Release Notes:
Version K.13.49 Software
for the ProCurve Series 3500yl, 6200yl, 5400zl, and 8212zl Switches

These release notes include information on the following:

- Downloading switch software and documentation from the Web (page 2)
- Best practices for major software updates, including contingency procedures for rolling back to previous software versions and configurations. **Please read before updating software versions from K.12.xx to K.13.xx** (page 7).
- Notes for ROM updates required for all yl and zl switches running K.13.45 or earlier (page 17)
- Clarifications for certain software features (page 20)
- A listing of software enhancements in recent releases (page 26)
- A listing of software fixes included in releases K.11.11 through K.13.49 (page 145)
- Support Notes and Known Issues in releases K.11.11 through K.13.49 (page 17)—includes "Security notes about SNMP access to the hpSwitchAuth MIB objects" and other topics.

Support Notices:

WARNING. Updating to Version K.13.xx: . It is important that you update to K.13.xx from a configuration that has not been previously converted from a pre-K.13.xx format (e.g. a K.11.xx or K.12.xx configuration). If you have previously updated to K.13.xx and rolled back to K.12.xx to workaround an issue, you should load a saved K.12.xx configuration to the switch and boot to it prior to updating to K.13 again.

Performing major software updates: Before updating your software version from K.12.xx to K.13.xx, read the recommended best practices for performing major software updates (page 7).

Restriction in number of ACL mirror destinations: The K.13.01 software introduced a new restriction to a single ACL mirror destination. For more information, see "Restriction in number of ACL mirror destinations (page 24) .

PIM-SM: PIM-SM users should make sure ProCurve switches that run K software should all be on the either pre-K.13.21 or post-K.13.21 versions of software due to a bug fix in K.13.21 that changes the way a rendezvous point is chosen.

© Copyright 2006-2008 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

5991-4720
January 2009

Applicable Products

ProCurve Switch 3500yl-24G-PWR Intelligent Edge	(J8692A)
ProCurve Switch 3500yl-48G-PWR Intelligent Edge	(J8693A)
ProCurve Switch 6200yl-24G-mGBIC	(J8992A)
ProCurve Switch 5406zl	(J8697A)
ProCurve Switch 5412zl	(J8698A)
ProCurve Switch 5406zl-48G	(J8699A)
ProCurve Switch 5412zl-96G	(J8700A)
ProCurve Switch 8212zl	(J8715A)

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 Customer Support/Warranty booklet included with the product.

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

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

Contents

Software Management 1

Premium License Switch Software Features 1

Software Updates 1

Download Switch Documentation and Software from the Web 2

View or Download the Software Manual Set 2

Downloading Software to the Switch 2

TFTP Download from a Server 3

Xmodem Download From a PC or Unix Workstation 3

Using USB to Download Switch Software 5

Saving Configurations While Using the CLI 6

Best Practices for Major Software Updates 7

Updating the Switch: Overview 7

Updating the Switch: Detailed Steps 8

Rolling Back Switch Software 11

Viewing or Transferring Alternate Configuration Files 12

ProCurve Switch, Routing Switch, and Router Software Keys 14

OS/Web/Java Compatibility Table 15

Minimum Software Versions 15

Support Notes 17

ROM Update Required! 17

Using SNMP To View and Configure Switch Authentication Features 17

Support for the Wireless Edge Services zl Module 18

CAUTION: Updating to Version K.13.xx 19

Clarifications 20

Known Issues 22

Release K.13.02 24

Release K.13.01 24

Enhancements 26
Release K.11.12 Enhancements 26
Release K.11.13 through K.11.32 Enhancements 26
Release K.11.33 Enhancements 26
Release K.11.34 Enhancements 26
Release K.11.35 Enhancements 27
Release K.11.36 through K.11.39 Enhancements 27
Release K.11.40 Enhancements 27
Release K.11.41 Enhancements 28
Release K.11.42 Enhancements 28
Release K.11.43 Enhancements 28
Release K.11.44 Enhancements 28
Release K.11.45 Through K.11.47 Enhancements 28
Release K.11.48 Enhancements 28
Release K.11.49 Enhancements 28
Release K.11.60 through K.11.63 Enhancements 29
Release K.11.64 Enhancements 29
Release K.11.68 Enhancements 29
Release K.11.69 Enhancements 29
Release K.12.01 Enhancements 30
Release K.12.02 Enhancements 32
Release K.12.03 Enhancements 32
Release K.12.04 Enhancements 33
Configuring MSTP Port Connectivity Parameters 33
Release K.12.05 Enhancements 36
How RADIUS-Based Authentication Affects VLAN Operation 36
Release K.12.06 Enhancements 43
Saving Security Credentials in a Configuration File 43
Release K.12.07 Enhancements 57
Release K.12.08 Enhancements 57
Configuring a System Contact and Location for the Switch 57
Release K.12.09 Enhancements 58

Release K.12.10 Enhancements 58
Show VLAN ports CLI Command Enhancement 58
Release K.12.11 Enhancements 60
Release K.12.12 Enhancements 60
Release K.12.13 Enhancements 60
Release K.12.14 Enhancements 60
Release K.12.15 Enhancements 60
Send SNMP v2c Informs 60
Release K.12.16 Enhancements 62
Release K.12.17 Enhancements 62
Release K.12.18 Enhancements 62
Release K.12.19 Enhancements 63
Release K.12.20 Enhancements 63
Release K.12.21 Enhancements 63
Release K.12.22 Enhancements 64
Release K.12.23 Enhancements 64
Release K.12.24 Enhancements 64
Release K.12.26 through K.12.29 Enhancements 64
Release K.12.30 Enhancements 64
Release K.12.31 Enhancements 64
Release K.12.32 Enhancements 64
Release K.12.33 through K.12.40 Enhancements 65
Release K.12.41 through K.12.42 Enhancements 65
Release K.12.43 Enhancements 65
Release K.12.44 Enhancements 65
Release K.12.45 Enhancements 66
Release K.12.46 Enhancements 66
Release K.12.47 Enhancements 66
Release K.12.48 Enhancements 66
Release K.12.49 Enhancements 66
Release K.12.50 Enhancements 66

Release K.12.51 Enhancements 66
Release K.12.52 Enhancements 67
Release K.12.53 through K.12.55 Enhancements 67
Release K.12.56 Enhancements 67
Release K.12.57 Enhancements 68
Release K.13.01 Enhancements 69
Release K.13.02 Enhancements 71
VRRP Pre-Emptive Delay Timer 71
Release K.13.03 Enhancements 75
New CLI Commands 75
Release K.13.04 Enhancements 76
Clear Module Configuration 76
VRRP—Dynamic Priority Change 77
DHCP Option 66 Automatic Configuration Update 83
BOOTP/DHCP Relay Gateway 85
Inbound Rate-Limiting for Broadcast and Multicast Traffic 87
DNS Capabilities for Telnet 89
Show Module Enhancement 90
VRRP Option with Debug Command 92
Copy Command with Show Tech Option 93
Release K.13.05 through K.13.15 Enhancements 94
Release K.13.16 Enhancements 94
Console/Telnet Inactivity Timer 94
Management Access Security Enhancement 95
Show Interfaces Custom 98
Mirror Port VLAN Tagging 101
Concurrent Web and MAC Authentication 104
SSH Enhancements 105
Release K.13.17 Enhancements 109
Release K.13.18 Enhancements 109
Release K.13.19 Enhancements 109
Using a Command Alias 109
Configure Logging via SNMP 111
Customizing Web Authentication HTML Files 114

Enabling Customized Web Authentication Pages 115
Dynamic IP Lockdown 129
Operating Notes 133
Release K.13.20 Enhancements 138
Release K.13.21 Enhancements 139
Release K.13.22 Enhancements 139
Release K.13.23 Enhancements 139
Release K.13.24 through K.13.25 Enhancements 139
Release K.13.26 through K.13.39 Enhancements 139
Release K.13.40 Enhancements 139
LACP and Link Traps Global Disable 139
Clear Statistics Without Reboot 140
Increase MAC Lockout to 64 141
Configure Logging via SNMP 141
Operating Notes 143
Release K.13.41 Enhancements 143
Release K.13.42 Enhancements 143
Release K.13.43 Enhancements 143
Release K.13.44 Enhancements 144
Release K.13.45 Enhancements 144
Release K.13.46 through K.13.48 Enhancements 144
Release K.13.49 Enhancements 144

Software Fixes in Release K.11.12 - K.13.49 145

Release K.11.12 145
Release K.11.13 146
Release K.11.14 146
Release K.11.15 146
Release K.11.16 147
Release K.11.17 147
Release K.11.32 147
Release K.11.33 150

Release K.11.34 151
Release K.11.35 151
Release K.11.36 152
Release K.11.37 152
Release K.11.38 152
Release K.11.39 152
Release K.11.40 153
Release K.11.41 153
Release K.11.43 153
Release K.11.44 154
Release K.11.46 154
Release K.11.47 155
Release K.11.48 155
Release K.11.49 155
Release K.11.61 156
Release K.11.62 156
Release K.11.63 157
Release K.11.64 157
Release K.11.65 158
Release K.11.66 158
Release K.11.67 159
Release K.11.68 159
Release K.11.69 160
Release K.12.01 160
Release K.12.02 161
Release K.12.03 162
Release K.12.04 163
Release K.12.05 164
Release K.12.06 164
Release K.12.07 164
Release K.12.08 165

Release K.12.09 165
Release K.12.10 165
Release K.12.11 166
Release K.12.12 166
Release K.12.13 166
Release K.12.14 166
Release K.12.15 167
Release K.12.16 168
Release K.12.17 168
Release K.12.18 169
Release K.12.19 169
Release K.12.20 170
Release K.12.21 170
Release K.12.22 171
Release K.12.23 171
Release K.12.24 172
Release K.12.25 172
Release K.12.26 through K.12.29 173
Release K.12.30 173
Release K.12.31 173
Release K.12.32 173
Release K.12.33 through K.12.40 173
Release K.12.41 through K.12.42 173
Release K.12.43 173
Release K.12.44 174
Release K.12.45 174
Release K.12.46 175
Release K.12.47 175
Release K.12.48 176
Release K.12.49 176
Release K.12.50 176

Release K.12.51 176
Release K.12.52 177
Release K.12.53 177
Release K.12.54 178
Release K.12.55 179
Release K.12.56 179
Release K.12.57 179
Release K.13.02 181
Release K.13.03 182
Release K.13.04 183
Release K.13.05 186
Release K.13.06 187
Release K.13.07 187
Release K.13.08 188
Release K.13.09 189
Release K.13.10 189
Release K.13.11 190
Release K.13.12 190
Release K.13.13 192
Release K.13.14 192
Release K.13.15 193
Release K.13.16 193
Release K.13.17 194
Release K.13.18 195
Release K.13.19 196
Release K.13.20 196
Release K.13.21 197
Release K.13.22 198
Release K.13.23 198
Release K.13.24 199
Release K.13.25 199

Release K.13.26 through K.13.39 200
Release K.13.40 200
Release K.13.41 201
Release K.13.42 201
Release K.13.43 202
Release K.13.44 202
Release K.13.45 203
Release K.13.46 204
Release K.13.47 206
Release K.13.48 206
Release K.13.49 207

Software Management

Premium License Switch Software Features

The ProCurve 3500yl and 5400zl switches ship with the ProCurve Intelligent Edge software feature set. The additional Premium License switch software features for the 3500yl and 5400zl switches can be acquired by purchasing the optional Premium License and installing it on the Intelligent Edge version of these switches. As of February 2008, the Premium License features include the following:

- OSPF
- PIM Dense mode
- PIM Sparse mode
- VRRP
- QinQ

Part numbers for the Premium Licenses are:

- 3500yl switches: J8993A
- 5400zl switches: J8994A

All software features are automatically included on the ProCurve 6200yl and 8212zl switches without the need for a Premium License.

To purchase a Premium License for the 3500yl or 5400zl switches, go to the following Web page and click on How To Buy.

www.hp.com/rnd/accessories/J8994A/accessory.htm

To view or download a listing of Intelligent Edge and Premium License features, refer to the *Software Features Index* available for download on the product documentation page for your switch model.

Note:
Switch software Version K.11.33 software or newer is required for proper functioning of Intelligent Edge features on ProCurve Switch 3500yl series, and ProCurve Switch 5400zl series

Software Updates

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

Download Switch Documentation and Software from the Web

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

View or Download the Software Manual Set

Go to: **www.procurve.com/manuals**

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

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

Downloading Software to the Switch

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

- For a TFTP transfer from a server, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.
  - Use the **copy tftp** command in the switch's CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and select the **Xmodem** option.
  - Use the **copy xmodem** command in the switch's CLI (page 3).
- Use the USB port to download a software file from a USB flash drive (page 5).
- Use the download utility in ProCurve Manager Plus.

Note

Downloading new software does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model.

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

TFTP Download from a Server

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

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

For example, to download a software file named K_11_1x.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_11_1x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

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

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

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:

   a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)

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

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

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

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

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

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

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

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

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

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

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

2. Execute the following command in the CLI:

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

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

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

4. If you increased the baud rate on the switch (step 1), use the same command to return it to its previous setting. (ProCurve recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)

5. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)

6. Reboot the switch from the flash area that holds the new software (primary or secondary).

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

Using USB to Download Switch Software

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

- The software version must be stored on the USB flash drive, and you must know the file name (such as K_12_10.swi).
- The USB flash drive must be properly installed in the USB port on the switch.

Note

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

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

For example, to download a software file named K_12_10.swi from a USB flash drive:

1. Execute the copy command as shown below:

```
ProCurve # copy usb flash K_12_10.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]?
```

Best Practices for Major Software Updates

Major software updates contain new features and enhancements, and are designated by an increment to the major release version number. That is, K.12.xx represents a major update to software version(s) K.11.xx, and K.13.xx represents a major update to K.12.xx, and so forth. To mitigate against potential migration issues when performing such an update, this section documents best practices for updating the switch, including contingency procedures for rolling back to previous software versions and saved configurations.

Caution

Before you update the switch software to a major new version, ProCurve strongly recommends that you save off a copy of your config file to an external location. ProCurve advises against rolling back (going from a newer software version to an older software version) without copying on a backup config file to the device.

Updating the Switch: Overview

To perform a major update to your switch software, follow the steps below (see page 8 for details):

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.13.06)
- Secondary image will hold the image you are currently running (for example, K.12.57)
- Primary image will boot with config1 (config file corresponding to new software version—in this example, K.13.06)
- Secondary image will boot with config2* (config file corresponding to previous software version—in this example, K.12.57)

* 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, ProCurve strongly recommends 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 major new release (in the example provided here, from version K.12.57 to version K.13.06).

