a port when excessive broadcasts are detected is not recommended at the core or distribution layers, due to the potential to disable large parts of the network that may be uninvolved, and for the opportunity to create a denial-of-service attack.

Within the Web Management interface, double clicking an event on a port that was configured with warn-and-disable and has met the threshold to trigger the disable action, will bring up a dialog box with the event details. The event dialog box now contains a button at the bottom of the page, which can be used to re-enable the disabled port. The button will remain, even if the port has already been brought up through a prior exercise of it, or if the port was re-enabled via some other interface (e.g. the command line). Re-enabling an already enabled port has no effect. The button to acknowledge the event remains unchanged.

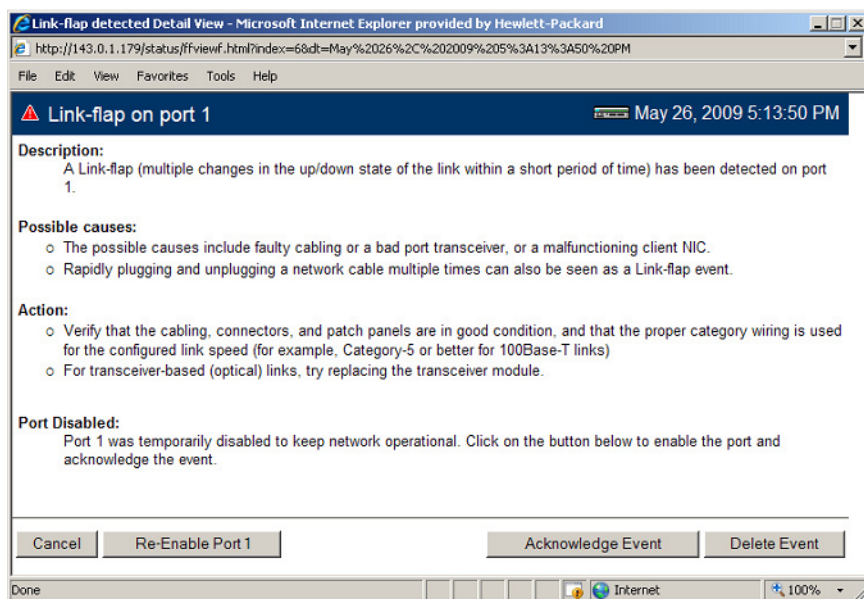


Figure 3. Link-flap on port 1 event detail dialog box

- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.
- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see the “RADIUS” chapter in the *Access Security Guide* for your switch.

- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. The command syntax is as follows:

```
ProCurveSwitch# debug ip pim packet <cr>
```

IP PIM debug output may be filtered further by specifying a source IP address, VLAN and group.

Use the CLI help for syntax details.

- **Enhancement (PR_0000041472)** — VRRP Ping Virtual IP of Backup. For more information, see the chapter “Virtual Router Redundancy Protocol (VRRP)” in the *Multicast and Routing Guide* for your switch.
- **Enhancement (PR_0000045438)** — The Out Of Band Management (OOBM) port on the HP ProCurve Switch 6600 Series is now enabled for IPv6 host functionality.
- **Enhancement (PR_0000045749)** — Module reload enhancement. For more information, see [“Module Reload \(5400zl and 8200zl switches\)”](#) below.

Module Reload (5400zl and 8200zl switches)

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

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

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

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

Note: This feature is not supported for ProCurve One modules.

at: Schedules a whole switch reload at a specified date and time. The time must not be more than 99 days in the future. Minimum required input is **HH:MM**. Cannot be used with the **module** option.

after: Schedules a whole switch reload after the specified length of time, which must not be more than 99 days in the future. Minimum required input is **MM**. Cannot be used with the **module** option

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

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

Figure 4. Example of Reloading a Specified Module

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

- A scheduled, pending reload of the entire switch
- A statement that no reload is scheduled

- The time of the last reload of each module on the system

```
ProCurve(config)# reload at 23:45
Reload scheduled at 23:45:47 6/16/2010
(in 0 days, 1 hours, 41 minutes)

ProCurve(config)# show reload at
Reload scheduled for 23:45:47 06/16/2010
(in 0 days, 1 hours, 40 minutes)

ProCurve(config)# show reload after
Reload scheduled for 23:45:47 6/16/2010
(in 0 days, 1 hours, 40 minutes)
```

Figure 5. Example of the Scheduled Reload At Information

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

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

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

Figure 6. Example of the Scheduled Reload After Information

```
ProCurve(config)# show reload module

Module Reload information:

Module | Last reload date
-----+-----
C      | 10:50:51 01/13/2010
```

Figure 7. Example of the Module Reload Information

Version K.15.01.0032 Enhancements

- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used.

Username and Password Size Increase

For security reasons, it is desirable to allow the configuration of longer usernames and passwords than is currently allowed on the switch. The limits on length will be extended to 64 characters for the following authentication methods:

- Front-end—WEB User Interface, SSH, and Telnet
- Back-end—RADIUS, TACACS+, and Local

General Rules for Usernames and Passwords

Usernames and passwords are case-sensitive. ASCII characters in the range of 33-126 are valid, including:

- A through Z uppercase characters
- a through z lower case characters
- 0 through 9 numeric characters
- Special characters ' ~ ! @ # \$ % ^ & * () - _ = + [] { } \ | ; : ' " , < > / ? (see Restrictions, below)

The SPACE character is allowed to form a username or password pass-phrase. The username must be in quotes, for example "The little brown fox". A space is not allowed as part of a username without the quotes. A password that includes a space or spaces should not have quotes.

Restrictions for the Setmib Command

Usernames and passwords can be set using the CLI command **setmib**. They cannot be set using SNMP.

- Quotes are permitted for enclosing other characters, for example, a username or password of **abcd** can be enclosed in quotes "**abcd**" without the quotes becoming part of the username or password itself. Quotes can also be inserted between other characters of a username or password, for example, **ab**"**cd**. A pair of quotes enclosing characters followed by any additional characters is invalid, for example, "**abc**"**d**.
- Spaces are allowed in usernames and passwords. The username or password must be enclosed in quotes, for example, "**one two three**". A blank space or spaces between quotes is allowed, for example, " ".

Additional Restrictions

Some authentication servers prevent the usage of special symbols such as the backslash (\) and quotes (""). The switch allows the use of these symbols in configurable credentials, but using them may limit access for some users who may use different client software. Please refer to the vendor's documentation for specific information about these restrictions.

Operating Notes on Upgrading or Downgrading Software Versions

When you update software from a version that does not support long passwords to a version that supports long passwords, the existing usernames and passwords continue to be there; no further action is required.

Before downgrading to a software version that does not include this feature, use one of the following procedures:

1. Reset the username and/or password to be no more than 16 characters in length, and without any special characters, using the CLI command **password** or the equivalent in the WebAgent. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

```
ProCurve(config)# password manager
New password: *****
Please retype new password: *****
ProCurve(config)# write mem
```

Or

2. Execute the CLI command **no password all**. This clears all the passwords. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

```
ProCurve(config)# no password all
Password protections will be deleted, do you want to continue [y/n]? y
ProCurve(config)# write mem
```

Or

3. Clear the password by using the "Clear" button on the switch. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

If You Cannot Access the Switch Using the Previous Password

If you cannot access the switch after a software version downgrade, clear the password by using the "Clear" button on the switch to regain access. Then boot into a software version that supports long passwords, and perform steps 1, 2, or 3 in the preceding section.

Version K.15.02.0004 Enhancements

Version K.15.02.004 includes the following enhancements.

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

Multicast ARP Support

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

Syntax: [no] ip arp-mcast-replies

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

Default: Disabled.

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

Figure 8. Example of Enabling the Acceptance of Multicast MACs in the IP Multicast Range

- **Enhancement (PR_0000044183)** —Display interface configuration enhancement.

Display Configuration of Selected Interface

The options provided in this feature allow you to display all the configurations on a specified interface or VLAN with a single command. You can use the options with the startup config command, **show config**, and the running config command, **show running-config**.

Running Configuration Output

You can display the running configuration using this command. An example of the output is shown in [Figure 9](#).

Syntax: show running-config [interface <port-list | loopback <0-7> | vlan <vlan-id-list>]

Displays running configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

Note

The **show running config interface/vlan/svlan** command output cannot be downloaded to the switch; it will not download correctly. Copying and pasting the displayed configuration information into the switch configuration is not supported. This feature only provides a display of all the configuration information for a selected interface or range of interfaces in a single view.

```
ProCurve(eth-A2-A4)# show running-config

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412z1"
interface A2
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans Block
  qos priority 4
  lacp Passive
  gvrp join-timer 30
  gvrp leave-timer 60
  gvrp leaveall-timer 700
exit
interface A3
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans Block
  qos priority 4
  lacp Passive
  gvrp join-timer 30
  gvrp leave-timer 60
  gvrp leaveall-timer 700
exit
vlan 1
  name "DEFAULT VLAN"
  untagged A1-A4,C1-C24,F1-F24
  ip address dhcp-bootp
  exit
interface A2
  dhcp-snooping trust
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  exit
interface A3
  dhcp-snooping trust
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  exit
```

Configuration information for interfaces A2 and A3 is shown in two different places in the config file.

Figure 9. Example of Running Configuration Output for Interfaces A2 - A4

Figure 10 shows an example of the running config for a range of interfaces. The configuration information for interfaces A2 and A3 is now displayed together.


```
ProCurve(config)# show running-config interface A2-A3
```

Running configuration:

```
interface A2
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
interface A3
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
```

All the information for interfaces A2 and A3 is shown together in the output.

Figure 10. Example of Running Config Output for a Specified Interface Range

Figure 11 shows an example of the running config file for a range of interfaces after some configuration changes have been made.

```
ProCurve(config)# no stack
ProCurve(config)# mesh 2-3
Command will take effect after saving configuration and reboot.

ProCurve(config)# write memory
ProCurve(config)# reload

ProCurve# show running-config interface 2-3

Running configuration:

interface 2
  untagged vlan 1
  mesh
  exit
interface 3
  flow-control
  untagged vlan 1
  mesh
  exit
```

Figure 11. Example of Running Config Output for a Range of Interfaces

Figure 12 is an example of the running config output showing VLAN information.

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

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412z1"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
ip routing
vlan 1
  name "DEFAULT VLAN"
  untagged A1-A4,C1-C24,F1-F24
  ip address dhcp-bootp
  exit
vlan 2
  name "test-vlan-2"
  ip helper-address 4.1.1.1
  ip helper-address 5.1.1.1
  ip address 1.1.1.1 255.255.255.0
  ipv6 address 2001::/64 anycast
  ipv6 enable
  exit
vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address
  exit
vlan 4
  name "VLAN4"
  ip address 5.1.1.1 255.255.255.0
  ip bootp-gateway 5.1.1.1
  exit
logging 10.0.102.90
logging system-module ospf
ip route 5.1.1.0 255.255.255.0 vlan 4 distance 3
```

VLAN 4 configuration information is not together in the config file output.

Figure 12. Example of Running Config Output Showing VLAN Information

In [Figure 13](#), the configuration information for VLAN 4 is now displayed in one place.

```
ProCurve(config)# show running-config vlan 3-4

Running configuration:

vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address
  exit
vlan 4
  name "VLAN4"
  ip address 5.1.1.1 255.255.255.0
  ip bootp-gateway 5.1.1.1
  ip route 5.1.1.0 255.255.255.0 distance 3
  exit
```

VLAN 4 configuration information is displayed together in the output.

Figure 13. Example of Running Config Output for a Range of VLANs

[Figure 14](#) shows an example of the running config for a range of VLANs after configuration changes have been made to selected VLANs.

```
ProCurve(config)# dhcp-snooping
ProCurve(config)# vlan 14
ProCurve(vlan-14)# exit
ProCurve(config)# vlan 15
ProCurve(vlan-15)# exit
ProCurve(config)# vlan 23
ProCurve(vlan-23)# exit
ProCurve(config)# dhcp-snooping vlan 14-15
ProCurve(config)# static-mac 00:11:22:33:44:55 vlan 23 interface A3
ProCurve(config)# spanning-tree instance 2 vlan 15

ProCurve(config)# show running-config vlan 14-15

Running configuration:

vlan 14
  name "VLAN14"
  no ip address
  dhcp-snooping
  exit
vlan 15
  name "VLAN15"
  no ip address
  dhcp-snooping
  spanning-tree instance 2
  exit
```

Figure 14. Example of Output for Running Config for a Range of VLANs

Startup Configuration Output

You can display the startup configuration using this command. An example of the startup configuration output is shown in [Figure 15](#).

Syntax: show config [interface <port-list | loopback <0-7> | vlan <vlan-id-list>]

Displays startup configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

```
ProCurve(config)# show config

Startup configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "ProCurve Switch 5412zl"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
vlan 1
    name "DEFAULT VLAN"
    untagged A1-A4,C1-C9,C15-C24,F1-F24
    ip address dhcp-bootp
    no untagged C10-C14
    exit
vlan 5
    name "VLAN5"
    untagged C10-C14
    ip address 5.1.1.1 255.255.255.128
    exit
interface loopback 5
    ip address 7.1.1.1
    exit
interface loopback 7
    ip address 12.1.1.1
    exit
snmp-server community "public" unrestricted
```

Figure 15. Example of Startup Configuration Output

Figure 16 shows an example of the startup config output for a selected VLAN.

```
ProCurve(vlan-5)# show config vlan 5

Startup configuration:

vlan 5
    name "VLAN5"
    untagged C10-C14
    ip address 5.1.1.1 255.255.255.128
    exit
```

Figure 16. Example of Startup Config Output for a Specific VLAN

Figure 17 shows an example of the startup config output for a range of interfaces for a specific VLAN.

```
ProCurve(vlan-5)# show config interface C10-C13

Startup configuration:

interface C10
    untagged vlan 5
    exit
interface C11
    untagged vlan 5
    exit
interface C12
    untagged vlan 5
    exit
interface C13
    untagged vlan 5
    exit
```

Figure 17. Example of Startup Config Output for a Range of Interfaces for a Specific VLAN

- **Enhancement (PR_0000045649)**—Post-logon banner enhancement.

Post-logon Banner Enhancement

A text message that has been configured with the **banner motd** command displays with the authentication prompt when a user opens a console, telnet, SSH, or WebAgent session.

The **exec** option of the **banner** command allows a user-configurable message to be displayed after the user has been authenticated. If there is no password on the switch, the exec banner message displays immediately.

Syntax: [no] banner exec <ASCII-string>

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

<ASCII-string>: The text must end with a delimiting character, which can be any single character except the tilde (~) character.

*The **no** version of the command removes the banner exec text.*

```
ProCurve(config)# banner exec &  
Enter TEXT message. End with the character &  
This is Switch A in the language lab &
```

Figure 18. Example of the banner exec Command

To display the status and text for the exec banner configuration, use the **show banner exec** command.