1. Download the latest release software image to your TFTP server from the ProCurve Web site.: http://www.hp.com/rnd/software/switches.htm
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(t2g)
                Dec  7 2007 14:54:57
                K.12.57
                2415
Boot Image:     Primary

Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 6782942   12/07/07 K.12.57
Secondary Image : 6765066   08/24/07 K.12.43
Boot Rom Version: K.12.12
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_12_57.cfg
```

Note

This step is necessary because ProCurve does 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   : 6782942   12/07/07 K.12.57
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
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

This step will enable you to revert from K_13_05 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_13_06.swi primary
The Primary OS Image will be deleted, continue [y/n]?
```

   At the prompt, answer **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.12.57 to K.13.06, you should see the following outputs from the switch show commands:

```
Switch1# show version
Image stamp:    /sw/code/build/btm(t2g)
                Mar 14 2008 09:59:53
                K.12.57
                2415
Boot Image:     Primary


Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7350018   03/14/08 K.13.06
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
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, answer **y**, for yes, and the switch will boot with the new image.

Note:

As an additional step, ProCurve advises 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_13_06.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.

To roll back your switch from K.13.06 to K.12.57, 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(t2g)
                Mar 14 2008 09:59:53
                K.13.06
                211
Boot Image:     Primary


Switch1# show flash
Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7350018   03/14/08 K.13.06
Secondary Image : 6782942   12/07/07 K.12.57
Boot Rom Version: K.12.12
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
```

Answer **y**, for yes, and the switch will boot from the secondary image (K.12.57, 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.12.57 and saved as config2, and if it is then viewed or transferred while the switch is running K.13.06, it will appear as though K.13.06 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.12.57 to a TFTP server with an IP address of 10.10.10.15 as follows:

```
ProCurve5406zl-onK1257# copy running-config tftp 10.10.10.15
5406onK1257
```

If, for example, the user deems it necessary to revert to the use of K.12.57, she 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.12.57 and then saved to flash:

```
ProCurve5406zl-onK1257# copy config config2 config K1257config <cr>
```

And later, the configuration that was created on K.12.57 is viewed while the switch is running K.13.06:

```
ProCurve5406zl-onK1306# show config K1257config <cr>
```

The command output will show how the K.12.57 config would be interpreted, *if it were to be used by the K.13.06 software*. Copying the K1257config 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.13.06 to K.12.57 with a command like the following (given that K.12.57 is stored in secondary flash), the K.12.xx formatted config is still intact and valid.

```
ProCurve5406zl# boot system flash secondary config K1257config
```

This "interpretation" during a TFTP or **show** command execution is inherent in the architecture of the switch. When switch features change significantly (e.g. 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.

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
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	Secure Router 7000dl Series (7102dl and 7203dl)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G) and Switch 8212zl.
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
T	Switch 2900 Series (2900-24G, and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
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)
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.)

OS/Web/Java Compatibility Table

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

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, SP2 and 7.0	Sun Java 2 Runtime Environment: – Version 1.5.0_11, Version 1.6.0
Windows Server SE 2003 SP2		
Windows Vista		

Minimum Software Versions

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

ProCurve Device	Product Number	Minimum Supported Software Version
ProCurve 100-BX-D SFP-LC Transceiver	J9099B	K.13.45
ProCurve 100-BX-U SFP-LC Transceiver	J9100B	K.13.45
ProCurve 1000-BX-D SFP-LC Mini-GBIC	J9142B	K.13.45
ProCurve 1000-BX-U SFP-LC Mini-GBIC	J9143B	K.13.45
ProCurve 10-GbE X2-SC LRM Optic	J9144A	K.13.20
ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module	J9051A and J9052A	K.12.43
Switch 8212zl Base System	J8715A	K.12.31
100-FX SFP-LC Transceiver	J9054B	K.12.01
Premium Features on Series 3500yl and 5400zl Switches	J8993A and J8994A	K.11.33
Switch 5400zl 24p Mini-GBIC Module	J8706A	K.11.33

ProCurve Device	Product Number	Minimum Supported Software Version
Switch 5400zl 4p 10-GbE CX4 Module	J8708A	K.11.33
Switch 6200yl-24G-mGBIC	J8992A	K.11.33
Switch 3500yl 2p 10GbE X2 + 2p CX4 Module	J8694A	K.11.17

Support Notes

ROM Update Required!

All yl and zl switches running K.12.45 system software or earlier, will have the BootROM updated by this new version of system software. This software download will boot the switch **twice,** first to update the BootROM to version K.12.14, and then to load the system software. Following file copy to the switch flash and initiation of the reload, no additional user intervention is needed. **Do not interrupt power to the switch** during this important update.

To confirm that the boot ROM and system software have updated successfully following a reload into software version K.13.49 or newer, follow the process below at your switch CLI.

```
ProCurve_zl_yl_Switch# show flash

Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 7497667   12/10/08 K.13.49 <--Indicates that system software is
updated
Secondary Image : 7497667   12/10/08 K.13.49
Boot Rom Version: K.12.14 <-- Indicates the boot ROM is updated
Default Boot    : Primary
```

Using SNMP To View and Configure Switch Authentication Features

Beginning with software release K.12.01, manager read/write access is available for a subset of the SNMP MIB objects for switch authentication (hpSwitchAuth) features. That is, in the default state, a device with management access to the switch can view the configuration for several authentication features, and using SNMP sets, can change elements of the authentication configuration.

Security Note

In the default configuration for SNMP MIB object access, SNMP sets can be used to reconfigure password and key MIB objects. This means that a device operating as a management station with access to the switch can be used to change the SNMP MIB settings. This can pose a security risk if the feature is used to incorrectly configure authentication features or to reconfigure authentication features to unauthorized settings.

If you want to block the SNMP MIB object access described above, use the following command to disable the feature:

```
ProCurve(config)# snmp-server mib hpswitchauthmib excluded
```

For more information on the above topic, refer to "Using SNMP To View and Configure Switch Authentication Features" in the "RADIUS Authentication and Accounting" chapter of the *Access Security Guide* for your switch. For an overview of the security features available on the switch, refer to chapter 1, "Security Overview", in the *Access Security Guide* for your switch.

Security:

Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. If this is not desirable for your network, ProCurve recommends that you disable it after downloading and rebooting with the latest switch software.

ACL numbering restrictions:

The K.12.01 release enforces ACL numbering restrictions.

See the Note under Version K.12.01 Software Fixes on page 160 (PR_1000389442) for details.

OSPF virtual link:

OSPF virtual links configurations will be lost with the update to K.12.01.

See the Note under Version K.12.01 Software Fixes on page 161 (PR_1000374003) for details.

MSTP auto-edge-port support and default settings:

With version K.12.04 (page 33), automatic detection of edge ports is supported, along with revised command options and default settings.

Resources (PR_1000388697):

When the switch is writing large files to flash (for example, a transfer of a very large configuration or a software update), switch resources may be impacted during the write operation, causing some potential loss of hello packets. This may impact VRRP, OSPF or spanning tree protocol. In order to mitigate potentially undesirable affects, updates to the switch software should be made during a scheduled downtime. Increasing the hello interval of time sensitive protocols may also assist with mitigation of this issue.

Support for the Wireless Edge Services zl Module

The addition of support for the zl Wireless Edge Services Module will change the way in which radio ports are treated by the zl and yl Series Switches. If the default setting of LLDP auto-provisioning is left intact, LLDP information from the ProCurve Radio Ports (J9004A, J9005A, J9006A) will trigger these devices to be placed into VLAN 2100 or the first available VLAN not already configured above that (see the section entitled Using Auto-Provisioning to Establish a Radio Port VLAN in the

Management and Configuration Guide for ProCurve Wireless Edge Services zl Module here: ftp://ftp.hp.com/pub/networking/software/WESM-zl-MgmtCfg-Aug2007-59918626.pdf). Network administrators who do not wish to have the radio ports moved to the auto-provisioned VLAN should disable this feature with the command "no lldp auto-proision" at the CLI.

CAUTION: Updating to Version K.13.xx

It is important that you update to K.13.xx from a configuration that has not been previously converted from a pre-K.13.xx format (e.g. a K.11.xx or K.12.xx configuration). If you have previously updated to K.13.xx and rolled back to K.12.xx to workaround an issue, you should load a saved K.12.xx configuration to the switch and boot to it prior to updating to K.13 again.

Clarifications

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

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

- **Maximum Number of Flows in the MRT —** Page 4-41 in the *Multicast and Routing Guide* dated January 2008 for switches running version K software incorrectly states that up to 1023 flows are supported. Up to 2048 flows are supported.

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

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

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

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

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

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

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

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

- **Reload Command Description**

  Syntax: **Reload**

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

  Using Reload

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

- **MSTP mCheck:**
  Unlike other MSTP parameters, 'mCheck' is not a configurable option. It is a flag that tells MSTP to initiate transmission of RST/MST BPDUs for a MigrateTime (3 secs) period, to test whether all STP Bridges on the attached LAN have been removed and the Port can migrate to the native MSTP mode and use RST/MST BPDUs for transmission. The 'mCheck' is always cleared (set FALSE) prior to port initialization.

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

Some of the earlier ProCurve MSTP implementations allowed the 'mCheck' option to be a configurable parameter. It was stored in the config. That was corrected beginning with version K.12.04.

Known Issues

Release K.13.25

The following problems are known issues as of release K.13.25.

SFTP/SCP (PR_0000008270) — An SFTP or SCP client session may not close after a config download session ends. The work-around is to close the client manually.

Release K.13.23

The following problems are known issues in release K.13.23 or newer.

- **MAC Authentication (PR_0000007477)** — When large numbers of MAC authentications are attempted immediately after the switch (re)boots, some of the MAC authentications may fail when they should succeed. Workaround: Increase the RADIUS server delay.

Release K.13.08

The following problems are known issues in release K.13.08 or newer.

- **CLI (PR_0000001893) —** The **copy flash** CLI command does not function in ProCurve 8212zl switches running K.13.05 or later. Workaround: use the CLI command **copy tftp flash**.
- **Config/TFTP (PR_1000748292)** — The switch allows conflicting configuration parameters to be loaded via TFTP transfer to the startup-config (**ip address** <x.x.x.x> and **no ip address**).
- **Port Security (PR_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Certificate (PR_1000416167)** — The Web Management interface submission form limits CA-signed certificates to 1800 bytes.
- **CLI (PR_1000760929)** — The CLI output from the command **show name int <x-x>** does not display the port number beyond the ninth port.
- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **SNMP Trap (PR_1000772026)** — The ProCurve 3500yl Switches do not send the proper OID value for a Redundant Power Supply (RPS) failure.

- **Web (PR_1000761014)** — The Web interface truncates 16 character passwords to 15 characters. Workaround: configure 16 character passwords via the CLI.
- **ICMP (PR_1000764033)** — ICMP *TTL expired* messages are being sent with a source address of the interface the message leaves from rather than the interface that receives the expired packet.
- **Auto-TFTP/Config (PR_0000001410)** — Auto-TFTP configuration is lost during the update from K.12.xx to K.13.03.
- **Web Authentication (PR_0000000968)** — Web authentication to IAS over PEAP may trigger a software exception crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID =
0x843c2b0 -> internal error
```

- **DHCP Snooping (PR_1000469934)** — When DHCP Snooping is enabled and configured, and a client sends a "DHCPINFORM" after receiving address information, the DHCP Server response is not forwarded to the client by the switch.
- **CLI (PR_1000745509)** — There are multiple issues with respect to the output from the CLI command **show ipv6 neighbor vlan <x>**.
- **Module Selftest (PR_0000001273)** — After reboot, ports 1-24 or ports 25-48 on the ProCurve 3500yl or ports 1-24 on the 6200yl Switches may become unresponsive followed by green and amber port LEDs remaining lit. Ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601
chassis: Ports 1-24: Lost Communications detected - Heart Beat Lost(4A)
chassis: Ports 1-24 Downloading
chassis: Ports 1-24 Download Complete
chassis: Ports 1-24 Ready
```

- **ECMP (PR_1000798467)** — A switch using OSPF ECMP may mis-route traffic for routes with long prefixes (/31 or /32).
- **CLI (PR_1000782972)** — The CLI command **show system power** provides incorrect output for those regions that use a 220 volt standard.
- **CLI (PR_1000430534)** — Output from the **show port-access mac-based** CLI command may omit connected clients.
- **CLI (PR_1000776583)** — The output for CLI command **show access-list resources** does not accurately display the number of QoS/ACL masks available.
- **Config Transfer (PR_1000781015)** — A config file transfer will fail with a "`corrupted configuration`" message, if the config file specifies MDIX-mode for a dual-personality port.

- **Config Transfer (PR_1000781004)** — The switch allows a config file transfer to set an invalid speed-duplex setting on a 100FX SFP.
- **Config Transfer (PR_1000781031)** — When the valid port setting 'auto-1000' is configured for a 10/100/1000 interface and the configuration gets copied to the switch, the port setting is altered to 'auto.'
- **Config Transfer (PR_1000781011)** — A config file copied to the switch allows an entry to enable flow control on a half-duplex interface. However, flow control on a half-duplex interface is disabled, as specified by IEEE 802.3 Annex 31B.
- **CLI (PR_1000775644)** — When flow control is enabled, the output from a **show int brief** CLI command inaccurately indicates that flow control is off.

Release K.13.02

The following are known issues in release K.13.02 or newer.

- **ACL Mirrors**: Beginning with K.13.02 software, ACLs can only be mirrored to a single destination.

Release K.13.01

The following are known issues in release K.13.01 or newer.

- **Rate-Limiting**: The "bps" mode for Ingress/Egress Rate-Limiting has been removed from the MIB, from the config, and as a CLI option (help-text also updated). Bandwidth is now measured in KBPS. Configurations which have rate-limiting configured in bps units will be successfully converted to the updated unit of measurement as the software is updated from K.11.xx or K.12.xx to K.13.xx.
- **PCM+ USB Autorun (PR_1000767612)** — Issuing the command copy startup-config usb test may crash the switch when executed in a PCM+ Autorun cmd file. The crash message is similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300:
  ```

- **Restriction in number of ACL mirror destinations** — The K.13.01 software introduced a new restriction to a single ACL mirror destination. K.12 versions of software allowed up to 4 ACL mirror destinations. Users with multiple ACL mirror sessions must edit their configurations so that they contain only a single mirror destination prior to updating to K.13.01 or newer software. If a switch with multiple ACL mirror destinations is updated from K.12.xx to K.13.01 or newer, only the first destination will function. The additional mirror sessions will have to be edited out of the configuration offline, and the valid configuration then loaded onto the switch.

Enhancements

Unless otherwise noted, each new release includes the enhancements added in all previous releases. Enhancements are listed in chronological order, oldest to newest software release. To review a summary of enhancements included since the last general release that was published, begin with "Release K.13.01 Enhancements" on page 69.

Descriptions and detailed instructions for enhancements included in Release K.13.01 or earlier are included in the latest release of manuals for the ProCurve Series 3500yl, 6200yl, 5400zl, and 8212zl switches (January 2008), available on the Web at **www.hp.com/rnd/support/manuals**.

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.12.31 was the first production software release for the ProCurve 8212zl switch. Release K.12.57 is the last public release of the K.12.*xx* software. The 3500yl, 6200yl, 5400zl, and 8212zl software code was rolled to the K.13.0*x* code branch with no intervening releases.

Release K.11.12 Enhancements

Release K.11.12 includes the following enhancement:

- MSTP Enhancement Implementation of legacy path cost MIB and CLI option for MSTP.

Release K.11.13 through K.11.32 Enhancements

No enhancements, software fixes only.

Release K.11.33 Enhancements

- With the K.11.33 software release, support for the following ProCurve products was added:
  - J8698A / J8700A(bundle) for the ProCurve switch 5412zl
  - J8706A - ProCurve Switch 5400zl 24p Mini-GBIC Module
  - J8708A - ProCurve Switch 5400zl 4p 10-GbE CX4 Module
  - J8992A - ProCurve Switch 6200yl-24G-mGBIC

Release K.11.34 Enhancements

Release K.11.34 includes the following enhancements:

- **Increased number of Telnet/SSH sessions**: The maximum number of simultaneous Telnet/SSH sessions has been increased from three to five. The CLI commands **show telnet** and **show ip ssh** now report on five sessions rather than just three.

- **CLI-configured sFlow with multiple instances:** In earlier software releases, the only method for configuring sFlow on the switch was via SNMP using only a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to three distinct sFlow instances. For more information, refer to the section on "CLI-Configured sFlow with Multiple Instances" in the chapter titled "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.
- **Event log display options**: Two new options have been added to provide greater flexibility in viewing event log entries via the CLI. The **show logging** command now includes an option to reverse the standard display, and a **clear logging** command has been added to remove all event log entries from the **show logging** display output. For more information, refer to the section on "Using the Event Log To Identify Problem Sources" in the Appendix titled "Troubleshooting" in the *Management and Configuration Guide* for your switch.
- **Scheduled reload:** Additional parameters have been added to the **reload** command to allow for a scheduled reboot of the switch via the CLI. For more information, refer to the section on "Rebooting your Switch" in the Chapter titled "Switch Memory and Configuration" in the *Management and Configuration Guide* for your switch.
- **Real-time rate display:** The **show interface port-utilization** command provides a real-time rate display for all ports on the switch.

Release K.11.35 Enhancements

Release K.11.35 includes the following enhancement:

- Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.

Release K.11.36 through K.11.39 Enhancements

No new enhancements, software fixes only.

Release K.11.40 Enhancements

Release K.11.40 includes the following enhancement:

- **RSTP/MSTP BPDU Protection**: When this feature is enabled on a port, the switch will disable (drop the link) of a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP trap.

Release K.11.41 Enhancements

Release K.11.43 includes the following enhancement:

- Added support for Unidirectional Fiber Break Detection (UDLD).

Release K.11.42 Enhancements

No enhancements, software fixes only.

Release K.11.43 Enhancements

Release K.11.43 includes the following enhancement:

- 802.1X Controlled Directions enhancement. With this change, Administrators can use "Wake-on-LAN" with computers that are connected to ports configured for 802.1X authentication.

Release K.11.44 Enhancements

Release K.11.44 includes the following enhancement:

- Loop Protection enhancement allows STP to detect and block network topology loops on a single port.

Release K.11.45 Through K.11.47 Enhancements

No enhancements, software fixes only.

Release K.11.48 Enhancements

Release K.11.48 includes the following enhancement:

- The **show tech transceiver** CLI command output now contains the HP part number and revision information for all transceivers (mGBICs) on the switch.

Release K.11.49 Enhancements

Release K.11.49 includes the following enhancement:

- DHCP Protection (Snooping) enhancement.

Release K.11.60 through K.11.63 Enhancements

No enhancements, software fixes only.

- Versions K.11.50 through K.11.59 were never built.
- Version K.11.60 was never released.

Release K.11.64 Enhancements

Release K.11.64 includes the following enhancement:

- Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

Release K.11.68 Enhancements

Release K.11.68 includes the following enhancement:

- Improved SFlow function to accommodate bursty traffic.

Release K.11.69 Enhancements

No new enhancements, software fixes only.

Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0*x* code branch with no intervening releases.

Release K.12.01 Enhancements

Release K.12.01 is a major software update containing many new features and enhancements to existing features. The following updates have been documented in the latest revisions to the manuals (February 2007). Refer to the manuals for additional details.

Software Manual/ Enhancements	Description
Management and Configuration Guide	
Bi-directional Rate Limiting:	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
Loopback Interface:	A virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. By default, each switch has an internal loopback interface (lo0). You can configure up to seven other loopback interfaces on the switch.
USB Support	Provides an option for using a USB device as a source or destination for file transfers. Refer to "Using USB To Download Switch Software" in the "File Transfers" appendix of the *Management and Configuration Guide* for your switch (February 2007 or newer). For information on USB device compatibility on the 3500yl, 5400zl, and 6200yl switches, refer to the HP ProCurve support Website: **http://www.hp.com/rnd/support/faqs/index.htm**.
Intelligent Mirroring	Enables copying of network traffic from a network interface to a local or remote exit port where a host such as a traffic analyzer or intrusion detection system (IDS) is connected.
DNS Resolver	Used in local network domains to enable the use of a hostname or fully-qualified domain name to perform ping and traceroute operations from the switch.
SNMP-Server Source IP Commands:	Provides added security by allowing you to send SNMP replies from the same IP address as the one on which the corresponding SNMP request was received.
SNMPv3 AES Support:	Authentication and privacy for SNMPv3 users has been enhanced to support AES 128-bit encryption as a privacy protocol in SNMPv3 messages in compliance with RFC 3826.
Multicast and Routing Guide	
OSPF NSAA:	Support for Not-So-Stubby-Areas (NSAA).
DHCP Relay:	Enhancements to the DHCP Relay feature allow you to disable the hop count in DHCP requests, and enable support for up to 2048 IP helper addresses of DHCP servers.

Software Manual/ Enhancements	Description
Advanced Traffic Management Guide	
Qos Queue Config:	Allows you to reduce the number of outbound queues that all switch ports will use to buffer packets for 802.1p user priorities.
Number of Default VLANs:	In the factory default state, support has been increased from 8 VLANs to 256 VLANs. (You can reconfigure the switch to support up to 2048 (vids up to 4094) VLANs.)
Migrating Layer 3 VLANs Using VLAN MAC Configuration:	Allows you to upgrade to ProCurve routing switches without stopping the operation of attached hosts that use existing routers as their default gateway to route traffic between VLANs.
Access Security Guide	
RADIUS AAA:	Provides client-level security that allows LAN access to individual 802.1X clients (up to 32 per port), where each client gains access to the LAN by entering valid user credentials. This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated.
SNMP Access to Switch Authentication features:	Enables manager read/write access for a subset of the SNMP MIB objects for switch authentication features. **Security Note:** Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. For more information, or to disable this feature see"Support Notes" on page 17 for details.
Password Set via SNMP:	Allows configuration of username and password via SNMP.
Client-based Access Control:	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
Virus Throttling on Bridged Traffic:	This enhancement allows connection-rate filtering on all IP traffic (not just routed traffic as in earlier releases).
ACLs on Port Traffic and Bridged Traffic:	Allows configuration of ACLs to filter traffic entering the switch on a VLAN or port.
Dynamic ARP Protection:	Protects your network from ARP cache poisoning by dropping packets, with an invalid IP-to-MAC address binding, that are received on untrusted ports.
Instrumentation Monitor:	Protects your network from a variety of common attacks by generating alerts for detected anomalies on the switch.

Software Manual/ Enhancements	Description
Controlled Directions Web/MAC Auth:	Allows you to use the aaa port-access controlled-directions command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state. This feature is available for both 802.1X and Web/MAC authorization.
Note on Manual Updates: In addition to the above updates to the manuals, the chapter on ACLs has been moved from the *Advanced Traffic Management Guide* to the *Access Security Guide*. The *Access Security Guide* also provides a new introductory "Security Overview" chapter, plus a new chapter on "Advanced Threat Protection" covering topics such as DHCP Snooping and Dynamic Arp Protection.	

In addition to the updates listed above, K.12.01 also provides the following enhancements:

- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR_1000373226)** — Support was added for the ProCurve 100-FX SFP-LC Transceiver (J9054B).
- **Enhancement (PR_1000376626)** — Enhance CLI **qos dscp-map help** and **show dscp-map** text to warn the user that inbound classification based on DSCP code points only occurs if **qos type-of-service diff-services** is also configured.

Release K.12.02 Enhancements

No enhancements, software fixes only.

Release K.12.03 Enhancements

Release K.12.03 includes the following enhancements:

- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.
- **Enhancement (PR_1000398393)** — For the **interface <*port-list*> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.
- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports.

  qos <udp-port | tcp-port> < *tcp/udp port number* | range <*tcp/udp port number* > <*tcp/udp port number* > > priority < 0 - 7>

For more information, refer to "QoS TCP/UDP Priority" in the *Advanced Traffic Management Guide*.

Release K.12.04 Enhancements

Release K.12.04 includes the following enhancement:

- **Enhancement MSTP (PR_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution. For more information on selected configuration options and updated MSTP port parameters, see "Configuring MSTP Port Connectivity Parameters" below.

Configuring MSTP Port Connectivity Parameters

With release K.12.04, all ports are configured as auto-edge-ports by default, and the spanning tree **edge-port** option has been removed. This section describes selected **spanning-tree <*port-list*>** command parameters for enhanced operation.

Basic port connectivity parameters affect spanning-tree links at the global level. Therefore, in most cases, ProCurve recommends that you use the revised default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links (for example, see the **root-guard** option below).

To display the spanning-tree settings for each port, use the **show spanning-tree config** command.

Syntax: [no] spanning-tree < *port-list* > < auto-edge-port | admin-edge-port | mcheck | root-guard | tcn-guard >

[auto-edge-port]

Enables **auto-edge-port** *operation for MSTP, and supports the automatic detection of edge ports. (Default:* **Yes**, *enabled)*

The port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets. If **admin-edge-port** *is enabled for a port, the setting for* **auto-edge-port** *is ignored whether set to yes or no. If* **admin-edge-port** *is disabled, and* **auto-edge-port** *has not been disabled, then the* **auto-edge-port** *setting controls the behavior of the port.*

The **no spanning-tree < *port-list* > auto-edge-port** *command disables* **auto-edge-port** *operation on the specified ports.*

[admin-edge-port]

Enables **admin-edge-port** *for RSTP/MSTP. If a bridge or switch is detected on the segment, the port automatically operates as non-edge, not enabled. (Default:* **No** *- disabled)*

If **admin-edge-port** *is disabled on a port and* **auto-edge-port** *has not been disabled, the* **auto-edge-port** *setting controls the behavior of the port.*

The **no spanning-tree < *port-list* > admin-edge-port** *command disables* **admin-edge-port** *operation on the specified ports.*

[mcheck]

Forces a port to send RSTP/MSTP BPDUs for 3 seconds. This allows for another switch connected to the port and running RSTP to establish its connection quickly and for identifying switches running 802.1D STP. If the whole-switch force-version parameter is set to stp-compatible, the switch ignores the mcheck setting and sends 802.1D STP BPDUs out all ports.

[root-guard]

MSTP only. When a port is enabled as **root-guard**, *it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior STP BPDUs. The BPDUs received on a* **root-guard** *port are ignored. All other BPDUs are accepted and the external devices may belong to the spanning tree as long as they do not claim to be the Root device. (Default:* **No** *- disabled)*

Note: *In standard Spanning Tree Protocol operation, the calculation of active network topologies may be an issue when switches outside the core region of a network are under shared or limited administrative control. Such a switch may become a Root Bridge for the entire network and create non-optimal forwarding paths. By enabling the* **root-guard** *feature on ports that face outside the core network, external boundaries for the core network are created to ensure the Root Bridge is located within the core network.*

[tcn-guard]

When **tcn-guard** *is enabled for a port, it causes the port to stop propagating received topology change notifications and topology changes to other ports. (Default:* **No** *- disabled)*

Syntax: spanning-tree < *port-list* > < hello-time | path-cost | point-to-point-mac | priority >

[hello-time < global | 1 - 10 >

When the switch is the CIST root, this parameter specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports. This interval also applies to all ports in all switches downstream from each port in the < *port-list* >*. A setting of* **global** *indicates that the ports in* < *port-list* > *on the CIST root are using the value set by the global spanning-tree* **hello-time** *value. When a given switch "X" is not the CIST root, the per-port* **hello-time** *for all active ports on switch "X" is propagated from the CIST root, and is the same as the* **hello-time** *in use on the CIST root port in the currently active path from switch "X" to the CIST root. (That is, when switch "X" is not the CIST root, then the upstream CIST root's port* **hello-time** *setting overrides the* **hello-time** *setting configured on switch "X". (Default Per-Port setting:* **Use Global***. Default Global Hello-Time:* **2***.)*

[path-cost < auto | 1.200000000 >]

Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree. In the default configuration (auto) the switch determines a port's path cost by the port's type:

- *10 Mbps:* **2000000**
- *100 Mbps:* **200000**
- *1 Gbps:* **20000**

point-to-point-mac <true | false | auto >

This parameter informs the switch of the type of device to which a specific port connects.

True ***(default)****: Indicates a point-to-point link to a device such as a switch, bridge, or end-node.*

False*: Indicates a connection to a hub (which is a shared LAN segment).*

Auto: *Causes the switch to set False on the port if it is not running at full duplex. (Connections to hubs are half-duplex.)*

priority < 0.15 >

MSTP uses this parameter to determine the port(s) to use for forwarding. The port with the lowest assigned value has the highest priority. While the actual priority range is 0 to 240, this command specifies the priority as a multiplier (0-15) of 16. That is, when you specify a priority multiplier of 0-15, the actual priority assigned to the switch is:

(priority-multiplier) x 16 = priority

The default priority-multiplier value is 8.

*For example, if you configure "***2***" as the priority multiplier for a given port, then the actual priority is 32. Thus, after you specify the port priority multiplier, the switch displays the actual port priority (and not the multiplier) in the* **show spanning-tree config** *display. You can view the actual multiplier setting for ports by executing* **show running** *and looking for an entry in this form:*

spanning-tree <*port-list*> priority <*priority-multiplier*>

For example, configuring port 2 with a priority multiplier of "3" results in this line in the **show running-config** *output:*