```
ProCurve(config)# show banner exec  
  
Banner Information  
  
Banner Status: Enabled  
Configured Banner:  
  
This is Switch A in the language lab
```

Figure 19. Example Displaying Exec Banner Configuration

WebAgent Display of Exec Banner Message

If the MOTD banner message has been configured, it is displayed first. If the **exec** banner option has also been configured, the MOTD banner message is followed by a [Continue](#) link to the next page.

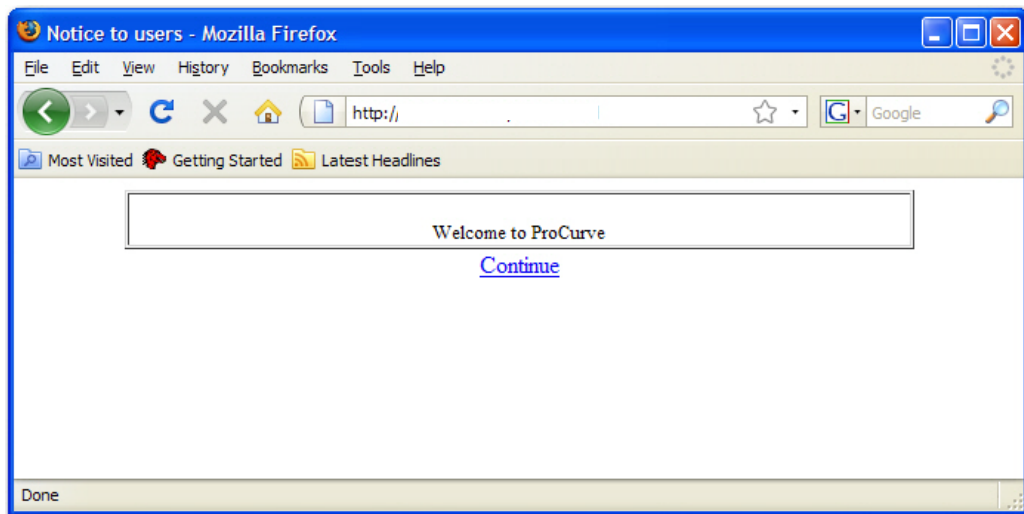


Figure 20. Example of MOTD Message in the WebAgent

Clicking on [Continue](#) displays the Username/Password dialog box if the switch has been configured with password security. If no password has been configured, the exec banner message displays immediately.

After being authenticated successfully when a password has been configured, the exec banner message displays. Click on the [Continue](#) link to proceed to the WebAgent Home Page.

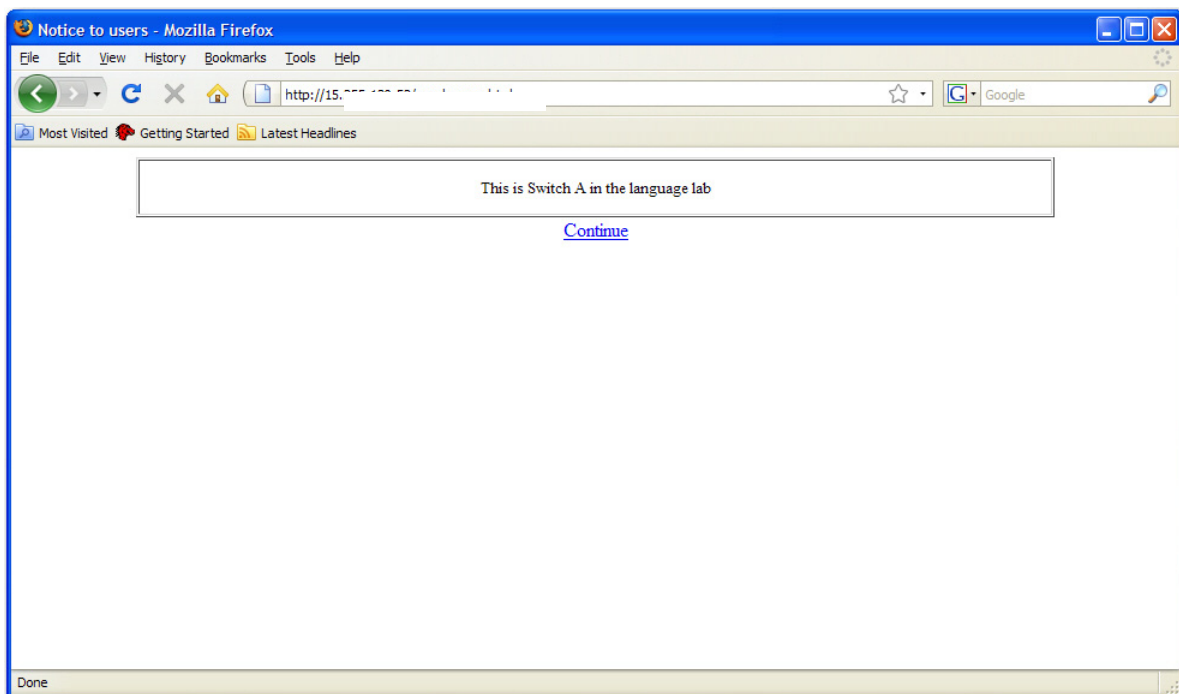


Figure 21. Example of Exec Banner Message

SNMP Support

The MIB variables required to support Exec banner are in the hpicfBasic.mib file.

Error Messages

Error Message	Description
Delimiter must be a single character	Use a single ASCII character for a delimiter at the end of the Exec Banner message
Tildes (~) are not allowed.	Do not use a tilde in the Exec Banner message.
String for Banner Exec is too long. Allowed length is 3070.	The Exec Banner message can be up to 3070 characters long.

- **Enhancement (PR_0000045707)**—The tilde character is now allowed in TACACS+ and RADIUS encryption keys.

Support for the Tilde (~) Character in TACACS+ and RADIUS Keys

This feature allows you to configure a TACACS+ or RADIUS encryption key that includes a tilde (~) as part of the key, for example, “hp~procurve”. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

SNMP already supports the inclusion of the tilde character in a key.

Configuring TACACS+ Keys

Global Keys. If you need only one encryption key for the switch to use in all attempts to authenticate through a TACACS+ server, configure a global key.

To configure a global encryption key for TACACS+, enter this command.

Syntax: [no] tacacs-server key <key-string>

Configures an optional global encryption key. Keys configured in the switch must exactly match the encryption keys configured in the TACACS+ servers that the switch will attempt to use for authentication.

*The **no** form of the command removes the global encryption key.*

ProCurve(config)# tacacs-server key hp~procurve											
ProCurve(config)# show tacacs											
Status and Counters - TACACS Information											
Timeout: 5											
Source IP Selection: Outgoing Interface											
Encryption Key: hp~procurve											
Server IP Addr Opens Closes Aborts Errors Pkts Rx Pkts Tx OOBM											

10.10.10.2	0	0	0	0	0	0	0	0	0	0	0

Figure 22. Example of Configuring a Global Encryption Key for TACACS+ with a ~ Character

Host-Specific Keys

If the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

Syntax: [no] tacacs-server host <ip-addr> [key <key-string>]

Adds a TACACS+ server and optionally assigns a server-specific encryption key.

*The **no** form of the command removes a TACACS+ server assignment (including its server-specific encryption key, if any).*

```
ProCurve(config)# tacacs-server host 10.10.10.2 key hp~procurve
```

Figure 23. Example of Configuring a Host-Specific Key

Use the **show running-config** command to display the key information.

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

Running configuration:

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

hostname "ProCurve Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
banner motd "good morning
tacacs-server host 10.10.10.2 key "hp~procurve"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 24. Example of the Running Configuration File Showing the Host-Specific Key for TACACS+ with the "~" Included

For more information about TACACS+, see the chapter "TACACS+ Authentication" in the *Access Security Guide* for your switch.

Configuring RADIUS Keys

Global Keys. To configure a global key for RADIUS authentication, enter this command.

Syntax: [no] radius-server key <global-key-string>

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key.

Default: Null

*The **no** form of the command removes the global encryption key.*

```
ProCurve(config)# radius-server key hp~procurve

ProCurve(config)# show radius
Status and Counters - General RADIUS Information
Deadtime (min): 0
Timeout: 5
Retransmit Attempts: 3
Global Encryption Key: hp~procurve
Dynamic Authorization UDP Port: 3799
Source IP Selection: Outgoing Interface

Auth Acct DM/Time

Server IP Addr Port Port CoA Window Encryption Key OOBM
-----
10.33.18.127 1812 1813 No 300 No
```

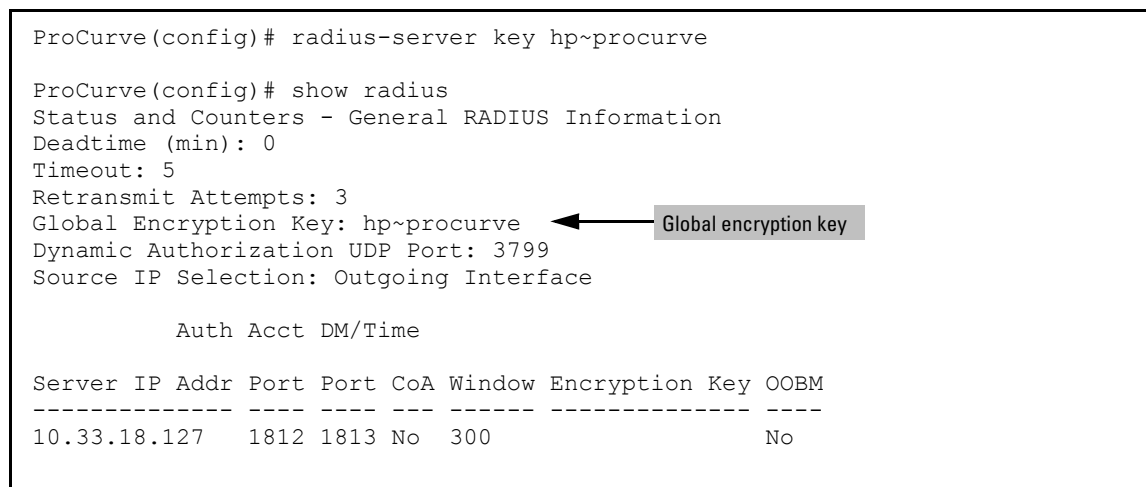


Figure 25. Example of RADIUS Global Encryption Key with a ~ Character Included

Host-Specific Keys. To configure a host-specific key for RADIUS authentication, enter this command.

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

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

Default: Null

*Use the **no** form of the command to remove the key for a specified server.*

```
ProCurve(config)# radius-server host 10.33.18.127 key hp~procurve
ProCurve(config)# show radius

Status and Counters - General RADIUS Information

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

Server IP Addr      Auth    Acct
-----
10.33.18.127      1812    1813    hp~procurve
```

Figure 26. Example of Host-Specific Key for RADIUS Authentication

```
ProCurve(config)# show running

Running configuration:

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

hostname "ProCurve Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
banner motd "good morning
radius-server host 10.33.18.127 key "hp~procurve"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 27. Example of Running Configuration File Showing the Host-Specific Key for RADIUS Authentication

For more information about RADIUS keys, see the chapter “RADIUS Authentication, Authorization, and Accounting” in the *Access Security Guide* for your switch.

- **Enhancement (PR_0000045711)** —Web authentication message enhancement.

Web Auth Deny Message

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

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

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

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

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

access-denied-str: *The text message that is appended to the end of the web page when there is an unsuccessful authentication request. The string can be up to 250 ASCII characters.*

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

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

Figure 28. Example of Configuring an Access Denied Message on the Switch

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

Port Access Web-based Configuration

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

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

Figure 29. Example of Output showing the Custom Access Denied Message

The example in [Figure 30](#) shows the text of the Access Denied Message when the **radius-response** option is configured.

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

Port Access Web-based Configuration

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

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

Figure 30. Example of Access Denied Message when radius-response is Configured

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

Web Page Display of Access Denied Message

The web page in [Figure 31](#) is an example of the denied access message that appears when **unauth-vid** is configured.

Invalid Credentials

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

Estimated time remaining: 35 seconds

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

Figure 31. Example of Web Page with Configured Access Denied Message When unauth-vid is Configured

[Figure 32](#) shows an example of a web page displaying the access denied message when un **auth-vid** is not configured.

Invalid Credentials

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

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

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

Figure 32. Example of Web Page with Configured Access Denied Message When unauth-vid is not Configured

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

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

Running configuration:

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

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

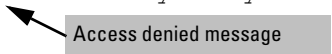


Figure 33. Example of Running Configuration Output Displaying Access Denied Message

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

Running configuration:

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

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

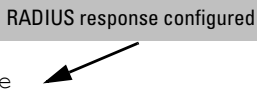


Figure 34. Example of Running Configuration Output When RADIUS Response is Configured

- **Enhancement (PR_0000045752)**—User-configurable per-port MAC address enhancement.

Port Security Per-Port MAC Increase

User-configurable per-port MAC addresses have been limited to 32 addresses. This enhancement increases the number of user-configurable per-port MAC addresses from 32 to 64 addresses. The switch-wide per-port address limit is unchanged.

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

PoE with LLDP

Overview

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

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

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

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

PoE Allocation

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

- Using LLDP MED TLVs: Disabled by default. Can be enabled using the **int <port-list> PoE-lldp-detect [enabled | disabled]** command, as shown below. LLDP MED TLVs sent by the PD are only used to negotiate power if the LLDP PoE+ TLV is disabled or inactive; if the LLDP PoE+ TLV is sent as well (not likely), the LLDP MED TLV is ignored.
- Using LLDP PoE+ TLVs: Enabled by default. The LLDP PoE+ TLV is always advertised unless it has been disabled. It is enabled using the **lldp config <port-list> dot3TlvEnable poeplus_config** command. See [“Enabling Advertisement of PoE+ TLVs” on page 51](#) for the command syntax.) It always takes precedence over the LLDP MED TLV.

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

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

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

Default: Disabled

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

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

or in interface context:

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

Note

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

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

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

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

Figure 35. Example of Port with LLDP Configuration Information Obtained from the Device

Enabling Advertisement of PoE+ TLVs

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

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

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

Default: Enabled

Displaying PoE When Using LLDP Information

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

Syntax: `show lldp config <port-list>`

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


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

LLDP Port Configuration Detail

Port : 4
AdminStatus [Tx_Rx] : Tx_Rx
NotificationEnabled [False] : False
Med Topology Trap Enabled [False] : False

TLVS Advertised:
* port_descr
* system_name
* system_descr
* system_cap

* capabilities
* network_policy
* location_id
* poe

* macphy_config
* poeplus_config

IpAddress Advertised:
```

Figure 36. Example of LLDP Port Configuration Information with PoE

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

- **Enhancement (PR_0000048021)**—Support was added for the following products.
 - J9310A - HP ProCurve 3500yl-24G-PoE+ Switch
 - J9311A - HP ProCurve 3500yl-48G-PoE+ Switch
 - J9312A - HP ProCurve 10-GbE 2-Port SFP+/2-Port CX4 yl Module.
- **Enhancement (PR_0000050143)** — Adds the ability for Interrupt-Driven Port-Down Notification.
Note: This enhancement was inadvertently omitted from the published K.15.02.0005 Release Notes.
- **Enhancement (PR_0000052732)**—Enhancement to increase the MAC Authentication Client Limit to 256.

Increase MAC Auth Client Limit to 256

The client limit is 256 clients per-port for MAC-auth and Web-auth; the client limit for 802.1X is 32 clients per port. The MAC-auth and Web-auth limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method.

The following commands are used to specify client limits:

```
aaa port-access mac-based <port-list> [addr-limit]
aaa port-access web-based <port-list> [client-limit]
aaa port-access authenticator <port-list> [client-limit]
```

- **Enhancement (PR_0000052801)**—Categorize CLI Return Messages enhancement.

Categorize CLI Return Messages

When a CLI command returns a message, that message is now prefixed with a category describing the type, as follows:

- Error
- Warning
- Information

Syntax: session show-message-type [enable | disable]

When enabled, the CLI return messages are prefixed with string that indicates the type of message. Entered at the manager level.

*The **disable** option disables prefixing returned messages for the session for which this command is executed.*

Note: This setting is not saved when the switch is rebooted.

Default: Disabled on all CLI sessions

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

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

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

Figure 37. Examples of Message Prefixes

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

```
ProCurve(config)# show session
Show Message Type: Enabled
CLI Interactive Mode: Enabled
```

Figure 38. Example Showing the label cli-return-message Command is Enabled

CLI Interactive Commands

When the CLI interactive command mode is enabled, you must explicitly enter the choice of yes (y) or no (n) for interactive commands. When interactive command mode is disabled, the default choice for all command is **yes**, except as noted below. The CLI interactive mode command enables or disables interactive mode for the CLI session.

Syntax: session interactive-mode [enable | disable]

Enables or disables interactive mode for the CLI session.

*The **disable** option disables interactive mode. The default choice for yes/no interactive commands will be **yes** except for commands when there is a prompt to save the config. The default for that is **no**.*

*The default choice for rebooting the switch is **yes**.*

Note: *This setting is not saved when the switch is rebooted.*

Default: Enabled on all sessions.

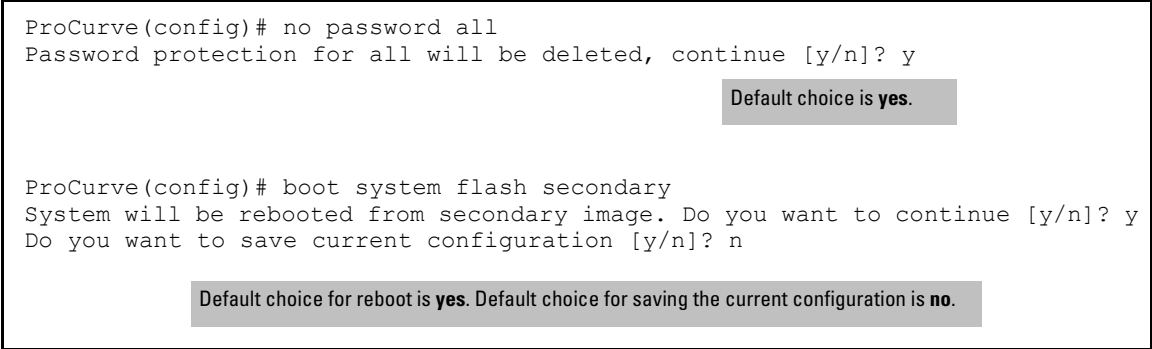


Figure 39. Example of CLI Interactive Mode When Disabled

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



Figure 40. Example Showing CLI Interactive Mode is Enabled

Interactive Commands Requiring Additional Options

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

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

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

Command	Non-Interactive Alternate Command
setup mgmt-interfaces	No equivalent non-interactive command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
password manager	password manager plaintext <password-string>

Command	Non-Interactive Alternate Command
password operator	password operator plaintext <password-string>
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
crypto host-cert generate self-signed	crypto host-cert generate self-signed <start-date> <end-date> <CNAME-STR> <ORG-UNIT-STR> <ORGANIZATION-STR> <CITY-STR> <STATE-STR> <code>

Menu Commands

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

```
ProCurve(config)# menu

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

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

- setup
- show interfaces display

SNMPv3 Special Cases

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

- **snmpv3 user:** In interactive mode, the command **snmpv3 user** will create snmpv3 users, even if snmpv3 has not been enabled.
- **snmpv3 enable:** When interactive mode is disabled, this command only enables snmpv3. It does not prompt for an authentication password. When the command is first executed, a default initial user is created. A message displays:
User 'initial' has been created.