```
spanning-tree B2 priority 3
```

Release K.12.05 Enhancements

Release K.12.05 includes the following enhancement:

- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. For more information, see "How RADIUS-Based Authentication Affects VLAN Operation" below.

How RADIUS-Based Authentication Affects VLAN Operation

Using a RADIUS server to authenticate clients, you can provide port-level security protection from unauthorized network access for the following authentication methods:

- 802.1X: Port-based or client-based access control to open a port for client access after authenticating valid user credentials.
- MAC address: Authenticates a device's MAC address to grant access to the network.
- Web-browser interface: Authenticates clients for network access using a Web page for user login.

Note

You can use 802.1X (port-based or client-based) authentication and either Web or MAC authentication at the same time on a port, with a maximum of 32 clients allowed on the port. (The default is one client.) Web authentication and MAC authentication are mutually exclusive on the same port. Also, you must disable LACP on ports configured for any of these authentication methods. For more information, refer to the "Configuring Port-Based and User-Based Access Control (802.1X)" and "Web and MAC Authentication" chapters of the *Access Security Guide*.

VLAN Assignment on a ProCurve Port

Following client authentication, VLAN configurations on a ProCurve port are managed as follows when you use 802.1X, MAC, or Web authentication:

- The port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. Tagged VLAN membership allows a port to be a member of multiple VLANs simultaneously.
- The port is temporarily assigned as a member of an untagged (static or dynamic) VLAN for use during the client session according to the following order of options.
  a. The port joins the VLAN to which it has been assigned by a RADIUS server during client authentication.
  b. If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the authorized-client VLAN configured for the authentication method.
  c. If the port does not have an authorized-client VLAN configured, but is configured for membership in an untagged VLAN, the switch assigns the port to this untagged VLAN.

Operating Notes

- During client authentication, a port assigned to a VLAN by a RADIUS server or an authorized-client VLAN configuration is an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN. The following restrictions apply:
  - If the port is assigned as a member of an untagged *static* VLAN, the VLAN must already be configured on the switch. If the static VLAN configuration does not exist, the authentication fails.
  - If the port is assigned as a member of an untagged *dynamic* VLAN that was learned through GVRP, the dynamic VLAN configuration must exist on the switch at the time of authentication and GVRP-learned dynamic VLANs for port-access authentication must be enabled

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

- To enable the use of a GVRP-learned (dynamic) VLAN as the untagged VLAN used in an authentication session, enter the **aaa port-access gvrp-vlans** command, as described in "Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions" on page 42.

- Enabling the use of dynamic VLANs in an authentication session offers the following benefits:

  - You avoid the need of having static VLANs pre-configured on the switch.
  - You can centralize the administration of user accounts (including user VLAN IDs) on a RADIUS server.

  For information on how to enable the switch to dynamically create 802.1Q-compliant VLANs on links to other devices using the GARP VLAN Registration Protocol (GVRP), refer to the "GVRP" chapter in the *Advanced Traffic Management Guide*.

- For an authentication session to proceed, a ProCurve port must be an untagged member of the (static or dynamic) VLAN assigned by the RADIUS server (or an authorized-client VLAN configuration). The port temporarily drops any current untagged VLAN membership.

  If the port is not already a member of the RADIUS-assigned (static or dynamic) untagged VLAN, the switch temporarily reassigns the port as an untagged member of the required VLAN (for the duration of the session). *At the same time, if the ProCurve port is already configured as an untagged member of a different VLAN, the port loses access to the other VLAN for the duration of the session.* (A port can be an untagged member of only one VLAN at a time.)

  When the authentication session ends, the switch removes the temporary untagged VLAN assignment and re-activates the temporarily disabled, untagged VLAN assignment.

- If GVRP is already enabled on the switch, the temporary untagged (static or dynamic) VLAN created on the port for the authentication session is advertised as an existing VLAN.

  If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in "Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session" on page 39), the disabled VLAN assignment is not advertised. When the authentication session ends, the switch:

  - Removes the temporary untagged VLAN assignment and stops advertising it.
  - Re-activates and resumes advertising the temporarily disabled, untagged VLAN assignment.

- If you modify a VLAN ID configuration on a port during an 802.1X, MAC, or Web authentication session, the changes do not take effect until the session ends.

- When a switch port is configured with RADIUS-based authentication to accept multiple 802.1X and/or MAC or Web authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session.

Therefore, on a port where one or more authenticated client sessions are already running, all such clients are on the same untagged VLAN. If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail. For more on this topic, refer to "802.1X Open VLAN Mode" in the "Configuring Port-Based and Client-Based Access Control (802.1X)" chapter in the *Access Security Guide*.

Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session

The following example shows how an untagged static VLAN is temporarily assigned to a port for use during an 802.1X authentication session. In the example, an 802.1X-aware client on port A2 has been authenticated by a RADIUS server for access to VLAN 22. However, port A2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in Figure 1.

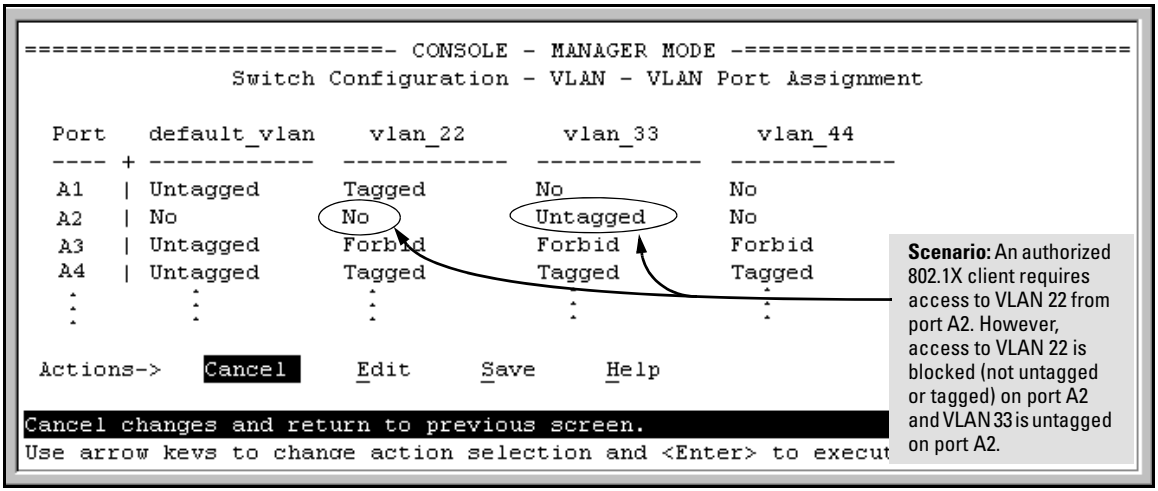

Figure 1. Example of an Active VLAN Configuration in the Menu Interface View

In Figure 1, if RADIUS authorizes an 802.1X client on port A2 with the requirement that the client use VLAN 22, then:

- VLAN 22 becomes available as Untagged on port A2 for the duration of the session.
- VLAN 33 becomes unavailable to port A2 for the duration of the session (because there can be only one untagged VLAN on any port).

To view the temporary VLAN assignment as a change in the active configuration, use the **show vlan <*vlan-id*>** command as shown in Figure 2, where **<*vlan-id*>** is the (static or dynamic) VLAN used in the authenticated client session.

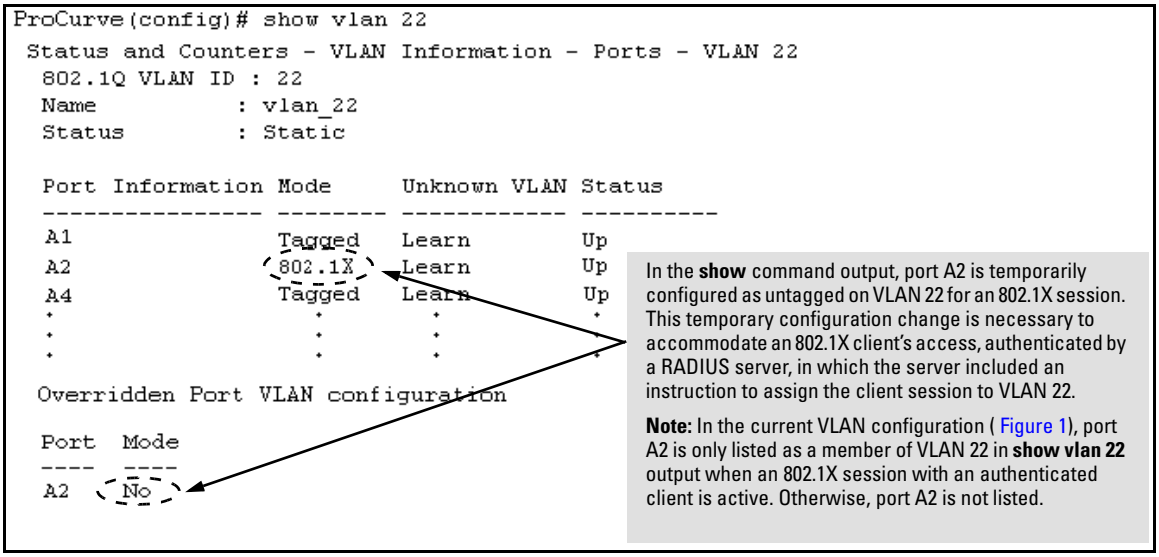

Figure 2. Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session

However, as shown in Figure 1, because VLAN 33 is configured as untagged on port A2 and because a port can be untagged on only one VLAN, port A2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of access to VLAN 33 by entering the **show vlan 33** command as shown in Figure 3.

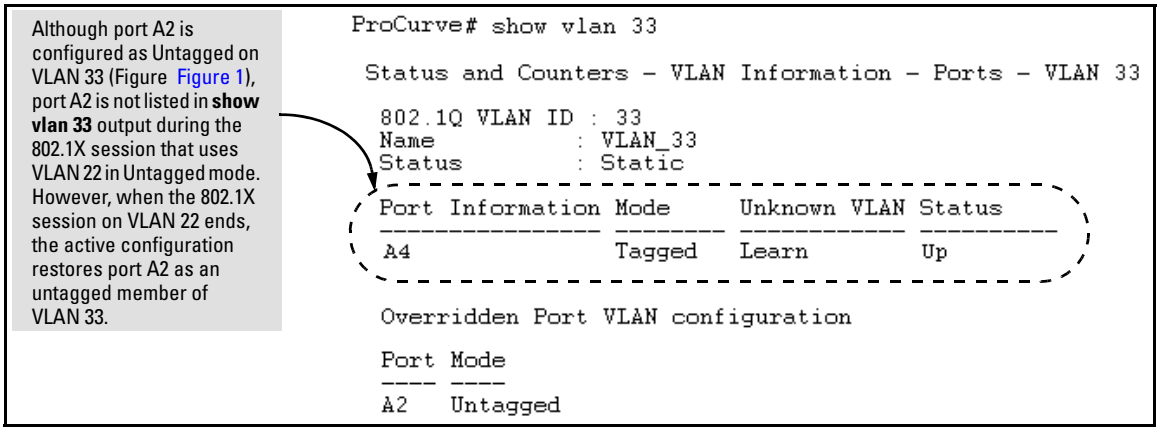

Figure 3. Active Configuration for VLAN 33 Temporarily Drops Port 22 for the 802.1X Session

When the 802.1X client session on port A2 ends, the port removes the temporary untagged VLAN membership. The static VLAN (VLAN 33) that is "permanently" configured as untagged on the port becomes available again. Therefore, when the RADIUS-authenticated 802.1X session on port A2 ends, VLAN 22 access on port A2 also ends, and the untagged VLAN 33 access on port A2 is restored as shown in Figure 4.

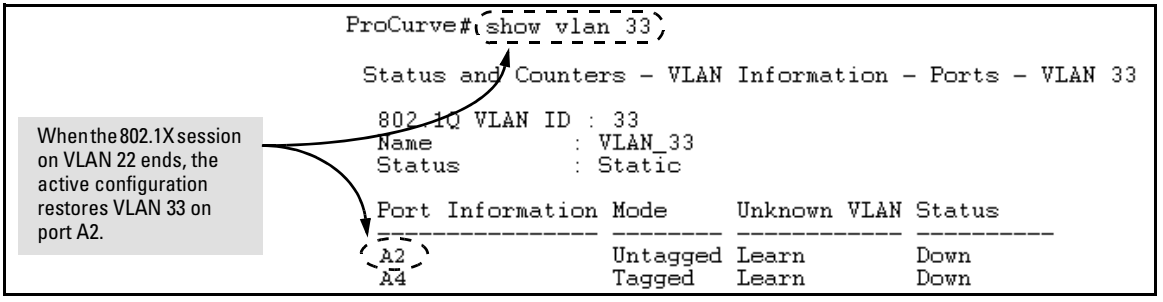

Figure 4. The Active Configuration for VLAN 33 Restores Port A2 After the 802.1X Session Ends

Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions

Syntax: aaa port-access gvrp-vlans

Enables the use of dynamic VLANs (learned through GVRP) in the temporary untagged VLAN assigned by a RADIUS server on an authenticated port in an 802.1X, MAC, or Web authentication session.

Enter the **no** *form of this command to disable the use of GVRP-learned VLANs in an authentication session.*

For information on how to enable a switch to dynamically create 802.1Q-compliant VLANs, refer to the "GVRP" chapter in the Access Security Guide.

Notes:

1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic VLAN configuration must exist at the time of authentication and GVRP for port-access authentication must be enabled on the switch.

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

2. After you enable dynamic VLAN assignment in an authentication session, it is recommended that you use the **interface unknown-vlans** *command on a per-port basis to prevent denial-of-service attacks. The* **interface unknown-vlans** *command allows you to:*

- *Disable the port from sending advertisements of existing GVRP-created VLANs on the switch.*
- *Drop all GVRP advertisements received on the port.*

For more information, refer to the "GVRP" chapter in the Advanced Traffic Management Guide.

3. If you disable the use of dynamic VLANs in an authentication session using the **no aaa port-access gvrp-vlans** *command, client sessions that were authenticated with a dynamic VLAN continue and are not deauthenticated.*

(This behavior differs form how static VLAN assignment is handled in an authentication session. If you remove the configuration of the static VLAN used to create a temporary client session, the 802.1X, MAC, or Web authenticated client is deauthenticated.)

However, if a RADIUS-configured dynamic VLAN used for an authentication session is deleted from the switch through normal GVRP operation (for example, if no GVRP advertisements for the VLAN are received on any switch port), authenticated clients using this VLAN are deauthenticated.

For information on how static and dynamic VLANs are assigned in a RADIUS-based 802.1X, MAC, or Web authentication session, refer to the "How RADIUS-Based Authentication Affects VLAN Operation" section in the "RADIUS Authentication and Accounting" chapter of the Access Security Guide.

Release K.12.06 Enhancements

Release K.12.06 includes the following enhancement:

- **Enhancement (PR_1000308332)** — Passwords (hashed) can be saved to the configuration file.

Saving Security Credentials in a Configuration File

In software release K.12.06 and greater, you can store and view the following security settings in the running-config file associated with the current software image by entering the **include-credentials** command. Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.

- Local manager and operator passwords and (optional) user names that control access to a management session on the switch through the CLI, menu interface, or Web browser interface
- SNMP security credentials used by network management stations to access a switch, including authentication and privacy passwords
- Port-access passwords and usernames used as 802.1X authentication credentials for access to the switch
- TACACS+ encryption keys used to encrypt packets and secure authentication sessions with TACACS+ servers
- RADIUS shared secret (encryption) keys used to encrypt packets and secure authentication sessions with RADIUS servers
- Secure Shell (SSH) public keys used to authenticate SSH clients that try to connect to the switch.

Benefits of Saving Security Credentials

The benefits of including and saving security credentials in a configuration file are as follows:

- After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.
- By permanently saving a switch's security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the ProCurve switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.

- By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files by changing the configuration file used when you reboot the switch.

For more information about how to experiment with, upload, download, and use configuration files with different software versions, refer to the following chapters:

- "Switch Memory and Configuration" and "File Transfers" in the *Management and Configuration Guide*
- "Configuring Username and Password Security" in the *Access Security Guide*

Security Settings that Can Be Saved

This section describes the security settings that can be saved to a configuration file in software release K.12.06 and greater:

- Local manager and operator passwords and user names
- SNMP security credentials, including SNMPv1 community names and SNMPv3 usernames, authentication, and privacy settings
- 802.1X port-access passwords and usernames
- TACACS+ encryption keys
- RADIUS shared secret (encryption) keys
- Public keys of SSH-enabled management stations that are used by the switch to authenticate SSH clients that try to connect to the switch

Local Manager and Operator Passwords

In software releases earlier than K.12.06, the manager and operator passwords and user names used to start a management session on the switch are treated as follows:

- You set the passwords and (optional) user names using the CLI or menu interface as described in "Configuring Local Password Security" in the *Access Security Guide*.
- Only the following information is saved to the running configuration:

```
password manager [user-name <name>]
password operator [user-name <name>]
```

In software release K.12.06 and greater, you cannot view the configured local password settings in plain text. However, by entering the **include-credentials** command described later, you can view a hash of the local password settings in the running-config file, in the format:

```
password manager [user-name <name>] <hash-type> <pass-hash>
password operator [user-name <name>] <hash-type> <pass-hash>
```

Where:
<*name*> is an alphanumeric string for the user name assigned to the manager or operator.
<*hash-type*> indicates the type of hash algorithm used: SHA-1.
<*pass-hash*> is the SHA-1 authentication protocol's hash of the password.

For example, a manager username and password may be stored in a running-config file as follows:

```
password manager user-name Spock SHA1
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

If you permanently save password configurations in the startup-config file by entering the **write memory** command, the passwords take effect when a switch boots with the software version associated with the configuration file.

Caution

If a startup configuration file does not contain a manager or operator password, the switch will not have password protection and can be accessed through Telnet, the serial port, or Web interface with full manager privileges.

Password Command

In software release K.12.06 and greater, the **password** command in the CLI is enhanced to support the following syntax:

Syntax: [no] password <manager | operator | port-access> [user-name <*name*>] <hash-type> <*password*>

Where:

- **manager** configures access to the switch with manager-level privileges.
- **operator** configures access to the switch with operator-level privileges.
- **port-access** configures access to the switch through 802.1X authentication with operator-level privileges.
- **user-name <*name*>** is the (optional) text string of the user name associated with the password.

- The **<*hash-type*>** parameter specifies the type of algorithm (if any) used to hash the password. Valid values are **plaintext** or **sha-1**.
- The **<*password*>** parameter is the clear ASCII text string or SHA-1 hash of the password.

  You can enter a manager/operator password in clear ASCII text or hashed format, while the port-access password must be clear ASCII text only. Manager and operator passwords are displayed and saved in a configuration file only in hashed format; port-access passwords are displayed and saved only as plain ASCII text.

After you enter the complete command syntax that includes the password, the password is set and you are not prompted to enter the password a second time.

This command enhancement allows you to configure manager, operator, and 802.1X port-access passwords using the CLI in only one step (instead of entering the **password** command and then being prompted twice to enter the actual password, as in software releases earlier than K.12.06).

- For more information about configuring local manager and operator passwords, refer to the "Configuring Username and Password Security" chapter in the *Access Security Guide*.
- For more information about configuring a port-access password for 802.1X client authentication, see "802.1X Port-Access Credentials" on page 47.

SNMP Security Credentials

In software releases earlier than K.12.06, SNMP security credentials are saved in a configuration file as follows:

- SNMPv1 community names and write-access settings are saved as shown in the following example:

  ```
  snmp-server community "vulcan" Unrestricted
  ```

- SNMPv3 authorization and privacy protocols and passwords used with each SNMPv3 user are not saved. However, SNMPv3 user names are saved; for example:

  ```
  snmpv3 user "initial"
  ```

In software release K.12.06 and greater, SNMPv1 community names and write-access settings, and SNMPv3 usernames are still saved in the running configuration when you enter the **include-credentials** command.

In addition, the following SNMPv3 security parameters are also saved:

```
snmpv3 user "<name>" [auth <md5|sha> "<auth-pass>"] [priv "<priv-pass>"]
```

Where:
<*name*> is the name of an SNMPv3 management station.
auth <md5 | sha> is the (optional) authentication method used for the management station.

<auth-pass> is the hashed authentication password used with the configured authentication method. **priv "*<priv-pass>*"** is the (optional) hashed privacy password used by a privacy protocol to encrypt SNMPv3 messages between the switch and the station.

The following example shows the additional security credentials for SNMPv3 users that can be saved in a running-config file:

```
snmpv3 user boris \
auth md5 “9e4cfef901f21cf9d21079debeca453” \
priv “82ca4dc99e782db1a1e914f5d8f16824”

snmpv3 user alan \
auth sha “8db06202b8f293e9bc0c00ac98cf91099708ecdf” \
priv “5bc4313e9fd7c2953aaea9406764fe8bb629a538”
```

Figure 5. Security Credentials for SNMPv3

Although you can enter an SNMPv3 authentication or privacy password in either clear ASCII text or the SHA-1 hash of the password, the password is displayed and saved in a configuration file only in hashed format, as shown in the preceding example.

For more information about the configuration of SNMP security parameters, refer to the “Configuring for Network Management Applications” chapter in the *Management and Configuration Guide*.

802.1X Port-Access Credentials

In software release K.12.06 and greater, 802.1X authenticator (port-access) credentials can be stored in a configuration file.

802.1X *authenticator* credentials are used by a port to authenticate supplicants requesting a point-to-point connection to the switch. 802.1X *supplicant* credentials are used by the switch to establish a point-to-point connection to a port on another 802.1X-aware switch. Only 802.1X authenticator credentials are stored in a configuration file. For information about how to use 802.1X on the switch both as an authenticator and a supplicant, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

In software release K.12.06 and greater, the local password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access)** is introduced to configure the local operator username and password used as 802.1X authentication credentials for access to the switch.

The **password port-access** values are now configured separately from the manager and operator passwords configured with the **password manager** and **password operator** commands and used for management access to the switch. For information on the new **password** command syntax, see “Password Command” on page 45.

After you enter the complete **password port-access** command syntax, the password is set. You are not prompted to enter the password a second time.

TACACS+ Encryption Key Authentication

You can use TACACS+ servers to authenticate users who request access to a switch through Telnet (remote) or console (local) sessions. TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local manager and operator passwords configured on the switch.

When you configure TACACS+, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so.

For improved security, you can configure a global or server-specific encryption key that encrypts data in TACACS+ packets transmitted between a switch and a RADIUS server during authentication sessions. The key configured on the switch must match the encryption key configured in each TACACS+ server application. (The encryption key is sometimes referred to as "shared secret" or "secret" key.) For more information, refer to the "TACACS+ Authentication" chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, the global and server-specific TACACS+ encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show tacacs** command.

In software release K.12.06 and greater, TACACS+ shared secret (encryption) keys can be saved in a configuration file with the following syntax:

```
tacacs-server key <keystring>
```

Where:
<keystring> is the encryption key (in clear text) used for secure communication with all or a specific TACACS+ server.

RADIUS Shared-Secret Key Authentication

You can use RADIUS servers as the primary authentication method for users who request access to a switch through Telnet, SSH, Web interface, console, or port-access (802.1X). The shared secret key is a text string used to encrypt data in RADIUS packets transmitted between a switch and a RADIUS server during authentication sessions. Both the switch and the server have a copy of the key; the key is never transmitted across the network. For more information, refer to the "RADIUS Authentication and Accounting" chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, the global and server-specific RADIUS encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show radius** command.

In software release K.12.06 and greater, RADIUS shared secret (encryption) keys can be saved in a configuration file with the following syntax:

radius-server key <*keystring*>

Where:
<keystring> is the encryption key (in clear text) used for secure communication with all or a specific RADIUS server.

SSH Client Public-Key Authentication

Secure Shell version 2 (SSHv2) is used by ProCurve switches to provide remote access to SSH-enabled management stations. Although SSH provides Telnet-like functions, unlike Telnet, SSH provides encrypted, two-way authenticated transactions. SSH client public-key authentication is one of the types of authentication used.

Client public-key authentication uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a public key stored on the switch can gain access at the manager or operator level. For more information about how to configure and use SSH public keys to authenticate SSH clients that try to connect to the switch, refer to the "Configuring Secure Shell" chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, client public-keys that are used to authenticate SSH clients are only stored in flash memory, not in the running-config file. You can view the SSH public keys stored on a switch by entering the **show crypto client-public-key** command. The only SSH security credential that is stored in the running configuration are the following commands:

aaa authentication ssh login public-key

aaa authentication ssh enable public-key

- The **aaa authentication ssh login public-key** command allows operator access using SSH public-key authentication.
- The **aaa authentication ssh enable public-key** command allows manager access using SSH public-key authentication.

In software release K.12.06 and greater, the SSH security credential that is stored in the running configuration is the syntax of the **ip ssh public-key** command used to authenticate SSH clients for manager or operator access, along with the hashed content of each SSH client public-key. The syntax of the **ip ssh public-key** command is as follows:

ip ssh public-key <manager|operator> <*keystring*>

Where:
manager allows manager-level access using SSH public-key authentication.
operator allows operator-level access using SSH public-key authentication.
<keystring> is a legal SSHv2 (RSA or DSA) public key. The text string for the public key must be a single quoted token.

If the keystring contains double-quotes, it can be quoted with single quotes ('*keystring*'). The following restrictions for a keystring apply:

- A keystring cannot contain both single and double quotes.
- A keystring cannot have extra characters, such as a blank space or a new line. However, to improve readability, you can add a backlash at the end of each line.

Note

In software release K.12.01 and earlier, you can add up to ten SSH client public-keys to the switch only by using the **copy** command; for example:

```
$ copy tftp public-key ip-addr filename <manager|operator> [append]
```

If you enter the optional **append** keyword, the transmitted public-keys are added to existing SSH public-key configurations. If you omit the **append** keyword, the transmitted keys overwrite existing SSH public-key configurations.

In software release K.12.06 and greater, the **ip ssh public-key** command allows you to configure only one SSH client public-key at a time. (This command behavior differs from the **copy** command, which in earlier software releases allows you to load up to ten SSH client public-key configurations at once if they are stored in a single file on a TFTP server.) Therefore, the **ip ssh public-key** command behavior includes an implicit append that never overwrites existing public-key configurations on a running switch.

In all software releases, if you download a software configuration file that contains SSH client public-key configurations, the downloaded public-keys overwrite any existing keys, as happens with any other configured values.

To display the SSH public-key configurations (72 characters per line) stored in a configuration file, enter the **show config** or **show running-config** command. The following example shows the SSH public keys configured for manager access, along with the hashed content of each SSH client public-key, that are stored in a configuration file:

```
...
include-credentials
ip ssh public-key manager “ssh-dss \
AAAAB3NzaC1kc3MAAACBAPwJHSJmTRtpZ9BUNC+ZrsxhMuZEXQhaDME1vc/ \
EvYnTKxQ31bWvr/bT7W58NX/YJ1ZKTV2GZ2QJCicUUZVWjNFJCsa0v03XS4 \
BhkXjtHhz6gD701otgizUOO6/Xzf4/J9XkJHkOCnbHIqtB1sbRYBTxj3NzA \
K1ymvIaU09X5TDAAAAFQCPwKxnbwFfTPasXnxfvDuLSxaC7wAAAIASBwxUP \
pv2scqPPXQghgaTkdPwGGtdFW/+K4xRskAnIaxuG0qLbnekohi+ND4TkKZd \
EeidgDh7qHusBhOFXM2g73RpE2rNqQnSf/QV95kdNwWIbxuusBAzvfaJptd \
gca6cYR4xS4TuBcaKiorYj60kk144E1fkDWieQx8zABQAAAIEAu7/1kVOdS \
G0vE0eJD23TLXvu94plXhRKCUAvyv2UyK+piG+Q1el1w9zsMaxPA1XJzSY/ \
imEp4p6WXEMcl0lpXMRnkhnuMMpaPMaQUT8NJTNu6hqf/LdQ2kqZjUuIyV9 \
LWyLg5ybS1kFLeOt0oo2Jbpy+U2e4jh2Bb77sX3G5C0= spock@sfc.gov” \
ip ssh public-key manager ‘ssh-rsa \
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDyO9RDD52JZP8k2F2YZXubgwRAN0R \
JRs1Eov6y1RK3XkmgVatzl+mspiEmPS4wNK7bX/IoXNdGrGkoE8tPkxlZOZ \
oqGCf5Zs50P1nkxXvAidFs55AWqOf4MhfCqvtQCe1nt6LFh4ZMig+YewgQG \
M6H1geCSLUbXXSCipdPHysakw== "TectiaClientKey [1024-bit rsa, \
nobody@testmachine, Mon Aug 15 2005 14:47:34]”’
ip ssh public-key manager “ssh-rsa \
AAAAB3NzaC1yc2EAAABIwAAAIEA1Kk9sVQ9LJOR6XO/hCMPxbiMNOK8C/ay \
+SQ10qGw+K9m3w3TmCfjh0ud9hivgbFT4F99AgnQkvm2eVsgoTtLRnfF7uw \
NmpzqOqpHjD9YzItUgSK1uPuFwXMCHKUGKa+G46A+EWxDAIypwVIZ697QmM \
qPFj1zdI4sIo5bDett2d0= joe@hp.com”
...
```

Figure 6. Example of Hashed Content of an SSH Client Public Key

If a switch configuration contains multiple SSH client public keys, each public key is saved as a separate entry in the configuration file. You can configure up to ten SSH client public-keys on a switch.

Enabling the Storage and Display of Security Credentials

To enable the security settings described in "Security Settings that Can Be Saved" on page 44 to be included and viewed in the running configuration on the switch, enter the **include-credentials** command.

Syntax: [no] include-credentials

Enables the inclusion and display of the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys in the running configuration. (Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.)