Banner MOTD Command with Non-Interactive Mode

The use of escape characters allows the **banner motd** command to be used in non-interactive mode for multiple message lines. In non-interactive mode, you can create a banner message enclosed in double quotes or other delimiter that uses escape characters within the delimiters. Other existing CLI commands do not support the escape characters.

The following escape characters are supported:

\"	double q
\'	single quote
\`	forward quote
\\	backslash
\f	form feed
\n	newline
\r	carriage return
\t	horizontal tab
\v	vertical tab

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

ProCurve(config)# show banner motd

Banner Information

Banner status: Enabled

Configured Banner:

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

    The banner motd command will support escape characters."
```

Figure 41. Example of Configuring the Banner Message Using Escape Characters Within Double Quote Delimiters

The running configuration file contains the banner message as entered in the command line.

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

Running configuration:

;J8693A Configuration Editor; Created on release #K.14.00x

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

Figure 42. Example of the Running Config File with Banner MOTD Configured in Non-interactive Mode

You can use a delimiting character other than quotes as well, as shown in [Figure 43](#).

```
ProCurve(config)# banner motd #
Enter TEXT message. End with the character '#'
You can use the \'banner motd\' CLI command in non-interactive mode.\n\n\tThe
banner motd command will support escape characters.#
```

Figure 43. Example of Configuring the Banner Message Using an Alternate Delimiter of '#'

- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az).

Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) follows the 802.3az standard, which provides support for a system to operate in low power idle mode during low link utilization. This allows both sides of a link to disable or turn off a portion of the system's transmit/receive circuitry, saving power. When traffic is ready for transmission, the interface sends a "wake-up" message to the link partner to prepare to receive the traffic. The circuitry is returned to "normal" mode. Both sides of the link must be EEE-capable to support the power-saving idle mode.

To enable EEE on a port or range of ports, enter this command.

Syntax: [no] int <port-list> energy-efficient-ethernet

Enables EEE for a given port or range of ports.

*The **no** form of the command disables EEE for a port or range of ports.*

Default: Enabled

```
ProCurve(config)# int B5-B7 energy-efficient-ethernet
```

```
ProCurve(config)# show energy-efficient-ethernet
```

Port	EEE Config	Current Status	txWake (μS)
B1	Enabled	Active	30
B2	Enabled	Inactive	-
B3	Disabled	Inactive	-
B4	Enabled	Unsupported	-
B5	Enabled	Active	30
B6	Enabled	Active	30
B7	Enabled	Inactive	-

Figure 44. Example of EEE Enabled on Ports B5 - B7

The parameters are explained in the following table.

Parameter	Description
EEE Config	The EEE configuration status, read from the configuration database.
– Enabled	EEE mode is enabled.
– Disabled	EEE mode is disabled.
Current Status	Current EEE operational status.
– Active	The port is advertised and auto-negotiated EEE with link partner (an EEE-capable partner). EEE mode is enabled.
– Inactive	Set to one of the following conditions: <ul style="list-style-type: none"> – EEE configuration is disabled on the local port. – Local port advertises EEE capabilities with “EEE disabled” link partner or non-EEE link partner. – Auto-negotiation is mandatory for EEE to work. EEE configuration will not be applied if the port is in Forced/Manual (speed-duplex) mode. The current status will be ‘inactive’ for Forced/Manual mode port configuration. – EEE is not supported for 10Base-T. The current status will be ‘inactive’ if the link is operating in 10Base-T mode.
– Unsupported	The local physical interface does not have EEE capability.
txWake	Current value of Transmit wake-up time (in microseconds).

Note The interface modules do not support adjustment of both Transmit and Receive wake-up times. Therefore, txWake is constant.

LLDP Support for EEE

Layer 2 (Data Link Layer) EEE capability is a feature that allows fine-tuning for EEE that uses LLDP TLVs for the negotiation of physical link partners' wake up time values. An EEE-capable port notifies its link partner about the EEE capabilities supported. The ports then negotiate how to best optimize energy efficiency.

To enable Layer 2 EEE and the advertisement of the EEE TLV, enter this command.

Syntax: [no] lldp config <port-list> dot3TlvEnable eee_config

Enables the advertisement of Layer 2 EEE TLVs for a given port or range of ports.

*The **no** form of the command disables the advertisement of EEE TLVs.*

Default: Enabled

```
ProCurve(config)# lldp config B5 dot3TlvEnable eee_config
ProCurve(config)# show lldp config B5

LLDP Port Configuration Detail

  Port : B5
  Adminstatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False

  TLVs Advertised:
    *port_descr
    *system_name
    *system_descr
    *system_cap

    *capabilities
    *network_policy
    *location_id
    *poe

    *macphy_config
    *poe_config
    *eee_config
```

Figure 45. Example of Configuring Layer 2 TLVs on a Port

To display the EEE TLV information for the local port, enter the **show lldp info local-device <port-list>** command.

```
ProCurve(config)# show lldp info local-device B5

LLDP Local Port Information Detail

Port       : B5
PortType   : local
PortID     : 5
PortDesc   : B5
Pvid       : 1

Energy Efficient Ethernet (EEE) Wake Times (microseconds)

Transmit           : 10
Receive            : 10
Echo Transmit      : 10
Echo Receive       : 10
Fallback Receive   : 10
```

Figure 46. Example of Output for LLDP Information for a Local Port

To display the EEE TLV information for the link partner, enter the **show lldp info remote-device <port-list>** command.

```
ProCurve(config)# show lldp info remote-device B6

LLDP Remote Device Information Detail

Local Port   : B6
ChassisType  : mac-address
ChassisID    : 00 15 23 ff 2d 49
PortType     : Local
PortID       : 3
SysName      : HP Switch
System Desc  : ProCurve Switch
PortDesc     : 3
Pvid         : 22
.
.
.
Energy Efficient Ethernet (EEE) Wake Times (microseconds)

Transmit           : 10
Receive            : 10
Echo Transmit      : 10
Echo Receive       : 10
Fallback Receive   : 10
```

Figure 47. Example of Output for LLDP Information for a Remote Port

- **Enhancement (PR_0000055751)**—Support was added for the following product.
J9153A—10-GbE SFP+ ER Transceiver (J9153A HP X132 10G SFP+ LC ER Transceiver)
- **Enhancement (PR_0000057058)**—Adds this feature to Nonstop Switching: synchronization for 802.1X supplicants originating from the switch.

- **Enhancement(PR_000057799)**—Support was added for the following products.

J9534A - HP ProCurve 24-port 10/100/1000 PoE+ v2 zl Module
J9535A - HP ProCurve 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module
J9536A - HP ProCurve 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module
J9537A - HP ProCurve 24-port SFP v2 zl Module
J9538A - HP ProCurve 8-port 10-GbE SFP+ v2 zl Module
J9547A - HP 24-port 10/100 PoE+ v2 zl Module
J9548A - HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module
J9549A - HP 20-port Gig-T / 4-port SFP v2 zl Module
J9550A - HP 24-port Gig-T v2 zl Module
J9637A - HP 12-port Gig-T / 12-port SFP v2 zl Module

Version K.15.03.0003 Enhancements

Version K.15.03.0003 includes the following enhancements.

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

Custom Default Configuration

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

The feature provides the ability to:

- Use a customized configuration file as a default configuration file
- Enable the switch to start up with the specified default configuration

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

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

Note

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

Creating the Custom Default Configuration File

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

To start creating the configuration file to be used as the custom default configuration file, enter the commands that configure the features desired and then save the configuration file using the **write memory** command. An example is shown in [Figure 48](#).

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

ProCurve(config)# write memory
```

Figure 48. Example of Creating a Config File with the Desired Features

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

To save this configuration as the custom default configuration, the startup configuration file is copied to the default configuration file, as shown in [Figure 49](#).

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

Figure 49. Example of Copying the Startup Configuration File to the Custom Default Configuration File

Copying an Existing Configuration File to the Custom Default Configuration File

The switch can have up to 3 different configuration files stored in flash memory. (For more information about multiple configuration files, see “Multiple Configuration Files” in the *Management and Configuration Guide* for your switch.) To copy a configuration file that exists in flash memory to the custom default configuration file, use this command.

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

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

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

Figure 50. Copying the abc.cfg Config File to the Custom Default Config File

Copying the Custom Default Config File onto the Switch

Using TFTP

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

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

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

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

Figure 51. Copying a Stored Config File to the Default Config File Using TFTP

Using XMODEM

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

Syntax: copy xmodem default-config

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

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

Figure 52. Copying a Stored Config File to the Custom Default Config File Using XMODEM

Using USB

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

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

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

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

Figure 53. Copying a Stored Config File to the Custom Default Config File Using USB

Copying the Custom Default Config File Off the Switch

Using TFTP

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

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

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

Using XMODEM

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

Syntax: copy default-config xmodem

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

Using USB

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

Syntax: copy default-config usb stored_config.cfg

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

Using SFTP and SCP to Transfer the Custom Configuration

While the switch supports an SSH server with SCP and/or SFTP running on it, the switch is not an SCP or SFTP client. To transfer the default custom configuration file to or from the switch, you must connect to the switch's SSH server using any SCP or SFTP client. Instead of the actual name of the custom default configuration file, an alias name of "default-config" is displayed in the file listings and for get/store functions.

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

Note

You must have an SCP/SFTP client implemented in order to execute **copy scp** or **copy sftp** commands on the switch.

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

```
C:\PuTTY> psftp 10.1.243.209

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

Please register your products now at: www.ProCurve.com

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

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

psftp>
```

This is the custom default config.

Figure 54. Example of Using SFTP

Erasing a Configuration File

If a custom default configuration file exists and the **erase startup-config** command is executed, the current active configuration is erased and the switch is booted with the custom default configuration.

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

Figure 55. Example of Erasing the Startup Config File When a Default Custom Config File Exists

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

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

Figure 56. Example of Erasing the Startup Config File When a Default Custom Config File Does Not Exist

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

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

Figure 57. Example of Erasing the Custom Default Config File

Displaying the Configuration Files

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

```
ProCurve(config)# show config files

Configuration files:

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

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

A custom default configuration file exists.

Figure 58. Example Output Displaying 3 Configuration Files

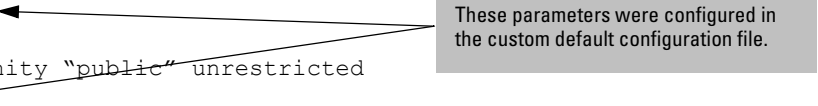
Enter the command **show default-config** to display the custom default configuration.

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

Custom default configuration:

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

hostname "ProCurve Switch"
module 1 type J86xxA
module 2 type J86xxA
vlan 1
    name "DEFAULT-VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
interface 4
    flow-control
    exit
snmp-server community "public" unrestricted
spanning-tree
```



These parameters were configured in the custom default configuration file.

Figure 59. Example of Output for Custom Default Configuration File

If a custom default configuration file exists and you erase the current active config file (using the **erase startup-config** command), then issue the **show running-config** command, the output will display the contents of the custom default configuration file. The custom default configuration file is loaded upon bootup. See [Figure 60](#).

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

Custom default configuration:

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

hostname "ProCurve Switch"
module 1 type J86xxA
module 2 type J86xxA
vlan 1
    name "DEFAULT-VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
interface 4
    flow-control
    exit
snmp-server community "public" unrestricted
spanning-tree
```

Figure 60. Example of Output of Custom Default Config File When Current Active Config File Erased

Troubleshooting Custom Default Configuration Files

- If the switch won't boot because of a problem with the custom default configuration file, the file can be removed using the ROM mode interface.
- The custom default configuration file cannot be erased using the front panel buttons on the switch. If the switch can be booted, use the **erase default-config** command to remove the custom default configuration file.
- **Enhancement (PR_0000045796)** — Adds the ability to enable SNMP traps when MAC addresses are added to or deleted from a port.

SNMP Trap Upon Port Addition or Deletion of MAC Addresses

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

Configuring SNMP Trap Generation

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

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

Globally enables or disables generation of SNMP trap notifications.

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

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

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

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

Figure 61. Example of trap-interval Option

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

Figure 62. Example of mac-move Option

Additional mac-notify Options

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

Note

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

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

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

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

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

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

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

Mac Notify Trap Information

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

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

Figure 63. Example of Configuring Traps on a Per-Port Basis for Learned MAC Addresses

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

Mac Notify Trap Information

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

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

Figure 64. Example of Configuring Traps on a Per-Port Basis for Removed MAC Addresses

Interface Context Level Configuration

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

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

Figure 65. Example of the Interface Context for mac-notify traps Command

Displaying the MAC Notify Traps Configuration Information

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

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

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

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

Mac Notify Trap Information

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

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

Figure 66. Example of Information for SNMP Trap Configuration

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

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

Running configuration:

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

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

The mac-notify commands that were configured.

Figure 67. Example of Running Config File With mac-notify Parameters Configured

- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed.

Log Message When Startup Config Updated

This enhancement enables notification to a management station when changes to the startup configuration file occur and are written to flash. Changes to the configuration file can occur when executing a CLI **write** command, executing an SNMP **set** command directly using SNMP, or when using the WebAgent.

A log message is always generated when a change occurs. An example log entry is:

I 07/06/10 18:21:39 02617 mgr: Startup configuration changed by SNMP. New seq. number 8

The corresponding trap message is sent if the **snmp-server enable traps startup-config-change** command is configured.

Syntax: [no] snmp-server enable traps startup-config-change

Enables notification of a change to the startup configuration. The change event is logged.

Default: Disabled

An example of configuring the command with the CLI is shown in [Figure 68](#). The number that displays when **show config** is executed is global for the switch and represents the startup configuration sequence number.

```
ProCurve(config)# snmp-server enable traps startup-config-change
ProCurve(config)# show config
Startup configuration: 16
; J8697A Configuration Editor; Created on release #K.14.54

hostname "ProCurve Switch"
module 1 type J8702A
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A24, B1-B10
    ip address dhcp-bootp
    exit
snmp-server community "public" unrestricted
```

The number "16" is global for the switch and represents the startup configuration sequence number.

Figure 68. Example of Enabling Notification of Changes to the Startup Config File

[Figure 69](#) displays an example of the fields in the trap when a change is made via SNMP (station ip=0xAC161251 (172.22.18.81), no username is set, and the new sequence number is 16).

```

+ Internet Protocol, Src: 172.22.18.57 (172.22.18.57), Dst: 172.22.18.81 (172.22.18.81)
+ User Datagram Protocol, Src Port: snmp (161), Dst Port: snmptrap (162)
+ Simple Network Management Protocol
  version: version-1 (0)
  community: public
+ data: trap (4)
  trap
    enterprise: 1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1 (SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1)
    agent-addr: 172.22.18.57 (172.22.18.57)
    generic-trap: enterpriseSpecific (6)
    specific-trap: 6
    time-stamp: 65437
  variable-bindings: 6 items
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.9 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.9): 16
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.1 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.1): 2
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.2 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.2): 4
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.3 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.3): AC161251
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.4 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.4): <MISSING>
    + SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.5 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.5): 1

```

Figure 69. Example of the Fields When the SNMP Trap is Set

- **Enhancement (PR_0000052738)** — Adds VLAN information to the output of the **show mac-address** commands.

Show MAC with VLAN

This feature displays the VLAN ID with each MAC address for the **show mac-address <option>** command.