To view the currently configured security settings in the running configuration, enter one of the following commands:

- **show running-config**: *Displays the configuration settings in the current running-config file.*
- **write terminal**: *Displays the configuration settings in the current running-config file.*

For more information, refer to the "Switch Memory and Configuration" chapter in the Management and Configuration Guide.

To copy the contents of the running-config file from the switch to a USB flash memory device, enter the **copy running-config usb** *command. For more information, refer to the "File Transfers" appendix in the Management and Configuration Guide.*

*The "***no***" form of the command disables only the display and copying of these security parameters from the running configuration, while the security settings remain active in the running configuration.*

Default*: The security credentials described in "Security Settings that Can Be Saved" on page 44 are not stored in the running configuration.*

Operating Notes

Caution

- When you first enter the **include-credentials** command to save the additional security credentials to the running configuration, these settings are moved from internal storage on the switch to the running-config file.

  You are prompted by a warning message to perform a **write memory** operation to save the security credentials to the startup configuration. The message reminds you that if you do not save the current values of these security settings from the running configuration, they will be lost the next time you boot the switch and will revert to the values stored in the startup configuration.

- When you boot a switch with a startup configuration file that contains the **include-credentials** command, any security credentials that are stored in internal flash memory are ignored and erased. The switch will load only the security settings in the startup configuration file, if any.

- In software releases earlier than K.12.06, configuration changes to some security credentials (described in "Security Settings that Can Be Saved" on page 44) are applied immediately and saved in internal storage (flash memory) on the switch. They do not require you to enter the **write memory** command to permanently save them in the startup configuration.

  However, in software release K.12.06 and greater, this switch behavior changes. Security settings are no longer automatically saved internally in flash memory and loaded with the startup configuration when a switch boots up. The configuration of all security credentials requires that you use the **write memory** command to save them in the startup configuration in order for them to not be lost when you log off or reboot the switch. A warning message reminds you to permanently save a security setting, which was formerly automatically saved in internal flash, after you configure it.

- After you enter the **include-credentials** command, the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys are saved in the running configuration.

  Use the **no include-credentials** command to disable the display and copying of these security parameters from the running configuration (using the **show running-config** and **copy running-config** commands), without disabling the configured security settings on the switch.

  After you enter the **include-credentials** command, you can toggle between the non-display and display of security credentials in **show** and **copy** command output by alternately entering the **no include-credentials** and **include-credentials** commands.

- After you permanently save security configurations to the current startup-config file using the **write memory** command, you can view and manage security settings with the following commands:
  - **show config**: Displays the configuration settings in the current startup-config file.
  - **copy config <*source-filename*> config <*target-filename*>**: Makes a local copy of an existing startup-config file by copying the contents of the startup-config file in one memory slot to a new startup-config file in another, empty memory slot.
  - **copy config tftp**: Uploads a configuration file from the switch to a TFTP server.
  - **copy tftp config**: Downloads a configuration file from a TFTP server to the switch.
  - **copy config xmodem**: Uploads a configuration file from the switch to an Xmodem host.
  - **copy xmodem config**: Downloads a configuration file from an Xmodem host to the switch.

  For more information, refer to the "Switch Memory and Configuration" chapter in the *Management and Configuration Guide*.

- The switch supports the storage of up to three configuration files. Each configuration file contains its own security credentials and these security configurations may differ. It is the responsibility of the system administrator to ensure that the appropriate security credentials are contained in the configuration file that is loaded with each software image.
  - When you load a configuration file associated with a software release earlier than K.12.06 on a switch running software release K.12.06 or greater, all security credentials in the configuration file are supported.
  - When you load a configuration file associated with a software release K.12.06 or greater on a switch running a software release earlier than K.12.06, all security credentials saved with the **include-credentials** command are rejected as invalid configurations by the earlier software.

- If you have already enabled the storage of security credentials (including local manager and operator passwords) by entering the **include-credentials** command, the **Reset-on-clear** option is disabled. When you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the running configuration. However, the switch does not reboot after the local passwords are erased. (The **reset-on-clear** option normally reboots the switch when you press the Clear button.)

  For more information about the **Reset-on-clear** option and other front-panel security features, refer to the "Configuring Username and Password Security" chapter in the *Access Security Guide*.

- If you upgrade ProCurve software on a switch from an earlier software release to software release K.12.06 or greater and then enter the **include-credentials** command, security passwords are managed as follows:
  - The manager password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have a manager password configured.
  - The operator password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have an operator password configured.
  - No port-access password for 802.1X authentication is configured. The operator password in the earlier software version is not automatically copied as the new port-access password. To configure password access to the switch through 802.1X authentication, use the **password port-access** command as described in "Password Command" on page 45. (It is not recommended that you use the same password for operator console access and for 802.1X port-access authentication.)
  - The SSH client public-keys for manager and operator access are copied from flash memory into the running configuration.
  - The RADIUS shared secret and TACACS+ encryption keys for access to authentication servers are already included in the running configuration.
  - SNMPv3 user credentials are already included in the running configuration.
- If you downgrade ProCurve software on a switch and use a software release earlier than K.12.06, security passwords are managed as follows:
  - Because SNMPv3 user credentials, RADIUS shared secret keys, and TACACS+ encryption keys are already included in the startup configuration, these security credentials are not lost. They continue to be used in the earlier software version.
  - The local manager and operator passwords are not recognized by an earlier software version and are not saved in the running configuration. However, passwords in inactive configuration files remain stored there. Although they are not displayed in **show config** command output, they are not automatically erased.
  - Although the hashed SSH client public-keys (for manager and operator access) are not recognized by an earlier software version, they remain stored so that they are immediately reloaded if you upgrade back to software release K.12.06 or greater.
  - As in a software upgrade, no port-access (operator) password for 802.1X authentication is saved from software release K.12.06 or greater.

Restrictions

The following restrictions apply when you enable security credentials to be stored in the running configuration with the **include-credentials** command:

- The private keys of an SSH host cannot be stored in the running configuration. Only the public keys used to authenticate SSH clients can be stored. An SSH host's private key is only stored internally; for example, on the switch or on an SSH client device.
- SNMPv3 security credentials saved to a configuration file on a switch cannot be used after downloading the file on a different switch. The SNMPv3 security parameters in the file are only supported when loaded on the same switch for which they were configured.

  The reason is that when SNMPv3 security credentials are saved to a configuration file, they are saved with the engine ID of the switch as shown here:

  ```
  snmpv3 engine-id 00:00:00:0b:00:00:08:00:09:01:10:01
  ```

  If you download a configuration file with saved SNMPv3 security credentials on a switch, when the switch loads the file with the current software version, the SNMPv3 engine ID value in the downloaded file must match the engine ID of the switch in order for the SNMPv3 users to be configured with the authentication and privacy passwords in the file. (To display the engine ID of a switch, enter the **show snmpv3 engine-id** command. To configure authentication and privacy passwords for SNMPv3 users, enter the **snmpv3 user** command.)

  If the engine ID in the saved SNMPv3 security settings in a downloaded configuration file does not match the engine ID of the switch:

  - The SNMPv3 users are configured, but without the authentication and privacy passwords. You must manually configure these passwords on the switch before the users can have SNMPv3 access with the privileges you want.
  - Only the **snmpv3 user <*user_name*>** credentials from the SNMPv3 settings in a downloaded configuration file are loaded on the switch; for example:

    ```
    snmpv3 user boris
    snmpv3 user alan
    ```

- In software release K.12.06 and greater, you can store 802.1X authenticator (port-access) credentials in a configuration file. However, 802.1X supplicant credentials cannot be stored.
- In software release K.12.06 and greater, the local operator password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access)** is introduced to configure the username and password used as 802.1X authentication credentials for access to the switch. You can store the **password port-access** values in the running configuration by using the **include-credentials** command.

Note that the **password port-access** values are configured separately from local operator username and passwords that are configured with the **password operator** command and used for management access to the switch. For more information about how to use the **password port-access** command to configure operator passwords and usernames for 802.1X authentication, refer to the "Configuring Port-Based and Client-Based Access Control (802.1X)" chapter in the *Access Security Guide*.

Release K.12.07 Enhancements

No enhancements, software fixes only.

Release K.12.08 Enhancements

Release K.12.08 includes the following enhancement:

- **Enhancement (PR_1000413764)** — Increase the size of the sysLocation and sysContact entries from 48 to 255 characters.

Configuring a System Contact and Location for the Switch

Both the **system-contact** and the **system-location** fields allow up to 255 characters when configured through the CLI or the Web browser interface.

CLI Command

Syntax: snmp-server [contact <*system-contact*>] [location <*system-location*>]

where < *system-contact* > and <*system-location* > are ASCII strings up to 255 characters each.

Web Browser Interface

Using the Web browser interface for the switch, click the **Configuration** tab, and select **System Info** to access the **System Location** and **System Contact** fields. In each field, you can enter ASCII strings up to 255 characters each. You can view all the characters by using the cursor to scroll through the field.

Menu Interface

Unlike the CLI command and the Web browser interface, the Menu interface will only allow configuration of System Contact and System Location strings of up to 48 characters. However, if a System Contact or System Location string length configured through the CLI command or Web browser interface exceeds 48 characters, the Menu fields will display "+" followed by the last 47 characters of the string. Use the CLI **show running, show config**, or **show system-information** commands to see the complete text string.

Release K.12.09 Enhancements

No enhancements, software fixes only.

Release K.12.10 Enhancements

Release K.12.10 includes the following enhancement:

- **Enhancement (PR_1000419653)** — The **show vlan ports** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged) for each port. See "Show VLAN ports CLI Command Enhancement" below.

Show VLAN ports CLI Command Enhancement

The **show vlan ports** command has been enhanced with an option (**detail**) to display VLAN memberships on a per-port basis when a range of ports is specified in the command. In addition, user-specified port names will be displayed (if assigned), along with tagged or untagged membership modes.

Displaying the VLAN Membership of One or More Ports

This command shows VLAN memberships associated with a port or a group of ports.

Syntax show vlan ports < *port-list* > [detail]

Displays VLAN information for an individual port or a group of ports, either cumulatively or on a detailed per-port basis.

port-list: *Specify a single port number, a range of ports (for example,* **a1-a16***), or* **all**.

detail: *Displays detailed VLAN membership information on a per-port basis.*

Descriptions of items displayed by the command are provided below.

Port name: *The user-specified port name, if one has been assigned.*

VLAN ID: *The VLAN identification number, or VID.*

Name: *The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of* **VLAN-*x*** *where "**x**" matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of* **GVRP_*x*** *where "**x**" matches the applicable VID.*

Status:

Port-Based: *Port-Based, static VLAN*

Protocol: *Protocol-Based, static VLAN*

Dynamic: *Port-Based, temporary VLAN learned through GVRP.*

Voice: *Indicates whether a (port-based) VLAN is configured as a voice VLAN.*

Jumbo: *Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled "Port Traffic Controls" in the* Management and Configuration Guide *for your switch.*

Mode: *Indicates whether a VLAN is tagged or untagged.*

The following examples illustrate the displayed output depending on whether the **detail** option is used.

```
ProCurve# show vlan ports a1-a33

 Status and Counters - VLAN Information - for ports A1-A33

  VLAN ID  Name                | Status     Voice Jumbo
  -------  ------------------- + ---------- ----- -----
  1        DEFAULT_VLAN        | Port-based No    No
  10       VLAN_10             | Port-based Yes   No
  20       VLAN_20             | Protocol   No    No
  33       GVRP_33             | Dynamic    No    No

ProCurve#
```

Figure 7. Example of "Show VLAN Ports" Cumulative Listing

```
 ProCurve# show vlan ports a1-a4 detail

  Status and Counters - VLAN Information - for ports A1

   Port name: Voice_Port
   VLAN ID  Name                | Status     Voice Jumbo Mode
   -------  ------------------- + ---------- ----- ----- ------
   1        DEFAULT_VLAN        | Port-based No    No    Untagged
   10       VLAN_10             | Port-based Yes   No    Tagged

  Status and Counters - VLAN Information - for ports A2

   Port name: Uplink_Port
   VLAN ID  Name                | Status     Voice Jumbo Mode
   -------  ------------------- + ---------- ----- ----- ------
   1        DEFAULT_VLAN        | Port-based No    No    Untagged
   20       VLAN_20             | Protocol   No    No    Tagged
   33       GVRP_33             | Dynamic    No    No    Tagged

  Status and Counters - VLAN Information - for ports A3

   VLAN ID  Name                | Status     Voice Jumbo Mode
```

Figure 8. Example of "Show VLAN Ports" Detail Listing

Release K.12.11 Enhancements

No enhancements, software never released.

Release K.12.12 Enhancements

No enhancements, software fixes only.

Release K.12.13 Enhancements

No enhancements, software never released.

Release K.12.14 Enhancements

No enhancements, software fixes only.

Release K.12.15 Enhancements

Release K.12.15 includes the following enhancement:

- **Enhancement (PR_1000427592)** — This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.

  The IP address of the client is included in the RADIUS accounting packet sent by the switch to the RADIUS server. The client obtains the IP address through DHCP, so DHCP snooping must be enabled for the VLAN of which the client is a member.

- **Enhancement (PR_1000428642)** — The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.

Send SNMP v2c Informs

Enabling and Configuring SNMP Informs

You can use the **snmp-server informs** command (SNMPv2c and SNMPv3 versions) to send notifications when certain events occur. When an SNMP Manager receives an informs request, it can send an SNMP response back to the sending agent. This lets the agent know that the informs request reached its destination and that traps can be sent successfully to that destination.

Informs requests can be sent several times until a response is received from the SNMP manager or the configured retry limits are reached. The request may also timeout.

To enable SNMP informs, enter this command:

Syntax: [no] snmp-server enable informs

Enables or disables the informs option for SNMP.

Default: Disabled

To configure SNMP informs request options, use the following commands.

Syntax: [no] snmp-server informs [retries<retries>] [timeout<seconds>] [pending <pending>]

Allows you to configure options for SNMP informs requests.

retries: Maximum number of times to resend an informs request. Default: 3

timeout: Number of seconds to wait for an acknowledgement before resending the informs request. Default: 30 seconds

pending: *Maximum number of informs waiting for acknowledgement at any one time. When the maximum configured number is reached, older pending informs are discarded. Default: 25*

To specify the manager that receives the informs request, use the **snmp-server host** command.

Syntax: snmp-server host < *ip-address* >[<traps | informs>] [version <1 | 2c | 3>]< *community-string* >

Using community name and destination IP address, this command designates a destination network-management station for receiving SNMP event log messages from the switch. If you do not specify the event level, then the switch does not send event log messages as traps. You can specify up to 10 trap receivers (network management stations).

Note: *In all cases, the switch sends any threshold trap(s) or informs to the network management station(s) that explicitly set the threshold(s).*

[traps | informs>]

Select whether SNMP traps or informs are sent to this management station.

[version <1 | 2c | 3>]

Select the version of SNMP being used.

Note: SNMP informs are supported on version 2c or 3 only.

[<none | all | non-info | critical | debug>]

Options for sending switch Event Log messages to a trap receiver. The levels specified with these options apply only to Event Log messages, and not to threshold traps.

You can see if informs are enabled or disabled with the **show snmp-server** command as shown in Figure 9.

```
ProCurve(config)# show snmp-server
 SNMP Communities
  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Manager  Unrestricted
 Trap Receivers
  Link-Change Traps Enabled on Ports [All] : All
  Send Authentication Traps [No] : No
 ┌ _ _ _ _ _ _ _ _ ┐
 │ Informs [Yes] : Yes │
 └ _ _ _ _ _ _ _ _ ┘
  Address              | Community       Events Sent in Trap
              ----------------------       ----------------
-------------------
 Excluded MIBs

 Snmp Response Pdu Source-IP Information
  Selection Policy   : Default rfc1517
 Trap Pdu Source-IP Information
  Selection Policy   : Default rfc1517
```

Figure 9. Example Showing SNMP Informs Option Enabled

Release K.12.16 Enhancements

No enhancements, software fixes only.

Release K.12.17 Enhancements

No enhancements, software fixes only.

Release K.12.18 Enhancements

Release K.12.18 includes the following enhancement:

- **Enhancement (PR_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 3.2 years). For more information, see the ProCurve *Multicast and Routing Guide*.
- **Enhancement (PR_1000438015)** — The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

Release K.12.19 Enhancements

No enhancements, software fixes only.

Release K.12.20 Enhancements

No enhancements, software fixes only.

Release K.12.21 Enhancements

Release K.12.21 includes the following enhancement:

- **Enhancement (PR_1000440049)** — Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Enhancement (PR_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections. For more information, see the ProCurve *Access Security Guide*.

Release K.12.22 Enhancements

Release K.12.22 includes the following enhancement:

- **Enhancement (PR_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR_1000444415)** — OSPF Passive Interface support was added. For more information, see the ProCurve *Multicast and Routing Guide*.

Release K.12.23 Enhancements

Release K.12.23 includes the following enhancement:

- **Enhancement (PR_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP. For more information, see the ProCurve *Access Security Guide*.

Release K.12.24 Enhancements

No enhancements, software fixes only.

Release K.12.26 through K.12.29 Enhancements

No enhancements; Never built.

Release K.12.30 Enhancements

No enhancements; Never released.

Release K.12.31 Enhancements

Release K.12.31 includes the following enhancement:

- **Enhancement** — Support for the following ProCurve product was added.

  J9091A / J8715A (bundle) for the ProCurve switch 8212zl

Release K.12.32 Enhancements

Never released. Build K.12.32 includes the following enhancement:

- **Enhancement** — Merged all of the K.12.24 and earlier software fixes and enhancements with the ProCurve switch 8212zl support.

Release K.12.33 through K.12.40 Enhancements

No enhancements; Never built.

Release K.12.41 through K.12.42 Enhancements

No enhancements; Never released.

Release K.12.43 Enhancements

Release K.12.43 includes the following enhancement:

- **Enhancement** — Support for the following ProCurve products was added.

  J9051A ProCurve Wireless Edge Services zl Module

  J9052A ProCurve Redundant Wireless Edge Services zl Module

For more information, see "Support for the Wireless Edge Services zl Module" on page 18.

Release K.12.44 Enhancements

Release K.12.44 includes the following enhancement:

- **Enhancement (PR_1000457691)** — This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. (This enhancement was subsequently improved, see "Release K.12.51 Enhancements" on page 66.) For more information on MSTP VLANs, see the ProCurve *Advanced Traffic Management Guide*.
- **Enhancement (PR_1000457868)** — Local Proxy ARP enhancement. For more information, see the ProCurve *Multicast and Routing Guide*.
- **Enhancement (PR_1000456271)** — PC attached to telephone. (This enhancement was subsequently removed, see "Release K.12.47 Enhancements" on page 66.) For more information on endpoint device discovery, see the sections on LLDP-MED in the ProCurve *Management and Configuration Guide*. This enhancement was added back with Release K.12.51 (see "Release K.12.51 Enhancements" on page 66).

Release K.12.45 Enhancements

No enhancements; Never released.

Release K.12.46 Enhancements

No enhancements; Never released.

Release K.12.47 Enhancements

Release K.12.47 includes the following enhancement:

- **Enhancement Removed (PR_1000468258) —** The PC attached to IP telephone enhancement was removed.

Release K.12.48 Enhancements

Release K.12.48 includes the following enhancement:

- **Enhancement Removed (PR_1000470136) —** Removal of the enhancement that allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. The initial implementation of this enhancement did not allow smooth migration of pre-existing MSTP configurations. (For information on the initial implementation, see "Release K.12.44 Enhancements" on page 65. This enhancement was subsequently improved and re-introduced, see "Release K.12.51 Enhancements" on page 66.).

Release K.12.49 Enhancements

No enhancements; Bug fixes only.

Release K.12.50 Enhancements

No enhancements; Bug fixes only.

Release K.12.51 Enhancements

Release K.12.51 includes the following enhancements:

- **Enhancement (PR_10004570598) —** An improved version of the MSTP-VLAN mapping enhancement referenced in PR_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000471015) —** Reintroduction of the feature referenced in PR_1000456271, that will allow a PC to connect with its RADIUS-assigned VLAN after an attached IP phone has authenticated on the authenticating port. For information on the initial implementation, see "Release K.12.44 Enhancements" on page 65.

Release K.12.52 Enhancements

Release K.12.52 includes the following enhancement (*Never Released.*):

- **Enhancement (PR_1000458484) —** This enhancement allows the user to set a maximum frame size for jumbo frames at the global level. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000461576) —** This enhancement introduces PVST Protection and Filtering. For more information, see the ProCurve *Advanced Traffic Management Guide*.
- **Enhancement (PR_1000462841) —** This enhancement changes the re-authentication process to allow an authenticated client to remain authenticated during re-authentication. For more information, see the ProCurve *Access Security Guide*.
- **Enhancement (PR_1000462104) —** This enhancement allows the configuration of modules not currently inserted in the switch. For more information, see the ProCurve *Management and Configuration Guide*.
- **Enhancement (PR_1000462847) —** This enhancement allows the configuration of transceivers not currently inserted in the switch. For more information, see the ProCurve *Management and Configuration Guide*.

Release K.12.53 through K.12.55 Enhancements

No enhancements; Bug fixes only.

Release K.12.56 Enhancements

Release K.12.56 includes the following enhancement:

- **Enhancement (PR_1000464170) —** This feature provides support for adding the LLDP VLAN Name TLV to LLDP advertisements generated by ProCurve switches. For more information, see the ProCurve *Management and Configuration Guide*.

Release K.12.57 Enhancements

Release K.12.57 includes the following enhancement:

- **Enhancement (PR_1000713394) —** Adjustable IGMP Querier interval. For more information, see the ProCurve *Management and Configuration Guide*.

Release K.12.57 is the last public release of the K.12.*xx* software. The series 3500yl, 6200yl, 5400zl, and 8212zl switches software code was rolled to the K.13.0*x* code branch with no intervening releases.

Release K.13.01 Enhancements

Release K.13.01 is a major software update containing many new features and enhancements to existing features, including IPv6 host and application layer features (see "IPv6 Configuration Guide for 2900/3500/5400/6200/8200" on page 71 for details).

The following enhancements have been documented in the latest revisions to the manuals (January 2008). Refer to the indicated manuals for additional details.

Software Manual/ Enhancements	Description
Management and Configuration Guide	
PoE Power Allocation Methods:	Allows you to manually allocate the amount of PoE power for a port by either its class or a defined value.
USB Secure Autorun:	Helps ease the configuration of ProCurve switches by providing a way to auto-execute CLI commands from a USB flash drive. Note that the ability to create a valid AutoRun file also requires ProCurve Manager. For details, see the section on "USB Autorun" in the Appendix on "File Transfers".
SNMP Traps:	Allow you to configure the switch to send network security and link-change notifications to configured trap receivers. More error conditions can be reported and logged to help resolve security threats and network issues.
MAC-based Remote Mirroring:	Allows you to use MAC as a criteria in selecting traffic that needs to be monitored in addition to current port, ACL, and direction criteria.
Show Command Changes:	The **show power-management** CLI command has been changed to **show power-over-ethernet**. You can use this command and the **show power slot <slot-id>** to display information about PoE power. The **show system-information** CLI command syntax has been changed to **show system** with additional options to display details of system components: **fans**, **information**, **power-supply**, and **temperature**.
Scalability:	Increased max trunks (60); and increased helper address (4k). For scalability values for VLANs, hardware, ARP, and routing, see the new Appendix titled "Scalability: IP Address, VLAN, and Routing Maximum Values".
Advanced Traffic Management Guide	
STP Root Guard:	STP root guard allows user to prevent changes to the root bridge and thus preventing malicious attackers from modifying the root switch and ensuring that the STP topology maintain the optimal setting.
QinQ:	QinQ (provider bridging) has been added to allow frames from multiple customers to be forwarded through another topology (provider network) using service VLANs or S-VLANs. For more information, see the new "QinQ Provider Bridging" chapter.

Software Manual/ Enhancements	Description
STP Diagnostics:	Adds more diagnostic functions to resolve STP issues. See the section on "Troubleshooting an MSTP configuration" in the chapter on Multiple Instance Spanning-Tree Operation.
Routing and Multicast Guide	
Host-based OSPF-ECMP:	Allows OSPF to add routes with multiple next-hop addresses and with equal costs to a given destination IP address.
Access and Security Guide	
Dynamic Configuration Arbiter:	ProCurve provides different methods (for example, CLI, SNMP, or IDM/RADIUS) to configure network and security parameters and respond to threats. This feature allows you to determine the client-specific parameters that are assigned in an authentication session by applying or removing them as needed in a specified hierarchy of precedence.
RADIUS Attributes:	Additional RADIUS attributes included with this release: • Change of authorization: allows changes to user service without re-authentication • Vendor-ID: allows Microsoft RADIUS servers to use vendor ID as part of the policy • Capability advertisement: allows the switch to advertise its capability to the RADIUS server • Session termination: allows the switch to report to the RADIUS server the reason a session is terminated For more information, see the section on "Additional RADIUS Attributes" in the chapter on "RADIUS Authentication and Accounting".
RADIUS VLAN Support:	Supports RADIUS-assigned tagged and untagged VLAN configuration on an authenticated port. This allows you, for example, to use IDM to dynamically configure tagged and untagged VLANs as required for different client devices, such as PCs and IP phones, that share the same switch port. See the section on "VLAN Assignment in an Authentication Session" in the chapter on "RADIUS Authentication and Accounting".
PoE Planning and Implementation Guide	
Power Redundancy:	Support has been added for PoE redundancy. When PoE redundancy is enabled, PoE redundancy occurs automatically. The switch keeps track of power use and won't supply PoE power to additional PoE devices trying to connect if that results in the switch not having enough power in reserve for redundancy if one of the power supplies should fail.

Software Manual/ Enhancements	Description

Note on Manual Updates:
In addition to the above updates to the manuals, with this release the 8212zl software manuals and 3500/5400/6200 software manuals have been combined into a single manual set. Where features apply only to a specific model or models, this will be indicated in the chapter or heading for that feature; for example, "Redundancy (Switch 8212zl)" or "Stack Management for the Series 3500yl Switches and the 6200yl Switch."

New Product Documentation:
IPv6 Configuration Guide for 2900/3500/5400/6200/8200. Provides background information on IPv6 technologies and concepts, plus complete coverage of ProCurve's implementation of CLI commands for configuring IPv6 host and application layer features, including IPv6 addressing, auto configuration, dual stack support (IPv4/IPv6), Multicast Listener Discovery (MLD), IPv6 management and diagnostics.

The *Master Index* is a new feature to help find information more readily, providing clickable links from a combined Master Index PDF to the per Chapter PDF files from all five software manuals. To locate and access topics across the combined manual set using the index, download the Master Index zip file from the Web to a directory on your computer.

Release K.13.02 Enhancements

Release K.13.02 includes the following enhancements.

- **Enhancement**: Beginning with K.13.02, DHCP can now be enabled on a Management VLAN. Since, by definition, there is no routing to or from a VLAN configured as a management VLAN, DHCP relay is still prohibited so the DHCP server must be attached to the management VLAN for that VLAN to acquire an address. All DHCP options will be supported.
- **Enhancement (PR_1000458124) —** VRRP Preemptive Delay Timer. For more information, see "VRRP Pre-Emptive Delay Timer" on page 71 below.

VRRP Pre-Emptive Delay Timer

In order to maintain availability of the default gateway router, the Virtual Router Redundancy Protocol (VRRP) advertises a "virtual" router to the hosts. At least two other physical routers are configured to be virtual routers, but only one router provides the default router functionality at any given time. If the Owner router or its VLAN goes down, the Backup router takes over. When the Owner Router comes back on line (Fail-back), it takes control of the virtual IP address that has been assigned to it. It begins sending out VRRP advertisement packets at regular intervals. The Backup router receives the VRRP advertisement packet and transitions to the Backup state.

When OSPF is Also Enabled on the VRRP Routers

When OSPF is enabled on the routers and a Fail-back event occurs, the Owner router immediately takes control of the virtual IP address and provides the default gateway functionality. If OSPF has not converged, the route table in the Owner router may not be completely populated. When the hosts send packets to the default gateway, the Owner router may not know where to send them and packets may be dropped.

Caution

While you can run OSPF and VRRP concurrently on a router, it is best not to run VRRP with other routing protocols such as RIP or OSPF on the same interface or VLAN as this can create operational issues.

Configuring the Preempt Delay Timer

The VRRP Pre-empt Delay Timer (PDT) allows you to configure a period of time before the Owner router takes back control of the virtual IP address. It does not transition to the Master state until the timer period expires. The timer value configured should be long enough to allow OSPF convergence following OSPF updates.

The PDT is applied only during initialization of the router, that is, when the router is rebooting with the VRRP parameters present in the startup config file.

Syntax: [no] preempt-delay-time <1-600 >

Allows you to specify a time in seconds that the Owner router will wait before taking control of the virtual IP address and beginning to route packets. You can configure the timer on VRRP Owner and Backup routers.

Note*: If you have configured the Preempt Delay Timer with a non-zero value, you must use the* **no** *form of the command to change it to 0 (zero).*

Default*: 0 (zero) seconds.*

Note

If the PDT is active for a virtual router, you cannot change the router's mode from Owner to Backup or Backup to Owner. To change the mode, make the PDT inactive and then reconfigure the mode. For example:

```
ProCurve(config)# no vlan 16 vrrp vrid 23 preempt-delay time 12
```

where

VID = 16
VRID = 23
PDT = 12 seconds

VRRP Preempt Mode with LACP and Older ProCurve Devices

There can be an issue with VRRP Preempt Mode if an older ProCurve device (2524, 2650, 2848, 3400cl, or 5300) is the intermediate device connecting to a VRRP router and has LACP set in "enable, passive" mode. This mode is set by default on older ProCurve devices, whereas it is disabled by default on later models such as the ProCurve Series 5400zl. ProCurve recommends that you use compatible LACP settings on devices that connect with VRRP routers on VRRP VLANs.