```

ProCurve(config)# show mac-address 4-6

Status and Counters - Port Address Table - 4

MAC Address    VLAN
-----
001186-f47ff4 2

Status and Counters - Port Address Table - 5

MAC Address    VLAN
-----
001279-7fbaf4 4

Status and Counters - Port Address Table - 6

MAC Address    VLAN
-----
001321-1763ca 4

```

Figure 70. Example of Output for show mac-address <port-list> Command

```
ProCurve(config)# show mac-address 001635-36de76

Status and Counters - Address Table - 001635-36de76

Port  VLAN
-----
7      5
```

Figure 71. Example of Output for show mac-address <mac-address> Command

```
ProCurve(config)# show mac-address vlan 5

Status and Counters - Address Table - VLAN 5

MAC Address  Port
-----
001635-36de76 7
```

Figure 72. Example of Output for show mac-address vlan <vid> Command

```
ProCurve(config)# show mac-address

Status and Counters - Port Address Table

MAC Address  Port  VLAN
-----
001635-36de76 7      1
00934f-894rd2 5      1
098745-de4928 6      1
```

Figure 73. Example of Output showing Ports and VLAN IDs for all MAC Addresses

- **Enhancement (PR_0000054042)** — Adds the ability to monitor egress queues for dropped packets when QoS is configured.

Outbound Queue Monitor

When QoS is used to prioritize traffic, different kinds of traffic can be assigned to different egress queues. If there is a great deal of traffic, some of the traffic to the lower priority queues may be dropped. This feature allows the egress queues for a port to be monitored for dropped packets.

Syntax: [no] qos watch-queue <port> out

Configures the switch to start monitoring the specified port for the dropped packets for each queue. Disabling and then re-enabling monitoring on a port clears the per-queue dropped packet counters.

*The **no** form of the command stops the collection of dropped traffic information.*

Default: Disabled

```
ProCurve(config)# qos watch-queue 5 out

ProCurve(config)# show qos watch-queue 5
Egress Queue Counters for Port 5
```

Queue	802.1p Priority	Dscp Mapped	Packet Drop Count
1	1-2	110000	5
2	0,3	none	55443
3	4-5	100100	0
4	6-7	101101	0

Figure 74. Example of Monitoring Egress Queues on a Port

- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information.

Show OSPF Neighbor Timers

This enhancement provides the ability to display the OSPF neighbor timer information by adding the **detail** option to the **show ip ospf neighbor** command.

Syntax: show ip ospf neighbor [detail [router-id]]

The detail option displays the OSPF neighbor timer information. You can optionally enter the router-id of the neighbor for which detail information is wanted.

There are two new counters that display neighbor timer information:

- **Dead-timer Expires (HH:MM:SS):** The time remaining for an active adjacency to expire if there are no more hello packets received.
- **Neighbor Uptime (HH:MM:SS):** The amount of time an adjacency is active.

If a neighbor loses adjacency and then re-establishes it, the Neighbor Uptime counter is set to zero. The Dead-timer Expires counter is set to the dead interval for the interface.

If a graceful restart of the neighbor occurs, the Neighbor Uptime counter continues to increment as the adjacency is considered active while the neighbor is restarting. The Dead-timer Expires counter is set to the hold timer for the neighbor. When the restart completes, the counter is set to the dead interval for the interface.

```
ProCurve(config)# show ip ospf neighbor detail

OSPF Neighbor Information for neighbor 10.10.10.2

IP Address: 10.10.10.2
Router ID : 10.10.10.2      State : FULL
Interface : vlan-10        Designated Router : 10.10.10.3
Area : backbone           Backup Designated Router : 10.10.10.2
Priority : 1               Retransmit Queue Length : 0
Options : 0               Neighbor Uptime : 0h:0m:32s
Events : 6                Dead Timer Expires : 32 sec
```

Figure 75. Example of Displaying OSPF Neighbor Timers

- **Enhancement (PR_0000054183)** — The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses.

IP Enable/Disable for All VLANs

This enhancement allows you to administratively disable the IP address on specified VLANs with static IP addresses without removing the Layer 3 configuration. The switch can be pre-configured as a backup router, then quickly transition from backup to active by re-enabling Layer 3 routing on one or more VLANs. While the switch is in “backup” mode, it will still performing Layer 2 switching.

A MIB object will be toggled to make Layer 3 routing active or inactive on a VLAN.

Interaction with Other Features

The feature affects management access to the switch as follows:

- IP—SNMP, Telnet, SSH, HTTP, TFTP, SCP, SFTP
- Routing—RIP, OSPF, PIM, VRRP

When the **disable layer3** command is configured on a VLAN, the behavior is as if no IP address were configured for that VLAN. There is no other change in behavior.

Syntax: [no] disable layer3 vlan <vid | range of vids>

In config context, turns off Layer 3 routing for the specified VLAN or VLANs. When executed in vlan context, turns off Layer 3 routing for that VLAN.

*The **no** form turns on Layer 3 routing for the specified VLAN or VLANs.*

*If QinQ is enabled, **svlan** can be configured as well.*

The **show ip** command displays “disabled” in the IP Config column if Layer 3 has been disabled, or if the VLAN has no IP configuration. You can tell which is the case by viewing the remaining columns; if there is no IP configuration, the remaining columns are blank.

```
ProCurve(config)# show ip

Internet (IP) Service

  IP Routing : Disabled

Default Gateway : 172.22.16.1
Default TTL     : 64
Arp Age        : 20
Domain Suffix   :
DNS server      :

VLAN            | IP Config | IP Address | Subnet Mask | Proxy ARP
-----+-----+-----+-----+-----
DEFAULT_VLAN    | DHCP/Bootp | 172.22.18.100 | 255.255.248.0 | No No
VLAN3           | Disabled  | 172.17.17.17  | 255.255.255.0 | No No
VLAN6           | Disabled  |               |               | 
VLAN7           | Manual    | 10.7.7.1      | 255.255.255.0 | No No
```

Figure 76. Example of VLAN Disabled for Layer 3

For IPv6, the “Layer 3 Status” field displays the status of Layer 3 on that VLAN.

```
ProCurve(config)# show ipv6

Internet (IPv6) Service

IPv6 Routing      : Disabled
Default Gateway   :
ND DAD            : Enabled
DAD Attempts      : 3

Vlan Name         : DEFAULT_VLAN
IPv6 Status       : Disabled
Layer 3 Status    : Enabled

Vlan Name         : layer3_off_vlan
IPv6 Status       : Disabled
Layer 3 Status    : Disabled

Address          |                               Address
Origin           | IPv6 Address/Prefix Length    Status
-----+-----
manual           | abcd::1234/32                 tentative
autoconfig       | fe80::218:71ff:febd:ee00/64   tentative
```

Figure 77. Example of IPv6 Layer 3 Status for a VLAN

Interactions with DHCP

Disabling Layer 3 functionality and DHCP are mutually exclusive, with DHCP taking precedence over **disable layer3** on a VLAN. The following interactions occur:

- If the **disable layer3** command is executed when DHCP is already configured, no disabling of the VLAN occurs. This error message displays —“Layer 3 cannot be disabled on a VLAN that has DHCP enabled.”
- From the CLI: If **disable layer3** is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set. The warning message displays— “Layer 3 has also been enabled on this VLAN since it is required for DHCP.”
- From the CLI: When disabling a range of VLAN IDs, this warning message displays— “Layer 3 will not be disabled for any LANs that have DHCP enabled.”
- From SNMP: If the **disable layer3** command is executed when DHCP is already configured, no disabling of the VLAN occurs. An INCONSISTENT_VALUE error is returned.
- From SNMP: If **disable layer3** is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set.

- **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries.

Logging for Routing ACLs

This feature will provide functionality for logging ACL “permit” entries in the same manner that ACL “deny” entries are currently logged.

Operating Notes

- Affects only ACLs that are statically configured using the CLI command interface.
- Existing ACL logging for “deny” entries does not change
- A detailed event will be logged for the first packet that matches a “permit” or “deny” ACL logged entry with the appropriate action specified.

- Subsequent packets matching ACL logged entries will generate a new event that summarizes the number of packets that matched each specific entry (with the time period), for example:

```
Mar 1 10:01:01 10.10.20.1 ACL:
ACL 03/01/10 10:01:01: ACL NO-TELNET seq#10 permitted 6 packets
```

- Events are logged as specified by the **debug <destination>** command.
- Events are only logged when ACL logging is enabled using the **debug acl** command. This feature should only be used to troubleshoot and verify ACL configurations as it can impact switch performance even when ACL debugging is disabled.

Standard ACLs

The following abbreviated syntax is for standard, named ACLs. See the chapter “IPv4 Access Control Lists (ACLs)” in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list standard < name-str >

*Places the CLI in the “Named ACL” (**nacl**) context specified by the < name-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*

< name-str >: Specifies an identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “**Accounting ACL**”.

< deny | permit >

< any | host < SA > | SA <mask | SA/mask-length >> [log]

*Executing this command appends the ACE to the end of the list of ACEs in the current ACL. In the default ACL configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.*

SA=Source Address

Note: To insert a new ACE between two existing ACEs, precede **deny** or **permit** with an appropriate sequence number.

< deny | permit >

*For named ACLs, used in the “Named ACL” (**nacl**) context to configure an ACE. Specifies whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

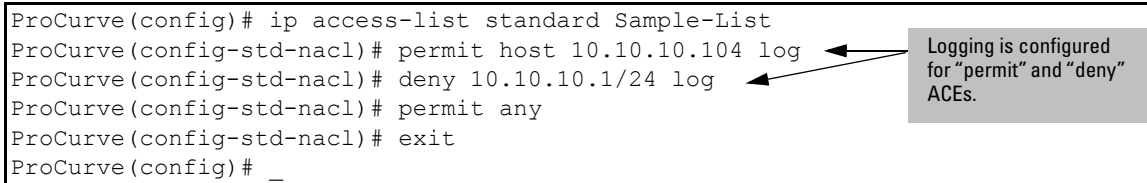
[log]

This option generates an ACL log message if:

- There is a match.
- ACL logging is enabled on the switch.

*(Use the debug command to direct ACL logging output to the current console session and/or to a Syslog server. Note that you must also use the **logging < ip-addr >** command to specify the addresses of Syslog servers to which you want log messages sent.*


```
ProCurve(config)# ip access-list standard Sample-List
ProCurve(config-std-nacl)# permit host 10.10.10.104 log
ProCurve(config-std-nacl)# deny 10.10.10.1/24 log
ProCurve(config-std-nacl)# permit any
ProCurve(config-std-nacl)# exit
ProCurve(config)# _
```



Logging is configured for "permit" and "deny" ACEs.

Figure 78. Example of Standard ACL showing the log Option configured for both "permit" and "deny" ACEs

Extended ACLs

The following abbreviated syntax is for extended, named ACLs. See the chapter "IPv4 Access Control Lists (ACLs)" in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list extended < name-str >

Places the CLI in the "Named ACL" (nacl) context specified by the < name-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.

< name-str >: Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: "Accounting ACL". You can also use this command to access an existing, numbered ACL.

Syntax: < deny | permit > < ip | ip-protocol | ip-protocol-nbr >
(nacl < any | host < SA > | SA / mask-length | SA < mask > >
context) < any | host < DA > | DA / mask-length | DA < mask > >
[precedence] [tos] [log]

*Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.*

SA=Source Address

DA=Destination Address

Note: *To insert a new ACE between two existing ACEs in an extended, named ACL, precede **deny** or **permit** with an appropriate sequence number along with the ACE keywords and variables you want.*

For a match to occur, a packet must have the source and destination addressing criteria specified in the ACE, as well as:

- *the protocol-specific criteria configured in the ACE, including any included, optional elements (described later in this section)*
- *any (optional) precedence and/or ToS settings configured in the ACE.*

< deny | permit >

*For named ACLs, these keywords are used in the “Named ACL” (**nacl**) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option can be used after the DA to generate an Event Log message if:

- *There is a match.*
- *ACL logging is enabled.*

```
ProCurve(config)# ip access-list extended Extended-List-01
ProCurve(config-ext-nacl)# permit tcp host 10.10.10.44 host
10.10.20.78 eq telnet
ProCurve(config-ext-nacl)# deny ip 10.10.10.1/24 10.10.20.1/24
ProCurve(config-ext-nacl)# permit ip 10.10.10.2/24 log
ProCurve(config-ext-nacl)# exit
ProCurve(config)# vlan 10 ip access-group Extended-List in
```

Logging is configured
for “permit” ACE.

Figure 79. Example of Standard ACL showing the log Option configured for a “permit” ACE

IPv6 Access Lists

The following abbreviated syntax is for IPv6, named ACLs. See the chapter “IPv6 Access Control Lists (ACLs)” in the *IPv6 Configuration Guide* for your switch for more details about IPv6 ACLs.

Syntax: `ipv6 access-list < ascii-str >`

*Places the CLI in the IPv6 ACL (**ipv6-acl**) context specified by the < ascii-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*

< ascii-str >: Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “Accounting ACL”. You can also use this command to access an existing ACL.

Syntax: `< deny | permit > < ipv6 | ipv6-protocol | ipv6-protocol-nbr >
(ipv6 acl context) < any | host < SA > | SA/ prefix-length >
< any | host < DA > | DA/ prefix-length >
[dscp < tos-bits | precedence] [log]`

*Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.*

SA=Source Address

DA=Destination Address

Note: *To insert a new ACE between two existing ACEs in an ACL, precede **deny** or **permit** with an appropriate sequence number.*

For a match to occur, a packet must have the source and destination IPv6 addressing criteria specified in the ACE, as well as:

- the protocol-specific criteria configured in the ACE, including any optional elements (described later in this section)*
- any (optional) DSCP settings configured in the ACE*

`< deny | permit >`

*These keywords are used in the IPv6 (**ipv6-acl**) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option can be used after the DA to generate an Event Log message if:

- *There is a match.*
- *ACL logging is enabled.*

For a given ACE, if **log** is used, it must be the last keyword entered.

```
Port-1(config)# show access-list config

ipv6 access-list "Test-01"
 10 permit ipv6 2001:db8::1:10:10/128 ::/0 log
 20 deny tcp 2001:db8::1:20:0/121 2001:db8::1:10:3/128 eq 23 log
 30 deny ipv6 2001:db8::1:20:0/121 2001:db8::1:10:4/128 log
 40 deny tcp 2001:db8::1:30:0/121 2001:db8::1:10:4/128 eq 23 log
 50 deny ipv6 2001:db8::1:30:0/121 2001:db8::1:10:3/128
 60 deny icmp ::/0 ::/0 133
 70 permit ipv6 ::/0 ::/0
exit
```

Logging is configured for "permit" and "deny" ACEs.

Figure 80. Example of Standard ACL showing the log Option configured for "permit" and "deny" ACEs

- **Enhancement (PR_0000058115)** — Allows the use of TCP/UDP source and destination port number for trunk load balancing.

Trunk Load Balancing Using L4 Ports

This enhancement allows the use of TCP/UDP source and destination port number for trunk load balancing. This is in addition to the current use of source and destination IP address and MAC addresses. Configuration of Layer 4 load balancing would apply to all trunks on the switch. Only non-fragmented packets will have their TCP/UDP port number used by load balancing. This ensures that all frames associated with a fragmented IP packet are sent through the same trunk on the same physical link.

The priority for using Layer 4 packets when this feature is enabled is as follows:

1. If the packet protocol is an IP packet and has Layer 4 port information, use Layer 4.
2. If the packet protocol is an IP packet and does not have Layer 4 information, use Layer 3 information.
3. If the packet is not an IP packet, use Layer 2 information.

Enabling L4-based Trunk Load Balancing

Enter the following command with the **L4-based** option to enable load balancing on Layer 4 information when it is present.

Syntax: trunk-load-balance <L3-based | L4-based>

*When the **L4-based** option is configured, enables load balancing based on Layer 4 information if it is present. If it is not present, Layer 3 information is used if present; if Layer 3 information is not present, Layer 2 information is used. The configuration is executed in global configuration context and applies to the entire switch.*

Default: L3-based load balancing

<L3-based>: Load balance on Layer 3 information if present, or Layer 2 information.

<L4-based>: Load balance on Layer 4 port information if present, or Layer 3 if present, or Layer 2.

```
HPswitch(config)# trunk-load-balance L4-based
```

Figure 81. Example of Enabling L4-based Trunk Load Balancing

```
HPswitch(config)# show trunk

Load Balancing Method: L4-based, L2-based if non-IP traffic

  Port | Name                                     Type      | Group  Type
  ---- + -
  41    |                                     100/1000T | Trk1   Trunk
  42    |                                     100/1000T | Trk1   Trunk
```

Figure 82. Example of Output When L4-based Trunk Load Balancing is Enabled

```

HPswitch(config) # show running-config

Running configuration:

; J9091A Configuration Editor; Created on release #K.15.02.0001x

hostname "Switch"
module 1 type J8702A
module 5 type J9051A
module 7 type J8705A
module 10 type J8708A
module 12 type J8702A
trunk-load-balance L4-based
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A24,G1-G24,J1-J4,L1-L24
    ip address dhcp-bootp
    tagged EUP
    no untagged EDP
    exit
snmp-server community "public" unrestricted

```

If L4 trunk load balancing is enabled, a line appears in the running-config file. If it is not enabled, nothing appears as this is the default and the default values are not displayed.

Figure 83. Example of Running Config File when L4-based Trunk Load Balancing is Enabled

- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs.

Wake-on-LAN Support Across VLANs

Wake-on-LAN is an Ethernet networking standard that allows a computer to be awakened by a network message, referred to as a “magic packet”. The packet is typically sent by a remote server to systems that are enabled to respond to these packets. This allows network administrators to troubleshoot or perform maintenance with minimal or no user intervention, even if the computers are turned off.

Wake-on-LAN commonly uses a broadcast address on UDP port 7 or port 9. The Layer 3 switches or routers must be configured to allow the broadcast packets, known as “directed broadcasts”. HP switches currently support directed broadcasts at the global switch level. This enhancement allows the configuration of directed broadcasts on a specific VLAN. An ACL can be configured to limit the Wake-on-LAN traffic to a specific subnet. This limits the servers that can send Wake-on-LAN packets, which helps prevent Denial-of-Service smurf attacks on the network.

The **ip directed-broadcast** command executed in VLAN context allows the configuration of Wake-on-LAN for a specific VLAN. Enabling directed broadcasts on an interface supersedes globally disabled directed broadcasts.

Syntax: [no] ip directed-broadcast

Enables or disables directed broadcast forwarding. Must be executed in VLAN context.

An example Wake-on-LAN configuration is shown in the following figure.

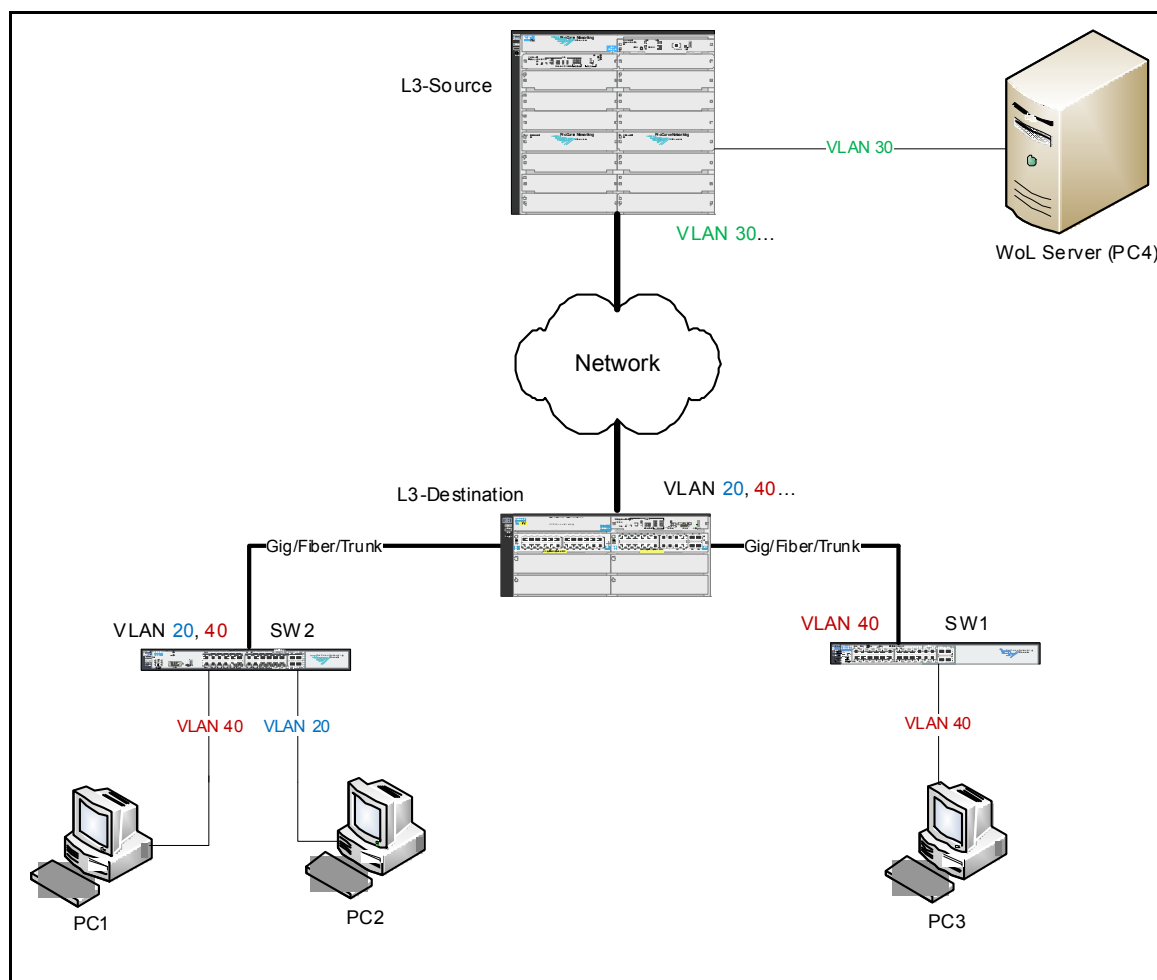


Figure 84. Example of Wake-on-LAN Configuration

In the example shown in [Figure 84](#):

- PC1, PC2 and PC3 are the client PCs that need to be awakened.
- PC4 is the Wake on LAN (WoL) server. This PC can also be the DHCP server with IP scopes for each of the VLANs (20, 30, 40). In this example the IP addresses are 172.168.20.1/24, 172.168.30.1/24 and 172.168.40.1/24, respectively.
- The WoL server is configured with a static IP address of 172.168.30.2/24.
- SW1 and SW2 are Layer 2 switches.
- L3-Source and L3-Destination are Layer 3 switches.

The configuration steps for the Layer 3-Destination switch are shown in [Figure 85](#).

```

HP Destination Switch(config)# ip routing
Enable routing.

Create ACL for VLAN 20, allow traffic on UDP port 7 only from WoL server.

HP Destination Switch(config)# ip access-list extended VLAN_20
HP Destination Switch(config-ext-nacl)# permit udp host 172.168.30.2 host
172.168.20.255 eq 7

Deny any other directed-broadcast traffic on this subnet.
HP Destination Switch(config-ext-nacl)# deny ip any 172.168.20.255/24
HP Destination Switch(config-ext-nacl)# permit ip any any
HP Destination Switch(config-ext-nacl)# exit

Create ACL for VLAN 40, allow traffic on UDP port 7 only from WoL server.

HP Destination Switch(config)# ip access-list extended VLAN_40
HP Destination Switch(config-ext-nacl)# permit udp host 172.168.30.2 host
172.168.40.255 eq 7

Deny any other directed-broadcast traffic on this subnet.
HP Destination Switch(config-ext-nacl)# deny ip any 172.168.40.255/24
HP Destination Switch(config-ext-nacl)# permit ip any any
HP Destination Switch(config-ext-nacl)# exit

Configure VLAN 20; enable directed-broadcast.

HP Destination Switch(config)# vlan 20
HP Destination Switch(vlan-20)# ip address 172.168.20.1/24
HP Destination Switch(vlan-20)# ip helper-address 172.168.30.2
HP Destination Switch(vlan-20)# ip directed-broadcast
HP Destination Switch(vlan-20)# ip access-group VLAN_20 out
HP Destination Switch(vlan-20)# exit

Configure VLAN 40; enable directed-broadcast.

HP Destination Switch(config)# vlan 40
HP Destination Switch(vlan-20)# ip address 172.168.40.1/24
HP Destination Switch(vlan-20)# ip helper-address 172.168.30.2
HP Destination Switch(vlan-20)# ip directed-broadcast
HP Destination Switch(vlan-20)# ip access-group VLAN_40 out
HP Destination Switch(vlan-20)# exit

Configure trunks, assign ports/trunks to VLANs, establish route to VLAN 30. Not shown in this example.

HP Destination Switch(config)# write memory

```

Figure 85. Example Configuration for the Destination Switch

The configuration steps for the Layer 3-Source switch are shown in [Figure 86](#).


```
HP Source Switch(config)# ip routing
```

Enable routing.

Configure VLAN 30. The WoL server is on this VLAN.

```
HP Source Switch(config)# vlan 30
HP Source Switch(vlan-30)# ip address 172.168.30.1/24
HP Source Switch(vlan-30)# exit
```

Configure trunks, assign ports/trunks to VLANs, establish route to VLANs 20 and 40. Not shown in this example.

```
HP Source Switch(config)# write memory
```

Figure 86. Example Configuration for the Source Switch

Displaying the Configuration for Directed-Broadcast

The **show running-config** command displays the configured information.

```
HP Switch(config)# show running-config

Running configuration:

: JXXXXA Configuration Editor; Created on release #K.XX.XX

hostname "ProCurve Switch
ip access-list extend "VLAN_20"
  10 permit udp 172.168.30.2 0.0.0.0 172.168.20.255 0.0.0.0 eq 7
  20 deny ip 0.0.0.0. 255.255.255.255 172.168.20.255 0.0.0.255
  30 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  exit
ip access-list extended "VLAN_40"
  10 permit udp 172.168.30.2 0.0.0.0 172.168.40.255 0.0.0.0 eq 7
  20 deny ip 0.0.0.0. 255.255.255.255 172.168.40.255 0.0.0.255
  30 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  exit
module 1 type JXXXXA
module 3 type JXXXXA
  ip routing
  ip udp-bcast-forward
  vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24, A1-A4
    ip address dhcp-bootp
    exit
  vlan 20
    ip helper-address 172.168.30.2
    ip address 172.168.20.1 255.255.255.0
    ip access-group "VLAN_20" out
    ip directed-broadcast
    exit
  vlan 40
    ip helper-address 172.168.30.2
    ip address 172.168.40.1 255.255.255.0
    ip access-group "VLAN_40" out
    ip directed-broadcast
    exit
snmp-server community "public" unrestricted
no autorun
```

Figure 87. Output of show running-config Command for the Configured Example

- **Enhancement (PR_0000058564)** — Adds the ability to send syslog messages via TCP.

Syslog via TCP

This enhancement provides TCP as a transport protocol option for delivering logging messages to the syslog server. Because TCP is a connection-oriented protocol, a connection must be present before the logging information is sent. This helps ensure that the logging message will reach the syslog server.

Each configured syslog server needs its own connection. You can configure the destination port that is used for the transmission of the logging messages.

Syntax: [no] logging <ip-addr> [udp <1024-49151> | tcp <1024-49151>]

Allows the configuration of the UDP or TCP transport protocol for the transmission of logging messages to a syslog server.

Specifying a destination port with UDP or TCP is optional.

*Default ports: UDP port is 514
TCP port is 1470*

Default Transport Protocol: UDP

Examples

```
HPswitch(config)# logging 192.123.4.5 tcp
```

Default TCP port 1470 is used.

Figure 88. Example of Configuring TCP for Logging Message Transmission Using the Default Port

```
HPswitch(config)# logging 192.123.4.5 tcp 9514
```

TCP port 9514 is used.

Figure 89. Example of Configuring TCP for Logging Message Transmission Using a Specified Port

```
HPswitch(config)# logging 192.123.4.5 udp
```

Default UDP port 514 is used.

Figure 90. Example of Configuring UDP for Logging Message Transmission Using the Default Port

```
HPswitch(config)# logging 192.123.4.5 udp 9512
```

UDP port 9512 is used.

Figure 91. Example of Configuring UDP for Logging Message Transmission Using a Specified Port

- **Enhancement (PR_0000058798)** — Adds the ability to enable an SNMP trap for any configuration change made in the switch's running configuration file.

SNMP Trap on Running Configuration Changes

This enhancement provides the functionality for sending a specific SNMP trap for any configuration change made in the switch's running configuration file. The trap will be generated for changes made from any of these interfaces:

- CLI
- Menu
- WebAgent (Web UI)
- SNMP (remote SNMP set requests).

The SNMP trap will contain the following information.

Information	Description
Event ID	An assigned number that identifies a specific running configuration change event.
Method	Method by which the change was made—CLI, Menu, WebAgent, or remote SNMP. For configuration changes triggered by internal events, the term "Internal-Event" is used as the source of the change.
IP Address Type	Indicates the source address type of the network agent that made a change. This is set to an address type of unknown when not applicable.
IP address	IP address of the remote system from which a user accessed the switch. If not applicable, this is an empty string and nothing is displayed, for example, if access is through a management console port.
User Name	User name of the person who made the change. Null if not applicable.
Date and Time	Date and time the change was made.

The SNMP trap alerts any interested parties that someone has changed the switch's configuration and provides information about the source for that change. It does not specify what has been changed.

Enabling Running Configuration Change SNMP Traps

The following command is used to enable SNMP traps for this feature.

Syntax: [no] snmp-server enable traps running-config-change [transmission-interval <0-4294967295>]

Enabled SNMP traps being sent when changes to the running configuration file are made.

Default: Disabled

transmission-interval <0-2147483647>: Controls the egress rate for generating SNMP traps for the running configuration file. The value configured specifies the time interval in seconds that is allowed between the transmission of two consecutive traps. All running configuration change events that occur within the specified interval will not generate SNMP traps, although they will be logged in the Configuration Changes History Table.

A value of 0 (zero) means there is no limit; traps can be sent for every running configuration change event.

Default: Zero.

Displaying Configuration File Change Information

The **changes-history** parameter is added to the existing **show running-config** command to display the history information for changes occurring to the running configuration file.

Syntax: show running-config [changes-history [1-32]] [detail]

Displays the history up to 32 events for changes made to the running-configuration file. The changes are displayed in descending order; the most recent change at the top of the list. You can specify from 1 to 32 entries for display.

*The **detail** option will display a more detailed amount of information for the configuration changes.*

```
HPSwitch(config)# show running-config changes-history

Running Config Last Changed      : 02/19/10 16:30:09
Number of Changes Since Reboot  : 150086
```

Event ID	Config Method	Date	Time
150086	CLI	02/19/10	16:30:09
150085	SNMP	02/03/10	14:50:12
150084	SNMP	02/03/10	14:50:12
150083	SNMP	02/03/10	14:45:59
150082	SNMP	02/03/10	14:27:15
150081	SNMP	02/03/10	13:11:00
150080	SNMP	02/03/10	13:11:00
150079	CLI	01/18/10	09:09:17

Figure 92. Example of Output for Running Configuration Changes History for All Ports

```
HPswitch(config)# show running-config changes-history 6

Running Config Last Changed      : 08/04/10 16:35:31
Number of Changes since Reboot  : 120
```

Event ID	Config Method	Date	Time
120	CLI	08/04/10	16:35:31
119	CLI	08/04/10	16:34:01
118	SNMP	08/04/10	15:32:22
117	WEBUI	08/03/10	12:55:21
116	MENU	07/01/10	01:45:26
115	CLI	06/23/10	11:34:23

Figure 93. Example of Output for Running Configuration Changes History

[Figure 94](#) and [Figure 95](#) display detailed information for configuration changes history.

```
HPswitch(config)# show running-config changes-history 3 detail

Event ID      : 120
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : CLI
Date          : 08/04/10
Time          : 16:35:31

Event ID      : 119
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : CLI
Date          : 08/04/10
Time          : 16:34:01

Event ID      : 118
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : SNMP
Date          : 08/04/10
Time          : 15:32:22
```

Figure 94. Example of Detailed Output for Running Configuration Changes History

```
HPswitch(config)# show running-config changes-history detail

Running Config Last Changed: 01/01/90 00:35:44
Number of changes since last boot : 6

Event ID      : 6
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:44

Event ID      : 5
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:39

Event ID      : 4
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:33

Event ID      : 3
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:27
```

Figure 95. Example of Output for Running Config Changes History with Detail

[Figure 96](#) displays the current status (enabled/disabled) of the SNMP trap type for running-configuration changes.

```

HPswitch(config)# show snmp-server traps

Trap Receivers

Link-Change Traps Enabled on Ports [All] : All

Traps Category                Current Status
-----
SNMP Authentication           : Enabled
Password change                : Enabled
Login failures                 : Enabled
Port-Security                 : Enabled
Authorization Server Contact   : Enabled
DHCP-Snooping                 : Enabled
Dynamic ARP Protection         : Enabled
Dynamic IP Lockdown           : Enabled
Running Configuration Changes : Enabled

Address      Community      Events  Type  Retry  Timeout
-----
173.33.25.201 public      None    trap   3      15

Excluded MIBs

```

SNMP trap status for running-config changes is enabled.

Figure 96. Example of SNMP Trap Configuration Status Information

- **Enhancement (PR_0000058804)** — Allows the redistribution into RIP of static blackhole or reject routes.

Static Summary Route to RIP

Overview

This enhancement allows the redistribution into RIP of static blackhole or reject routes. Blackhole or reject route redistribution can be manually enabled using the **redistribute static include-all** command.

Note

Reject routes are null routes configured to drop traffic for the device at the configured address and return an ICMP error message. Blackhole routes are null routes that silently drop traffic for the configured network.

Redistributing Static Reject and Blackhole Routes

The static configuration of blackhole and reject routes is configured with the existing command:

```
[no] ip route <dest-ip-address/mask-length> <reject | blackhole>
```

Use the **include-all** parameter in the following command to enable redistribution of static reject and blackhole routes. The **include-all** option operates in conjunction with any other statically configured routes. It does not change the behavior of routes that are excluded from redistribution by the **restrict** option, that is, static blackhole and reject routes will not be redistributed if a matching **restrict** configuration exists.

Syntax: [no] redistribute <static [include-all] | connected | ospf> [route-map <name>]

Enables redistribution of the specified route type to the RIP domain. Executed in RIP context.

static: *Redistribute from manually configured routes.*

include-all: *Enables redistribution of static reject and blackhole routes. Default is disabled.*

connected: *Redistribute from locally connected network(s).*

ospf: *Redistribute from OSPF routes*

route-map <name>: *Optionally specify the name of a route-map to apply during redistribution*

*The **no** form of the command disables redistribution for the specified route type.*

Default: Disabled

```
HPswitch(config)# router rip
HPswitch(rip)# redistribute static include-all
HPswitch(rip)# restrict 11.0.0.0 255.0.0.0
HPswitch(rip)# write mem
HPswitch(rip)# exit
```

Figure 97. Example of Redistributing Static Reject and Blackhole Routes

```
HPswitch(config)# show ip rip redistribute

RIP redistributing

Route type RouteMap      Options
-----
connected  PRNMAP
static     SRVMAP             Includes blackhole
                                   and reject
```

Figure 98. Example of RIP Redistribution Information Including Reject and Blackhole Routes

- **Enhancement (PR_0000060972)** — Enables configuration of RADIUS attributes for downstream supplicant devices. This allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits.

Dynamic Port Access Auth via RADIUS

Overview

In some situations, it is desirable to configure RADIUS attributes for downstream supplicant devices that allow dynamic removal of the 802.1X, MAC, and Web authentication limits on the associated port of the authenticator switch. This eliminates the need to manually reconfigure ports associated with downstream 802.1X-capable devices, and MAC relay devices such as IP phones, on the authenticator switches. When the RADIUS authentication ages out, the authentication limits are dynamically restored. This enhancement allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits. The changes are always applied to the port on the authenticator switch associated with the supplicant being authenticated.

Note

All the changes requested by the VSAs must be valid for the switch configuration. For example, if either MAC-based or Web-based port access is configured while 802.1X port access is in client mode, a RADIUS client with a VSA to change the 802.1X port access to port-based mode is not allowed. 802.1X in port-based mode is not allowed with MAC-based or web-based port access types. However, if the authenticating client has VSAs to disable MAC-based and Web-based authentication in conjunction with changing 802.1X to port-based mode, then client authentication is allowed.

Configuring the RADIUS VSAs

Only RADIUS -authenticated port-access clients will be able to dynamically change the port access settings using the new proprietary RADIUS VSAs. The settings that can be overridden are:

- Client limit (address limit with mac-based port access)
- Disabling the port-access types
- Setting the port mode in which 802.1X is operating

If the VSA client limit decreases the switch's configured client limit, all clients except the client that is overriding the settings is deauthenticated. Only one client session at a time can override the port-access settings on a port. When the client session is deauthenticated, the port resets itself to the configured settings. This port reset causes the deauthentication of all clients for the port-access authentication types that had their settings changed dynamically.

The new VSAs are:

- **HP-Port-Client-Limit-Dot1x:** This VSA temporarily alters the 802.1X authentication client limit to the value contained in the VSA. Values range from 0 to 32 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 10.
- **HP-Port-Client-Limit-MA:** This VSA temporarily alters the MAC authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 11.
- **HP-Port-Client-Limit-WA:** This VSA temporarily alters the Web authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 12.
- **HP-Port-Auth-Mode-Dot1x:** This VSA temporarily alters the 802.1X authentication mode to be either port-based or user-based depending on the value in the VSA. A port-based VSA is set with a value of 1; a user-based VSA is set with a value of 2. This is an HP proprietary VSA with a value of 13.
- If an 802.1X port is operating in port-based mode, it is invalid to set the 802.1X client limit using the HP-Port-Client-Limit VSA.

Note

The changing of the client limits for a port using VSAs is temporary. The running configuration file is not changed and still displays the client limit and address limit settings.

Each authentication type may have a unique value for the client limit. If the value of the VSA is zero, the authentication type corresponding to that VSA will be disabled.

Settings for these VSAs are in effect for the duration of the authenticated session of the downstream supplicant switch. If for any reason there is a loss of the session (link loss between authenticator switch and supplicant switch, or authentication failure during reauthentication), the originally configured 802.1X and MAC authentication limits are restored.

Displaying the Port-access Information

The **show port-access summary** command displays the dynamically changed client limit settings.

Syntax: show port-access summary [radius-overridden]

Displays summary configuration information for all ports, including the ports that have client limits set by RADIUS VSAs.

radius-overridden: *Displays only the ports with client limits that are overridden by RADIUS attributes.*

Note

If the command **no aaa port-access authentication <port-list> client-limit** is executed, the port access is in port-mode. If the 802.1X client-limit is configured with a value from 1-32, the port access is in user-mode.

```
HPswitch(config)# show port-access summary

Port Access Status Summary

Port-access authenticator activated [No] : No
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Note: * indicates values dynamically overridden by RADIUS
```

Port	Authenticator		Web Auth		MAC Auth	
	Enabled	Mode Limit	Enabled	Limit	Enabled	Limit
1	Yes	user* 1*	Yes	1	Yes	1
2	Yes	user 32	Yes	32*	Yes	32
3	Yes	port 1	No	1	No	1
4	No	port 1	No	1	No*	1

Figure 99. Example of Summary Configuration Information Showing RADIUS Overridden Client Limits

To display the configuration information for just those ports that are dynamically overridden by RADIUS attributes, use the **show port-access summary radius-overridden** command.

```
HPswitch(config)# show port-access summary radius-overridden

Port Access Status Summary

Port-access authenticator activated [No] : No
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Note: * indicates values dynamically overridden by RADIUS
```

Port	Authenticator		Web Auth		MAC Auth	
	Enabled	Mode Limit	Enabled	Limit	Enabled	Limit
1	Yes	user* 1*	Yes	1	Yes	1
2	Yes	user 32	Yes	32*	Yes	32
4	No	port 1	No	1	No*	1

Figure 100. Example of Output for Client-limit Values that are RADIUS Overridden

Operating Notes

- Only RADIUS authentication supports the new VSAs. Other authentication types, such as TACACS, are not supported.
- The new VSAs are not supported in IDM and they cannot be specified in the configurations. The new VSAs must be configured manually.
- If the RADIUS server delivers a new VSA to an authenticator switch that does not understand it, the Access-Accept message is rejected.

Software Fixes

Note

Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

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

For software fixes in prior versions (K.14.*xxx* or earlier), see the Release Notes provided with those versions.

Version K.15.01.0031

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

The following problems were resolved in software version K.15.01.0031.

- **802.1X (PR_0000047025)** — After the switch reboots and before IP communication is initialized, the switch accepts authentication requests from 802.1X clients. Because the switch cannot communicate with the RADIUS server yet, it sends EAP-Failure notifications to the client, which causes client authentication to fail.
- **ACL/QoS (PR_0000045616)** — ACL/QOS Error return definitions as measured by the hardware layer are out-of-synch with SNMP values.
- **ACLs (PR_0000045003)** — Updated IPv6 rules for IDM ACLs.
- **Authentication (PR_0000043924)** — The switch responds with invalid PEAP packets when the RADIUS server request includes optional EAP TLVs, resulting in authentication failure.
- **Banner MOTD (PR_0000042871)** — The message returned by the CLI in response to the banner MOTD configuration command erroneously states that a banner of up to 3071 characters is supported; the actual maximum number of characters is 3070.
- **CLI (PR_0000009814)** — When an attempt is made to configure a mirror or monitor port for a 10-GbE transceiver not present in the switch, the error message is vague (`invalid value`). This fix provides a more meaningful error message.
- **CLI (PR_0000044704)** — The switch does not properly adjust terminal size display, if the user telnets to the switch and then changes the terminal size. This can cause the username to display when the password is requested, instead of a blank field.
- **CLI (PR_0000045556)** — Mesh ports cannot be configured to mirror or monitor. For example, when issuing the CLI command `int mesh monitor`, the switch reports: `Unknown port type`.
- **CLI (PR_0000047545)** — The CLI command `no telnet-server` is not saved in the config file.
- **CLI (PR_0000049955)** — The output of `show tech route` does not include all the information it is intended to provide.
- **CLI (PR_0000050078)** — When a PoE power supply is hot-swapped into a Switch 5400zl or 8200zl, the output of the CLI command `show system power` always lists the power supply as being 120 V, 875 W, even if it is a different voltage/wattage power supply.

- **CLI (PR_0000050088)** — If the user removes an interface module from the switch configuration (for example with the command, **no module 1**), an SNMP link-change trap configuration for ports on that module is truncated instead of removed from the configuration. For example, the configuration **no snmp-server enable traps link-change A1-A2** is truncated to **no snmp-server enable traps link-change**, which is an invalid configuration. If the user saves that configuration to a server, the config file cannot be successfully downloaded to the switch because of the incomplete command.

- **CLI Help (PR_0000046320)** — AAA command in-line help lists the options even after an option has already been typed into that command.

```
ProCurve Switch 3500yl-48G(config)# aaa authentication port-access chap-radius server-group pat cached-reauth ?
```

```
none          Do not use backup authentication methods.
authorized    Allow access without authentication.
cached-reauth Grant access in case of reauthentication retaining the current
              session attributes.
```

```
<cr>
```

The options should not be displayed, since an option (in this case, **cached-reauth**) has already been typed in the command line.

- **Command Authorization (PR_0000043525)** — HP-Command-String authorization does not work as expected.
- **Config (PR_0000040782)** — When an HP ProCurve Gigabit 1000Base-T Mini-GBIC (J8177C) is configured with the **speed-duplex auto-100** setting, that configuration is lost from both running and startup configurations after a switch reload.
- **Config (PR_0000043984)** — The switch allows an inherent configuration conflict; the **rate-limit** and **service-policy** parameters should not be allowed concurrently on an interface.
- **Config (PR_0000046578)** — An IP BOOTP gateway configured on subnet zero is not displayed in the startup or running configuration file. The gateway is used correctly by the switch; this is a configuration display issue only.
- **Console Connectivity (PR_0000042248)** — The console port on a switch may get into a state where it appears to be unresponsive.
- **COS (PR_0000046599)** — The switch reports incorrect Class Of Service (COS) information in the output of the command **show port-access auth <port>** when the default COS (value 255) is in effect.
- **Crash (PR_0000018180)** — The switch may reboot unexpectedly during PIM-SM configuration and display a message similar to the following.

```
Software exception at pim_sm_ctrl.c:376 -- in 'mPimsmCtrl'
```

- **Crash (PR_0000040241)** — The switch may reboot unexpectedly with a message similar to the following (message may vary).

```
Software exception at hwBp.c:156 -- in 'mBSRCtrl', task ID = 0x7f06db0
-> MemWatch Trigger: Offending task 'mPimsmCtrl'. Offending IP=0x845580
```

- **Crash (PR_0000041445)** — When Web Authentication is in use, the switch may experience conditions that cause it to reboot unexpectedly with a crash message similar to the following.

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

- **Crash (PR_0000043167)** — When using TFTP with "octet" mode to upload the switch's configuration file, the switch may reboot unexpectedly with a message similar to the following.

```
Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabeb240
-> MemWatch Trigger: Offending task 'tTftpDmn'. Offending IP=0x1cb174
```

- **Crash (PR_0000043217)** — If a VLAN containing a candidate RP is deleted, the switch will reboot unexpectedly, recording a crash message similar to the following.

```
Software exception at vls_util.c:133 -- in 'mBSRCtrl'
```

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

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

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

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

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

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

The switch logs a message similar to the following.

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

- **Crash (PR_0000051910)** — SSH login to the switch might fail, and the switch may reboot unexpectedly with a message similar to the following.

```
NMI event SW:IP=0x00f64f88 MSR:0x02029200 LR:0x00f654dc cr:0x20000000  
sp:0x05337598 xer:0x00000000 Task='tTelnetOut2' Task ID=0xa903000
```

- **DHCP Snooping (PR_0000040580)** — Configuration of trust status for DHCP snooping on ports participating in a dynamic trunk yields undesirable results when the ports of the trunk are removed. This configuration should not be allowed on dynamic trunks (e.g. **dhcp-snooping trust Dyn1**), and this fix enforces that limitation at the CLI with an error message.

- **DHCP Snooping (PR_0000046831)** — The switch forwards DHCP Discovery packets out untrusted ports.

- **DHCP Snooping (PR_0000048426)** — With DHCP Snooping enabled, a client DHCP request is forwarded out untrusted ports.

- **Enhancement (PR_0000011015)** — Cached Re-authentication (Hold State if Radius Server Unavailable). For more information, see [“Enhancements” on page 28](#).

- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link "flapping" rapidly between link-up and link-down states. A new fault event "link-flap" has been created to detect these events. Additionally, a new action, "warn-and-disable," has been created to report and disable the events. Together, these enhancements allow the errant condition to be detected, and the port in question optionally disabled. For more information, see [“Flapping Transceiver Mitigation” on page 28](#).

- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.

- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see the “RADIUS” chapter in the *Access Security Guide* for your switch.
- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. For more information, see [“Enhancements” on page 28](#).
- **Enhancement (PR_0000041472)** — VRRP Ping Virtual IP of Backup. For more information, see the chapter “Virtual Router Redundancy Protocol (VRRP)” in the *Multicast and Routing Guide* for your switch.
- **Enhancement (PR_0000045438)** — The Out Of Band Management (OOBM) port on the HP ProCurve Switch 6600 Series is now enabled for IPv6 host functionality.
- **Enhancement (PR_0000045749)** — Module reload enhancement. For more information, see [“Module Reload \(5400zl and 8200zl switches\)” on page 30](#).
- **Event Log (PR_0000043041)** — When the switch downgrades a port from Gigabit to 10/100 operation, the resulting event log "FFI" message is displayed twice.
- **Fault Finder (PR_0000045772)** — When the switch fault-finder feature is configured to disable a transceiver port in response to link-flapping, and the disable has occurred, fault-finder will no longer properly disable that port following transceiver hot-swap.
- **GVRP (PR_0000012224)** — Changing the GVRP unknown-vlan state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **GVRP (PR_0000040238)** — After a dynamically-learned VLAN is converted to a static port-based VLAN, and an interface is made a static member of that VLAN, disabling GVRP causes the port to lose the VLAN membership. The running-config, startup-config and the SNMP egress static member list for the VLAN show the port as member of the VLAN. All other data shows the port is no longer a member of the VLAN. VLAN communication over the affected interface is no longer possible until the one of the two following workarounds is executed. Workarounds: Either re-issue the tag and untag commands for VLAN port assignment, or reload the system.
- **GVRP (PR_0000040758)** — Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs).
- **IGMP (PR_0000018494)** — IGMP joins may cause multicast streams to flood, briefly, across the VLAN.
- **IP Communication (PR_0000043121)** — Execution and subsequent interruption of the CLI command **show tech route** during a vulnerability scan negatively affects IP communication.
- **IP Communication (PR_0000044004)** — Switches may experience a self-limiting resource leak in ICMP.
- **IPv6 (PR_0000045773)** — IPv6 duplicate address detection (DAD) does not work properly in some topologies.
- **LLDP (PR_0000048124)** — The LLDP Port VLAN ID TLV is incorrectly advertised as 0 for Trunked ports.
- **LLDP-MED (PR_0000050798)** — In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.
- **Management (PR_0000016049)** — If a console or telnet session to the switch is used to execute a CLI command (for example, execution of the **show tech** command) and then the management session is abandoned before the task is completed (e.g., the window is closed), that session becomes unresponsive. If, at that point, another management session is established and the CLI command **kill** is executed to end the initial, now unresponsive session, the new management session will become unresponsive as well, until all sessions are in use and unresponsive.
- **Mini-GBIC (PR_0000044130)** — The HP ProCurve Gigabit-SX-LC Mini-GBIC (J4858C) does not transmit after a switch reboot or hot-swap when it is used in a dual-personality port.

- **Module Crash (PR_0000043280)** — With IP routing and QinQ enabled, a switch module may reboot unexpectedly with a message similar to the following.

00374 chassis: Ports C: Lost Communications detected - Heart Beat Lost

- **MSTP/QinQ (PR_0000041219)** — When QinQ (Provider Bridging) is operating in mixed mode, switch identification of S-VLANs (Service VLANs) and C-VLANs (Customer VLANs) may be sometimes inaccurate. As a result, the switch allows S-VLANs to be assigned as members of MSTP instances and disallows some C-VLANs from being properly assigned to an MSTP instance.
- **Multicast (PR_0000041104)** — A software flaw was found which may have resulted in a variety of unexpected behaviors.
- **PC Phone/Authentication (PR_0000038652)** — When an IP phone is connected in tandem with a PC, the switch would not allow the PC user to be in an unauthenticated VLAN or authenticate using 802.1X, Web auth, or MAC authentication.
- **PIM (PR_0000012391)** — When OSPF, IGMP, and PIM are all configured, the switch reaches a sustained or increasing level of greater than 50% CPU utilization when a multicast stream with TTL=1 is received.
- **PIM (PR_0000018504)** — When a multicast stream is flowing through a PIM network using a better path (as determined by the DR) than the one through the rendezvous point, PIM does not adjust the multicast stream properly (it stops flowing) when PIM gets disabled on a VLAN along the data path.
- **PIM (PR_0000040412)** — When software is routing multicast packets, the packets are sent as CPU originated packets. As a result, features that rely on knowing the inbound source port (e.g., source port filtering) do not get applied.
- **PIM (PR_0000041887)** — When a PIM router is the elected Bootstrap Router (BSR), then fails a future BSR election, it keeps stale candidate Rendezvous Point (RP) information. If this device later becomes the elected BSR again, this stale information is then included in the BSM packets created by the BSR. This can cause long delays in failovers if the stale information includes RP's which are no longer reachable.
- **PIM (PR_0000043798)** — PIM debug output has the wrong bits set for (*,G) join-prune packets.
- **PIM (PR_0000050672)** — Fragmented PIM packets are not correctly routed by the switch.
- **PIM-SM (PR_0000012262)** — In a topology with a statically configured rendezvous point, a client's initial join will trigger receipt of the multicast stream. However, after leaving and re-joining the group, one of the following will happen.
 - If the multicast stream address is still present in the client's local router's multicast routing table, there is a delay of up to a minute after the IGMP join before the client receives the stream.
 - If the client's local router's multicast routing table has timed-out the multicast stream address, then the stream is never received by the client after it re-joins the group.
- **PIM-SM (PR_0000016110)** — When the DR_Priority option is configured to a value of zero (default priority is 1), the option is no longer included in the hello message as it should be.
- **PIM-SM (PR_0000040618)** — When the last known neighbor on an interface times out, PIM-SM fails to remove the flows which have that interface as the Reverse Path Forward (RPF) to the source. This causes the multicast streams to stop, instead of moving to the Reverse Path Tree (RPT) if possible.
- **PIM-SM (PR_0000040621)** — When information about a multicast group with any source (*,G) is received for downstream interfaces, the outbound list is only modified if it is a new *,G; it needs to be about to modify the outbound list for existing groups as well.
- **PIM-SM (PR_0000040825)** — Candidate-Rendezvous Point Advertisement (C-RP-Adv) messages are still sent out after the Candidate RP source-VLAN is down. This results in other PIM routers in the domain continuing to send Register messages to the unavailable RP.

- **PIM-SM (PR_0000041446)** — When a Bootstrap Router (BSR) receives a Candidate-RP Advertisement (C-RP-Adv) with a zero holdtime, it does not send a Bootstrap Message (BSM) with a zero holdtime; instead, it stops including the C-RP in subsequent bootstrap messages.
- **PIM-SM (PR_0000042163)** — Multicast traffic is lost for 20-30 seconds, approximately 5 minutes after a failed-over topology has recovered.
- **PIM-SM (PR_0000042263)** — PIM may send RPT joins or prunes to itself when it is the rendezvous point.
- **PIM-SM (PR_0000042433)** — When a multicast client joins and then leaves a multicast stream, there may be a delay of approximately 20 seconds before that client can join again.
- **PIM-SM (PR_0000042647)** — The PIM bootstrap router (BSR) has a memory leak when static rendezvous points are used.
- **PIM-SM (PR_0000042654)** — PIM may send a join or prune to a device that it inappropriately sees as an upstream neighbor.
- **PIM-SM (PR_0000043801)** — PIM is not sending compound (*,G) Prune (S,G) for SG's not joined.
- **PIM-SM (PR_0000045837)** — Following link failover and failback along the active data path, PIM-SM floods the UDP stream from the source to multiple RP's.
- **PoE (PR_0000045766)** — There are intermittent issues in the support of some pre-standard PoE phones; sometimes phones will boot and sometimes they don't. Grouping four or more phones together in consecutive ports may trigger this issue more often.
- **Port Access (PR_0000017541)** — The switch allows an inherent configuration conflict; port-based 802.1X should not be allowed concurrently with Web and MAC authentication.
- **Port Communication (PR_0000043048)** — The switch will not allow a port to link if the MDIX-MODE is set to MDI or MDIX (only the **auto-MDIX** setting will allow link).
- **Port Connectivity (PR_0000038601)** — The time between a port coming up and that port being online and passing traffic varies, and at times, may be extended to over a minute.
- **QoS (PR_0000042343)** — QoS on Ports may not behave correctly when trunks are involved, e.g., if QoS is configured on a port that is a member of a trunk, the CLI command **no qos** does not disable the feature as it should.
- **RADIUS (PR_0000045092)** — The Radius A/V pair option, 'NAS-IP-Address' does not get populated when the Out of Band Management (OOBM) port is the source of the packet.
- **RADIUS (PR_0000046154)** — MAC Based Radius Sessions go unauthenticated even if cached reauth is enabled when Radius Server Groups are set
- **RADIUS Accounting (PR_0000042522)** — The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.
- **Rate Limiting (PR_0000047195)** — HP ProCurve ONE environment protects the network from non-ONE applications by imposing rate limits on the ONE Services zl module ports. In some cases, a demonstration activation license for a ONE application is not interpreted correctly as a valid ONE activation license and the rate limits are imposed.
- **Redundant Management (PR_0000037617)** — Synchronization of redundant management modules on an 8200zl switch fails if there are more than 2 characters in the minor revision field of the switch system software version.
- **SNMP (PR_0000045869)** — When a large number of SNMPSET commands (on the order of 100 commands) are sent to the switch, at some point the switch runs out of room to store those entries. When the switch's memory limit is reached it gives this error message: "snmp: event 1997; events file too big; record not written." This fix increases the available memory to allow the switch to accept up to 380 SNMPSET commands.

- **SNMP (PR_0000046735)** — Event log messages of type "Info" are sent as traps even after applying the configuration command **snmp-server host <IPaddress> <community> not-info**.
- **SNMP (PR_0000046906)** — Responses to SNMP queries on a switch configured with trunk groups are slow, which can lead to SNMP polling failures.
- **SNTP (PR_0000048717)** — The switch does not ensure the VLAN is up before sending SNTP requests, which can result in SNTP timeouts.
- **SSH (PR_0000014531)** — Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.
- **SSH (PR_0000046860)** — After a client public key is copied to the switch via TFTP, if the user uses SSH to connect to the switch, when the SSH session is closed the switch reboots unexpectedly with a software exception message.
- **STP (PR_0000017189)** — When the switch is running in RSTP-mode (through the use of the CLI configuration command **spanning-tree force-version rstp-operation**) and MSTI settings are still present in the switch, a TCN is triggered when the MSTI settings are modified or removed.
- **TACACS (PR_0000047886)** — When a TACACS server is not available, the switch waits 40 seconds or more before the TACACS request is timed out and the configured secondary authentication method is tried. By default, the timeout should take 5 seconds.
- **Terminal Display (PR_0000008239)** — When a switch telnet session is opened from a Unix/Linux terminal, the line wrap of the terminal is not preserved after logout.
- **TFTP (PR_0000040441)** — When an attempt is made to download a configuration file from the TFTP server, there is an invalid error being logged if the config file does not exist on the TFTP server: `tftp: RCVD error:0, msg:.` Changes have been implemented so that the error message accurately indicates the cause of the file transfer failure.
- **TFTP (PR_0000046063)** — When the management VLAN is changed from the default (VLAN 1), the switch does not respond to TFTP requests.
- **Transceivers (PR_0000045170)** — The J8437A X2-SC LR Optic (transceiver) continues to transmit after the interface is disabled, which causes the far end to think the link is still up.
- **Transceivers (PR_0000045482)** — Some J9152A SFP+ LRM transceivers do not turn on the laser after the switch reboots. *Workaround:* remove, then re-insert the transceiver.
- **UDLD (PR_0000043071)** — UDLD transmits a burst of packets when any port on the switch goes down (1 packet is sent for each port that goes down), falsely triggering a failure state.
- **UDLD (PR_0000047414)** — When UDLD is enabled, communication with the switch might be inconsistent, affecting the switch response to ping, telnet, 802.1X requests, SNMP requests, and SNTP packets.
- **UDLD (PR_0000050402)** — With UDLD enabled, a trunk that uses fiberoptic transceivers stops forwarding traffic after a switch reboot.
- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (unauth-vid) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an unauth-vid for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

Best Practice Tip: 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if

the first packet sent was not 802.1X, then Web- or MAC-auth could be initiated before 802.1X places the user in the unauthenticated VLAN; when Web- or MAC-auth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

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

- Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):
Configuration change denied for port <number>. Only Web or MAC authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please disable Web and MAC authentication on this port using the following commands:

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

no aaa port-access mac-based <PORT-LIST>

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

- Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):
Configuration change denied for port <number>. Only Web or MAC authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please remove the unauthenticated VLAN from 802.1X authentication on this port using the following command:

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

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

- Message 3:
Configuration change denied for port <number>. Only Web or MAC authenticator can have unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port. Please use unauthenticated VLAN for Web or MAC authentication instead.

Event log message when the configuration is changed:

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

- **Unauthenticated VLAN (PR_0000045072)** — An unauthenticated VLAN cannot be configured for 802.1X authentication, when another authentication method is also in use on a port. This fix also adds the **unauth-period** parameter for MAC authentication.
- **VRRP (PR_0000018777)** — In a VRRP topology with two VRRP routers configured as Backup VRRP routers of the same priority, a simultaneous reboot of the two VRRP routers may lead to a situation where no VRRP router becomes the Master. This fix enhances VRRP functionality for skew time implementation as per RFC 3768.
- **VRRP (PR_0000049259)** — In some situations the VRRP Virtual IP does not respond to ping. This fix refines the enhancement introduced with PR_0000041472.

Version K.15.01.0032

Status: Never released.

The following problems were resolved in software version K.15.01.0032.

- **Authentication (PR_0000054821)** — With "mixed port access mode" enabled, a client with valid credentials is authenticated but not authorized on the authorized VLAN.
- **CLI (PR_0000056904)** — The output of the CLI command **show tech** does not include Standby Management Module (SMM) information.
- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used. For more information, see [page 32](#).
- **File Transfer (PR_0000048178)** — While loading switch software via Secure Copy (SCP) or TFTP, the switch can be rebooted by the user before the software file load completes.
- **File Transfer (PR_0000055817)** — During a software update to version K.15.xx, the part of the process that includes a System Support Module (SSM) update fails with the following error message.

```
Updating SSM ...Error on line 20: syntax error.  
Program terminated.
```
- **IPv6 (PR_0000055882)** — After reboot, the switch's IPv6 EUI-64 addresses are changed from the configured values.
- **OSPF (PR_0000054952)** — Default routes in LSAs received from Area Border Routers are not accepted.
- **Spanning Tree (PR_0000056941)** — After a management module failover, ports on the switch might be erroneously blocked by Spanning Tree.
- **VRRP (PR_0000055742)** — If the VRRP advertisement interval is configured to be different than the default value of 1, failover from Active to Standby management module may take 15 seconds.

Version K.15.01.0033

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

The following problems were resolved in software version K.15.01.0033.

- **CLI (PR_0000058300)** — When the active and standby management modules are running different software versions (one boots from software in primary flash, the other boots from software in secondary flash), the output of the CLI command **show redundancy** incorrectly displays redundancy as `Nonstop switching` instead of `Warm-standby`.
- **OSPF (PR_0000057764)** — With OSPF routing and Spanning Tree enabled, if the Spanning Tree path cost is changed to force a specific link to block, the switch might reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
OSPFv3 - Software exception at rt_table.c:4197 -- in 'eRouteCtrl',  
task ID = 0xa968300-> Routing Stack: Assert Failed
```

Version K.15.02.0004

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

The following problems were resolved in software version K.15.02.0004.

- **802.1X (PR_0000038874)** —When using 802.1X in client mode, the command **aaa port-access authenticator 1 client-limit 2** should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.
- **802.1X (PR_0000047205)** — Cached reauthentication does not work with Windows XP running Service Pack 3.
- **Authentication (PR_0000054344)** —The request sent from switch to RADIUS server truncates the username to 16 characters, which causes authentication failure if the username is longer than 16 characters.
- **Authentication (PR_0000058602)** —A client using 802.1X, Web, or MAC authentication might lose access to the network immediately after being authenticated.
- **Banner MOTD (PR_0000053198)** —When using TACACS for telnet authentication, if a banner MOTD is longer than four lines, the first four lines of the banner are not visible on the screen.
- **CDP (PR_0000056202)**— When CDP is disabled with the CLI command **no cdp run**, the switch forwards CDP packets it receives.
- **CLI (PR_0000050756)**— When the user presses "<Ctrl>c" to cancel the output of a previously-issued command, in some cases the "<Ctrl>c" does not appear to have any effect, and the switch displays the remaining output of the previous command.
- **CLI (PR_0000050800)** —The output of the CLI command **show tech instrumentation** displays incorrect values for "port toggles".
- **CLI (PR_0000052748)** — The switch does not allow a VLAN number higher than 4 to be configured as the primary VLAN.
- **CLI (PR_0000059016)**— When the user types **logout** from a console session, the switch closes the session without the Do you want to log out [y/n]? and Do you want to save current configuration [y/n/^C]? prompts.
- **CPU Utilization (PR_0000059792, PR_0000061703)** — Certain situations with ECMP, a large number of routes (on the order of 3000), or use of the **clear arp** command, may result in high CPU utilization and decreased performance on the switch.
- **Crash (PR_0000039465)** — Rarely, a switch with DHCP Snooping configured may experience an unexpected reboot that triggers a crash message similar to the following.


```
TLB Miss: Virtual Addr=0x00000004 IP=0x800e3e30 Task='mDsnoop003 '
Task ID=0x85dbb190 fp:0x00000000 sp:0x85dbae88 ra:0x80384c40 sr:0x1000fc01
```
- **Crash (PR_0000052464)** — A switch that has a large number of ACLs applied by the Identity Driven Manager (IDM) application might reboot unexpectedly with a message similar to the following.


```
Software exception at enDecode.c:54 -- in 'midmCtrl', task ID = 0xa946380
-> out of memory!
```
- **Crash (PR_0000054005)** — If an SFP+ transceiver or cable is present in the switch and the menu interface is used to make port or trunk configuration changes, the switch might reboot unexpectedly with a message similar to the following.

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

- **Crash Messaging (PR_0000015799)** — Important data may be truncated from the crash message.
- **DHCP (PR_0000054749)**—When the switch acts as a DHCP relay agent, it erroneously removes the "end" option (code 255) from DHCP packets.
- **DHCP Snooping (PR_0000056774)** — When DHCP snooping is enabled, valid PXE boot packets that have yiaddr = 0.0.0.0 are dropped by the switch.
- **DIPLD (PR_0000052518)** — With Dynamic IP Lockdown enabled, there is no communication between clients on the switch.
- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement. For more information, see [“Multicast ARP Support” on page 33](#).
- **Enhancement (PR_0000044183)** — Display interface configuration enhancement. For more information, see [“Display Configuration of Selected Interface” on page 34](#).
- **Enhancement (PR_0000045649)** — Post-login banner enhancement. For more information, see [“Post-login Banner Enhancement” on page 40](#).
- **Enhancement (PR_0000045707)** — The tilde character is now allowed in TACACS+ and RADIUS encryption keys. For more information, see [“Support for the Tilde \(~\) Character in TACACS+ and RADIUS Keys” on page 42](#).
- **Enhancement (PR_0000045711)**— Web authentication message enhancement. For more information, see [“Web Auth Deny Message” on page 45](#).
- **Enhancement (PR_0000045752)** —User-configurable per-port MAC address enhancement. For more information, see [“Port Security Per-Port MAC Increase” on page 49](#).
- **Enhancement (PR_0000046912)** — Adds support for LLDP PoE+. For more information, see [“PoE with LLDP” on page 49](#).
- **Enhancement (PR_0000048021)** — Support was added for the following products.
 - J9310A - HP ProCurve 3500yl-24G-PoE+ Switch
 - J9311A - HP ProCurve 3500yl-48G-PoE+ Switch
 - J9312A - HP ProCurve 10-GbE 2-Port SFP+/2-Port CX4 yl Module.
- **Enhancement (PR_0000050143)** — Adds the ability for Interrupt-Driven Port-Down Notification. Note: This enhancement was inadvertently omitted from the published K.15.02.0005 Release Notes.
- **Enhancement (PR_0000052732)**—Enhancement to increase the MAC Authentication Client Limit to 256. For more information, please see [“Increase MAC Auth Client Limit to 256” on page 52](#).
- **Enhancement (PR_0000052801)** — Categorize CLI Return Messages enhancement. For more information, please see [“Categorize CLI Return Messages” on page 53](#).
- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az). For more information, please see [“Energy Efficient Ethernet \(EEE\)” on page 56](#).
- **Enhancement (PR_0000055751)** — Support was added for the following product. J9153A 10-GbE SFP+ ER Transceiver (J9153A HP X132 10G SFP+ LC ER Transceiver)
- **Enhancement (PR_0000057058)** — Adds this feature to Nonstop Switching: synchronization for 802.1X supplicants originating from the switch.

- **Enhancement(PR_000057799)**—Support was added for the following products.
 - J9534A - HP ProCurve 24-port 10/100/1000 PoE+ v2 zl Module
 - J9535A - HP ProCurve 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module
 - J9536A - HP ProCurve 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module
 - J9537A - HP ProCurve 24-port SFP v2 zl Module
 - J9538A - HP ProCurve 8-port 10-GbE SFP+ v2 zl Module
 - J9547A - HP 24-port 10/100 PoE+ v2 zl Module
 - J9548A - HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module
 - J9549A - HP 20-port Gig-T / 4-port SFP v2 zl Module
 - J9550A - HP 24-port Gig-T v2 zl Module
 - J9637A - HP 12-port Gig-T / 12-port SFP v2 zl Module
- **Event Log (PR_0000050999)** — If the CLI command is issued to download software to the switch, and during that download an SNMP request to download software is sent to the switch, the resulting error message is garbled.
- **File Transfer (PR_0000039190)**— A configuration file that has a QoS policy applied to a VLAN (**vlan <vlan-id> service-policy <policy-name> in**) cannot be downloaded to the switch.
- **File Transfer (PR_0000054790)** — Switch software cannot be updated via HTTPS.
- **IGMP (PR_0000052737)**— With Forced Fast-Leave disabled (which is the default), upon receipt of a "leave" message from a client, the switch sends a Group Specific Query with a Max Response Time of zero seconds, which is not a valid value.
- **IP Communication (PR_0000053603)**— The switch responds to an ARP request received on one VLAN but sent from a different VLAN. This situation can occur when a client's port is moved from one VLAN to another, and the client sends an ARP request from an IP address on the original VLAN.
- **IP Communication (PR_0000053861)** — The switch is unable to telnet or ping to supernatted IP addresses, and supernatted IP addresses cannot be configured on the switch.
- **IPv6 (PR_0000056259)**— The switch does not use the longest matching prefix for default address selection, which violates rule 8 in section 5 of RFC 3484.
- **IPv6 (PR_0000056301)**— Autoconfigured addresses remain in effect after preferred and valid prefix lifetimes expire.
- **LLDP (PR_0000058583)** — After a switch port loses link, the output of **show power brief <port_number>** wrongly indicates that no PoE power is being delivered.
- **MSTP (PR_0000058462)** — Under certain circumstances, the switch might increment the Topology Change Count when it should not. The topology change is incorrectly detected on a link that is blocked at the far end.
- **Nonstop Switching (PR_0000050740)**—RADIUS accounting statistics are not maintained during a management module failover.
- **OSPF (PR_0000040435)** — If the switch is configured as an OSPF Area Border Router (ABR) with a Loopback 0 address assigned to area 0.0.0.0, the switch does not exchange inter-area routes after the last physical interface in area 0.0.0.0 goes down.
- **OSPF (PR_0000045110)** — With OSPF routing and OSPF traps enabled, the switch's available memory decreases over time.
- **OSPF (PR_0000046029)** — If there are routers in an OSPF area that do not support "demand circuits", virtual links (which are treated as demand circuits and should stop LSA aging) cause the LSAs to age out, causing SPF recalculation and periodic route flapping.
- **OSPF (PR_0000055768)**— After 255 topology changes, the next OSPF topology change resets the Shortest Path First (SPF) counter to 1 instead of incrementing to 256.

- **OSPF (PR_0000058797)** — With OSPF and VRRP enabled, a route to a specific host might be lost during a VRRP failover. The switch will display this event log message: `IpAddrMgr: Failed to add FIB entry - route matches existing next-hop router.`
- **PIM (PR_0000054424)** — When a multicast source is connected to a VLAN with multiple IP address ranges (a "multinetted VLAN"), and the multicast source is configured with an IP address in one of the secondary IP address ranges, the multicast streams are not forwarded by the switch.
- **PIM-SM (PR_0000050032)** —The switch logs erroneous `No pim neighbor on vid <VLAN-ID>, cannot send joinprune packet` messages. The event log messages are the only problem; PIM-SM functions properly.
- **PoE (PR_0000053516)** — If a faulty PoE+ power supply is installed in the zl Power Shelf, the switch does not properly indicate that the power supply is bad. Instead, the switch displays `0W /Connected` in the **show power-over-ethernet** output. With this fix, a) the command output displays `0W /Connected - Faulted`, b) an event log message is generated: `Ext Power Supply <power-supply-number> measured out of spec or is faulty. Please change or contact support.,` and c) the Power Supply Status LED flashes orange.
- **Port Connectivity (PR_0000050635)** — When 7-meter Direct Attach Cables (J9285B) connect two switches, if one of the switches is rebooted, the connected ports might begin to toggle offline/online repeatedly.
- **Rate Limiting (PR_0000045467)** — Ingress rate-limiting that is configured via RADIUS or Identity Driven Manager (IDM) is not applied to OSI Layer 2 traffic.
- **Routing (PR_0000053115)** — With the VLAN MAC Address Reconfiguration feature enabled, routed packets are forwarded at very slow rates if the switch's route table has a large number of entries.
- **sFlow (PR_0000012123)** — The switch does not allow sFlow to be configured on a mirror port.
- **sFlow (PR_0000041583)**— The switch does not send VLAN tag information in sFlow data.
- **Spanning Tree (PR_0000058714)**— After loading a configuration file with non-default Spanning Tree path costs defined for 10-Gigabit ports, the 10-Gigabit port path costs revert to their default value of 2000.
- **SSH (PR_0000052970)**— The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB).
- **Stacking (PR_0000052110)** — When a commander accesses a member switch and the user issues the **show tech all** command, in some situations the session from commander to member can become unresponsive. Workaround: from the commander switch, **kill** the unresponsive session.
- **TACACS (PR_0000052495)**— If the switch is configured to use TACACS for telnet access and the TACACS timeout is configured for a value greater than 75 seconds, the switch waits much longer than 75 seconds before timing out the TACACS request.
- **TELNET (PR_0000061481)**— When connecting to the switch via TELNET, if a router between the client and the switch has an MTU setting of less than 1500 bytes, the first attempt to TELNET fails.
- **TFTP (PR_0000046863)** — The switch experiences a loss of free memory each time a software image is downloaded via TFTP, unless there is a redundant management module installed.

Version K.15.02.0005

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

The following problems were resolved in software version K.15.02.0005.

- **OSPF (PR_0000063104)**— OSPF unicast packets are sent to the medium priority queue instead of the high priority queue.
- **SSH (PR_0000062414)** — When a configuration file is copied onto a switch and the switch reboots as a result of this copy, the SSH key information is deleted from the configuration file.

Version K.15.03.0003

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

The following problems were resolved in software version K.15.03.0003.

- **802.1X (PR_0000005372)** — Some combinations of source and destination MAC addresses may cause 802.1X to stop functioning on a port; only a reboot will recover functionality.
- **ACLs (PR_0000059674)** — After updating switch software from K.13.58 or later (with a K.13 config file) to K.15 software, ACL rate-limit commands that are applied to multiple interfaces are duplicated for each interface in the config file. That is, a uniquely-numbered but identical policy is created for each interface, instead of applying a single policy to each interface. The policies function properly, but the config file is more difficult to interpret.
- **ACLs (PR_0000061483)** — The Access Control Entry (ACE) **permit tcp any <destination_IP> established** does not function properly.
- **Authentication (PR_0000058253)** - The switch's event log reports `auth: Invalid user name/password on SSH session`, even though the client is already authenticated.
- **BPDU Protection (PR_0000047748)** - This fix corrects the output of an SNMP query. Before the fix, the switch might incorrectly respond that BPDU protection is disabled on a port, when in fact it is enabled and functioning properly.
- **CLI (PR_0000015197)** — The CLI response to **sho int eth <port_number>** displays only the second half of the first byte of the MAC address. The switch response to **show mac** and other commands that list the MAC address accurately display the proper format of MAC addresses.
- **CLI (PR_0000061404)** — After configuring an SFP slot with the CLI command **speed-duplex 100-half** and saving the configuration, that setting is erased when the switch reboots.
- **Console (PR_0000001136)** — Rarely, the switch console may hang after a software image transfer to the switch. Workaround: **<Ctrl-C>** will restore the command prompt.
- **Counters (PR_0000062966)** — The Drops Tx counter is not reset when a port goes offline, which can cause erroneous FFI (Find, Fix, Inform) High collision or drop rate messages after the port comes back online.
- **Crash (PR_0000050103)** — The switch allows setMIB commands to create invalid configurations, which might cause the switch to reboot unexpectedly when the user issues the **show running-config** command, with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

Software exception at cli_xlate.c:5340 -- in 'mSess1', task ID = > 0xa924e00
- **DHCP Snooping (PR_0000046276)** — With DHCP snooping enabled, a MAC-Authentication client whose session times out cannot reauthenticate.

- **Distributed Trunking (PR_0000048802)** — After powering down a switch participating in a distributed LACP trunk, the remaining switch does not take over the conversations previously running through the offline switch. Workaround: Do not power down a switch running Distributed Trunking. If a reload is required, first unplug the Distributed Trunk links from the switch, wait at least one minute, then unplug the Inter-Switch Connection (ISC), then reload or power down the switch.
- **Enhancement (PR_0000045685)** — Allows creation of a custom default configuration for the switch. For more information, see [“Custom Default Configuration” on page 60](#).
- **Enhancement (PR_0000045796)** — Adds the ability to enable SNMP traps when MAC addresses are added to or deleted from a port. For more information, see [“SNMP Trap Upon Port Addition or Deletion of MAC Addresses” on page 66](#).
- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed. For more information, see [“Log Message When Startup Config Updated” on page 69](#).
- **Enhancement (PR_0000052738)** — Adds VLAN information to the output of the **show mac-address** commands. For more information, see [“Show MAC with VLAN” on page 70](#).
- **Enhancement (PR_0000054042)** — Adds the ability to monitor egress queues for dropped packets when QoS is configured. For more information, see [“Outbound Queue Monitor” on page 71](#).
- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information. For more information, see [“Show OSPF Neighbor Timers” on page 72](#).
- **Enhancement (PR_0000054183)** — The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses. For more information, see [“IP Enable/Disable for All VLANs” on page 73](#).
- **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries. For more information, see [“Logging for Routing ACLs” on page 74](#).
- **Enhancement (PR_0000058115)** — Allows the use of TCP/UDP source and destination port number for trunk load balancing. For more information, see [“Trunk Load Balancing Using L4 Ports” on page 79](#).
- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs. For more information, see [“Wake-on-LAN Support Across VLANs” on page 81](#).
- **Enhancement (PR_0000058564)** — Adds the ability to send syslog messages via TCP. For more information, see [“Syslog via TCP” on page 85](#).
- **Enhancement (PR_0000058798)** — Adds the ability to enable an SNMP trap for any configuration change made in the switch's running configuration file. For more information, see [“SNMP Trap on Running Configuration Changes” on page 86](#).
- **Enhancement (PR_0000058804)** — Allows the redistribution into RIP of static blackhole or reject routes. For more information, see [“Static Summary Route to RIP” on page 89](#).
- **Enhancement (PR_0000060972)** — Enables configuration of RADIUS attributes for downstream supplicant devices. This allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits. For more information, see [“Dynamic Port Access Auth via RADIUS” on page 90](#).
- **Event Log (PR_0000059300)** — Event log message #608 displays "vlan 0" instead of a valid failure type.
- **Guaranteed Minimum Bandwidth (PR_0000042500)** — The switch does not allow Guaranteed Minimum Bandwidth (GMB) to be configured on port L24. Also, a configuration file with GMB on port L24 fails to load onto the switch.
- **IP Communication (PR_0000042790)** — A very busy switch may cease all IP communication when the CLI command **show tech route** is executed. Messages similar to the following may be seen in the event log when this occurs.

W <date> <time> 00436 NETINET: 1 route entry creation(s) failed.

W <date> <time> 00075 system: Out of pkt buffers; miss count: 0

- **IP Connectivity (PR_0000046280)** — After updating software, the hostname is removed from the configuration and the switch does not respond to SSH requests.
- **LLDP-MED (PR_0000018681)** — LLDP-MED responses from a device connected to the switch are stored in the wrong order, which causes errors when the user uses **snmpwalk** to see the stored values on the switch.
- **Port Authentication (PR_0000043433)** — The switch allows the user to configure reauthentication on ports that are not yet configured for authentication. With this fix, an error message will be generated if the user attempts that invalid configuration.
- **Port Communication (PR_0000060305)** — The interrupt-driven port-down notification introduced in K.15.02 may, in rare situations, cause a port to block outgoing traffic after a switch reboot.
- **Port Communication (PR_0000061884)** — A PoE+ switch port configured with **speed-duplex auto-10-100** and connected to an Intel NIC 82566 with Wake on LAN enabled might stop responding after one or two hours. Workaround: configure the port with the **speed-duplex auto** setting.
- **Savepower (PR_0000056993)** — Savepower commands are not available on the 3500 series switches.
- **SNMP (PR_0000046848)** — SNMP traps are sent to the in-band VLAN, even if configured to send SNMP traps to the Out-of-Band Management (OOBM) interface. This fix adds an option in CLI to specify OOBM as the trap destination.
- **SNMP (PR_0000060189)** — The MIB object "dot3PauseOperMode" has incorrect information about the state of flow control on a port.
- **SNMP (PR_0000060257)** — The port type for 100-BX and 1000-BX transceivers is incorrectly identified when requested via SNMP.
- **SNTP Authentication (PR_0000048588)** — With SNTP authentication disabled, the switch sends extra, unnecessary authentication information in the SNTP request packet.
- **SSH (PR_0000045158)** — SSH login to the switch might fail.
- **Syslog (PR_0000012167)** — Syslog messages longer than 119 characters get truncated.
- **TELNET (PR_0000061045)** — After opening and then closing a Telnet session to another switch, the message "Telnet closed: Connection reset by peer" is displayed instead of "Telnet closed: Connection closed by host".
- **UDLD (PR_0000058636)** — A port that is configured for UDLD may be in a UDLD blocking state for five seconds after the link comes up, which can cause issues with VRRP.
- **Web Authentication (PR_0000042284)** — When an EWA server is used for Web authentication, authentication is successful but custom graphics are not displayed.
- **Web Authentication (PR_0000048486)** — When an EWA server is used for Web authentication, the EWA login page is not presented properly with some versions of Safari Web browser.
- **Web Management (PR_0000054861)** — The Web "device view" of a switch shows the power supply status as green for all installed internal power supplies, even if a power supply is installed with no power cord connected.
- **Web Management (PR_0000060813)** — Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access.

Version K.15.03.0004

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

The following problems were resolved in software version K.15.03.0004.

- **CLI (PR_0000061969)** — The switch responds with `translator failed` messages when the user enters **copy config** and **show tech** commands. This is seen with very large configuration files.
- **Self Test (PR_0000064124)** — Rarely, the LEDs for one or more ports indicate "selftest failure" after switch reboot, although there is no message in the event log.
- **SNTP (PR_0000064369)** — When the switch updates its system time via SNTP, the event log entry does not include the IP address of the SNTP server, and the previous and updated times are not displayed.

Version K.15.03.0005

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

The following problem was resolved in software version K.15.03.0005.

- **OSPF (PR_0000065337)** — When routing information changes lead to OSPF recalculation, the switch can experience packet loss under heavy traffic loads.

Version K.15.03.0006

Status: Never released.

The following problems were resolved in software version K.15.03.0006.

- **CLI (PR_0000067688)** — The output of the **show system** command might display an incorrect value for Free Memory.
- **Crash (PR_0000066570)** — After a large number of startup configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Unable to allocate message buffer  
Software exception in ISR at btmDmaApi.c:370
```
- **Direct Attach Cables (PR_0000065839)** — Some Direct Attach Cables (DACs) might be identified as "unsupported" when inserted in a v2 zl module running software versions K.15.03.0003 through K.15.03.0005. This issue only affects DACs with part numbers 8121-1148, 8121-1149 and 8121-1155.
- **SNMP (PR_0000068087)** — Two of the OIDs related to SNTP are in the wrong sequence in switch software. The affected OIDs are `hpSntpInetServerIsOobm` and `hpSntpInetServerAuthKeyId`.

Version K.15.03.0007

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

The following problem was resolved in software version K.15.03.0007.

- **Transceivers (PR_0000066558)** — With one or more J8177B/C 1000Base-T Mini-GBICs (HP X121 1G SFP RJ45 T Transceivers) installed in a 6200yl switch running K.15.02 or K.15.03.0003 through K.15.03.0006 software, the J8177B/C in the highest-numbered slot will not link when the switch reboots. Workaround: hot-swap the transceiver that does not link.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/

© Copyright 2010-2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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 will not be liable for technical or editorial errors or omissions contained herein.



February 2011

Manual Part Number
5998-1186