What Occurs at Startup

When the Owner router comes online, it will wait for the configured amount of time before taking control of the virtual IP address. This period of time is calculated as follows:

If the value of the Master down time (3 * advertisement interval) is less than or equal to the preempt delay time, then the Owner router will wait until the Master down time (3 * advertisement interval) has expired.

During this waiting period, if the Owner router receives a VRRP packet for its virtual IP address from the Backup router, it will wait until the PDT expires before taking control of its virtual IP address. If the Owner router does not receive any VRRP packets and the Master down time expires, the Owner router can take control of its virtual IP address immediately.

If the value of the Master down time (3 * advertisement interval) is greater than the preempt delay time, then the Owner Router will wait until the PDT expires before taking control of its virtual IP address.

Selecting a Value for the PDT

You should select the value for the PDT carefully to allow time for OSPF to populate the Owner router's route tables. The choice depends on the following:

- The OFPF router dead interval—the number of seconds the OSPF router waits to receive a hello packet before assuming its neighbor is down.
- The number of router interfaces that participate in OSPF
- The time it may take from reception of the OSPF packets to when the population of the route table is completed.

There are trade-offs between selecting a small advertisement value and a large preempt delay time. A small advertisement value results in a faster failover to the Backup router. A larger PDT value allows OSPF to converge before the Owner router takes back control of its virtual IP address.

Choosing a large PDT value (greater than the Master down time) may result in an unnecessary failover to the Backup router when the VRRP routers (Owner and Backup) start up together. Choosing a large advertisement interval and thereby a large Master down time results in a slower failover to the Backup router when the Owner router fails.

Possible Configuration Scenarios

Preempt Delay Time = Zero Seconds. This is the default behavior. It works in the same way that VRRP works currently.

Preempt Delay Time is Greater Than or Equal to the Master Down Time (3 times the advertisement interval).

a. An Owner Virtual Router after reboot—waits for the Master Down Time. If the Owner router does not receive a packet during this time, it becomes the Master. If it receives a VRRP advertisement from its peer during this time, it waits until the expiration of the preempt delay time before becoming the Master.

b. A Backup Virtual Router after reboot—waits for the Master Down Time. If the Backup router does not receive a packet during this time, it becomes the Master. If it receives a VRRP advertisement from its peer during this time, it waits until the expiration of the preempt delay time before becoming the Backup.

Preempt Delay Time is Less Than the Master Down Time.

a. Owner router—becomes the Master after expiration of the preempt delay time.

b. Backup router—becomes the Backup after expiration of the preempt delay time.

When the Preempt Delay Time is not Applicable

Once the router has rebooted and is in steady state VRRP operation, the PDT is not applicable if:

- The VRRP VLAN goes down and comes back up
- The Virtual Router is disabled and re-enabled
- VRRP is globally disabled and then re-enabled

Backward Compatibility

If a VRRP router functions with an older version that does not have the pre-empt delay timer enhancement, it will take over virtual IP address control immediately on start-up or when there is a fail-back event. There should be no backward compatibility issues.

Error Messages

Error	Error Message
Attempting to assign the preempt delay time to the Virtual Router before declaring it as an Owner or Backup	The Virtual Router must be defined as an Owner or Backup router first.
Attempting to assign an out of range preempt delay time to the Virtual Router instance.	Invalid input: <out of range value>
Attempting to change the preempt delay time value when the Virtual Router is active.	VR operation must be "down" prior to modifying VR's parameters

Release K.13.03 Enhancements

Release K.13.03 includes the following enhancements.

- **Enhancement (PR_1000400991) —** The 802.1X Controlled Directions feature now functions independently of the STP configuration, allowing you to run STP and 802.1X separately. For more information, see "New CLI Commands" below.

New CLI Commands

These three commands show the administrative state of the controlled-directions:

show port-access authenticator config
show port-access mac-based config
show port-access web-based config

These three commands show the operational state of the controlled-directions:

show port-access authenticator
show port-access mac-based
show port-access web-based

Release K.13.04 Enhancements

Release K.13.04 includes the following enhancements.

- **Enhancement (PR_ 0000000081) —** The CLI **clear module** command allows you to remove module configuration information from the configuration file.

Clear Module Configuration

Overview

Because of the hot-swap capabilities of the modules, when a module is removed from the chassis of a ProCurve series 5400 switch, the module configuration remains in the configuration file. This enhancement allows you to remove the module configuration information from the configuration file.

Syntax: [no] module <slot>

Allows removal of the module configuration in the configuration file after the module has been removed. Enter an integer between 1 and 12 for <slot>.

For example:

```
ProCurve(config)# no module 3
```

Note

This does not change how hot-swap works.

Operating Notes

The following restrictions apply:

- The slot being cleared must be empty
- There was no module present in the slot since the last boot
- If there was a module present after the switch was booted, the switch will have to be rebooted before any module (new or same) can be used in the slot.
- This does not clear the configuration of a module still in use by the switch.

- **Enhancement (PR_ 0000000082) —** The CLI **track interface** command allows you to configure tracking for a port or list of ports, or a trunk or list of trunks.

VRRP—Dynamic Priority Change

Overview

This enhancement provides the ability to dynamically change the priority of the virtual router (VR) when certain events occur. The Backup VR releases virtual IP address control by reducing its priority when tracked entities such as ports, trunks, or VLANs go down. You can also force the Backup to take ownership of the VR if you have previously caused it to release control.

In normal VRRP operation, one router (Router-1) is in the Master state and one router (Router-2) is in the Backup state. Router-1 provides the default gateway for the host. If Router-1 goes down for any reason, the Backup router, Router-2, provides the default gateway for the host.

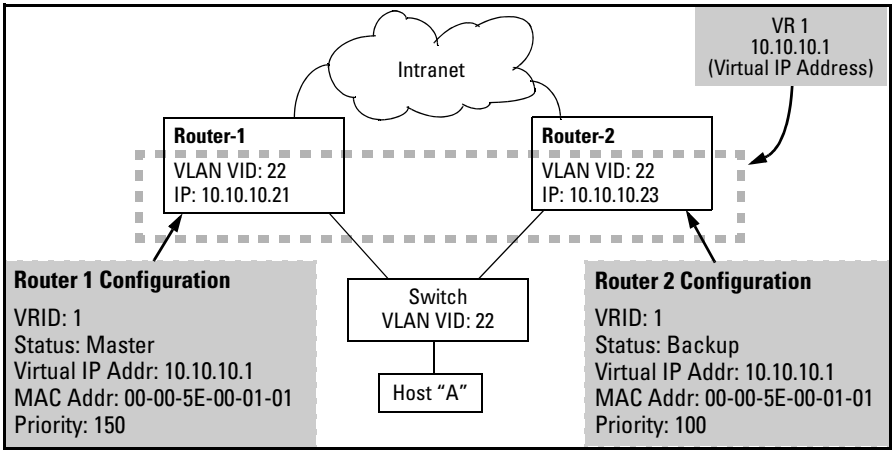

Figure 10. Example VRRP Configuration

If all the tracked entities configured on Router-1 go down, Router-1 begins sending advertisements with a priority of zero. This causes Router-2 to take control of the virtual IP.

Any applications or routing protocols such as RIP or OSPF on Router-1 that were using its IP address are no longer able to use that IP interface. Router-1 does not respond to any ARP requests for that IP address. Router-2 takes control of the IP address and responds to ARP requests for it with the virtual MAC address that corresponds to VRID-1.

Note

A Backup VR switches to priority zero instead of its configured value when all its tracked entities go down. An Owner VR always uses priority 255 and never relinquishes control voluntarily.

CLI Commands

The following commands are used for this enhancement.

Note

You can only configure tracked interfaces or VLANs on the Backup router.

Configuring Track Interface

The **track interface** command allows you to configure tracking for a port or list of ports, or a trunk or list of trunks.

Note

VR operation must be down before executing this command. Use the **no enable** command to disable VR operation.

Syntax: [no] track interface <port-list/trunk-list>

Allows you to specify a port or port list, or trunk or trunk list, that will be tracked by this virtual router. If the port or trunk is down, the virtual router switches to the router specified by the priority value. The command is executed in VRID instance context.

For example:

```
ProCurve(config)# vlan 25
ProCurve(vlan-25)# vrid 1
ProCurve(vlan-25-vrid-1)# track interface 10-12, Trk1
```

Configuring Track VLAN

The **track vlan** command allows you to specify a VLAN or range of VLANs to be tracked by the VR.

Notes

VR operation must be down before executing this command. Use the **no enable** command to disable VR operation.

The VRs operating VLAN can't be configured as a tracking VLAN for that VR.

Syntax: [no] track vlan <vlan-id range>

Allows you to specify a VLAN or range of VLANs that will be tracked by this virtual router. If the VLAN is down, or the VLAN or IP address has been deleted, the virtual router switches to the router specified by the dynamic priority value. The command is executed in VRID instance context.

For example:

```
ProCurve(config)# vlan 25
ProCurve(vlan-25)# vrid 1
ProCurve(vlan-25-vrid-1)# track vlan 10 24-26
```

Note

When the first tracked port or tracked VLAN comes up after being down, the VR waits for the preempt delay time before it tries to take control back. The VR resumes being a Backup with its configured priority as soon as the first tracked entity is up.

The behavior of the VR is not affected by any tracked entities until after the expiration of the preempt delay time. However, if while waiting for the preempt delay time to expire, a Master goes down, the VR tries to take control of the virtual IP.

Removing all Tracked Entities

Use the **no track** command to remove all interfaces and vlans from being tracked.

Syntax: no track

The command allows you to remove tracking for all configured track entities (ports, trunks, and VLANs). The command is executed in VRID instance context.

For example:

```
ProCurve(vlan-25-vrid-1)# no track
```

Failover Operation

Failover operation involves handing off of the VRs control of the virtual IP to another VR. Once a failover command is issued, the VR begins sending advertisements with priority zero instead of the configured priority. When the VR detects a peer VR taking control, it releases control of the virtual IP and ceases VR operation until a failback is executed. Failover only occurs on a Backup VR operating as Master.

If you specify the **with-monitoring** option, the VR continues to monitor the virtual IP after ceasing VR operation. If the Master VR goes down, it then re-takes control of the virtual IP.

Syntax: failover [with-monitoring]

Allows you to force the Backup VR operating as Master to relinquish ownership of the VR instance. The command is executed in VRID instance context.

Failback Operation

The **failback** command forces the Backup VR to take ownership of the VR instance. Failback is disabled on the Owner VR; it can only be executed on the Backup VR. Failback can only occur on a VR on which **failover** or **failover with-monitoring** has been executed.

Syntax: failback

Forces the Backup VR to take ownership of the VR instance. This command only takes effect if the Backup VR instance has a higher priority than the current Owner, which is normal VRRP router behavior. The command is executed in VRID instance context.

Displaying the VRRP Configuration

You can display the VRRP tracked entities by entering the command shown in Figure 11.

```
ProCurve(vlan-25-vrid-1)# show vrrp tracked-entities

 VRRP Tracked entities

  VLAN ID    VR ID      Type       ID
  ---------- ---------- ---------- ------------------------------
  25         1          port       7
  25         1          port       12
  25         1          port       13
  25         1          port       14
  25         1          vlan       1
```

Figure 11. Example of show vrrp tracked entities Command

You can display the VRRP configuration by entering the command shown in Figure 12.

```
ProCurve(vlan-25-vrid-1)# show vrrp vlan 25 vrid 1 config

 VRRP Virtual Router Configuration Information

  Vlan ID : 25
  Virtual Router ID : 1

  Administrative Status [Disabled] : Enabled
  Mode [Uninitialized] : Owner
  Priority [100] : 255
  Advertisement Interval [1] : 1
  Preempt Mode [True] : True
  Preempt Delay Time [0] : 0
  Primary IP Address : Lowest

  IP Address      Subnet Mask
  --------------- ---------------
  10.10.10.1      255.255.255.0
```

Figure 12. Example Showing the VRRP Configuration

Operating Notes

- There are no backward compatibility issues with this enhancement. If a VRRP router has an older firmware version that does not have the dynamic priority changeover feature, it will not have the needed configuration options.

- The VRs operating VLAN can't be configured as a tracking VLAN for that VR.
- Ports that are part of a trunk can't be tracked.
- A port that is tracked can't be included in a trunk.
- Trunks that are tracked can't be removed; you are not able to remove the last port from the trunk.
- LACP (active or passive) cannot be enabled on a port that is being tracked.
- If a VLAN is removed or a port becomes unavailable, the configuration is retained and they are tracked when they become available again.
- After the Owner VR relinquishes control of its IP address, that IP address becomes unavailable to all other applications and routing protocols such as RIP and OSPF.
- To avoid operational issues, it is recommended that VRRP is not run on the same interface/VLAN with other routing protocols, such as RIP and OSPF.

Error Messages

Track Interface

Message	Description
VR must be defined as "backup" first	You have to declare a VR as Backup before assigning a track interface to it.
Invalid input: <out of range value>	You have to assign a valid port or trunk to the VR instance.
VR operation must be "down" prior to modifying VR's parameters	You cannot change the track interface when the VR is active. Use the **no enable** command to disable the VR.
Can't track a port that is part of a trunk	You can't configure tracking on a port that is a member of a trunk.
Tracking is disabled on owner	You can't configure a track interface on an Owner VR.
Cannot remove trunk being tracked by VRRP	You can't remove a trunk that is being tracked by a VR
Cannot enable LACP on a VRRP tracked port	You can't enable LACP on a port that is being tracked by a VR.
Too many entities to track	You have selected too many entities to be tracked by the VR.
Cannot track trunk/LACP member	You can't track the specified trunk or LACP member.
VRRP tracked port is not allowed in trunk	You can't add this tracked port to a trunk.
VRRP tracked port is not allowed in LACP	You can't use LACP with the tracked port.
Operation is not permitted on VR when it is configured as owner or is uninitialized.	The VR must be a Backup and initialized in order to execute the operation.

- **Enhancement (PR_ 0000000084) —** DHCP Option 66 provides a way to automatically download and initially boot from a configuration that is different from the factory-shipped configuration.

DHCP Option 66 Automatic Configuration Update

Overview

ProCurve switches are initially booted up with the factory-shipped configuration file. This enhancement provides a way to automatically download a different configuration file from a TFTP server using DHCP Option 66. The prerequisites for this to function correctly are:

- One or more DHCP servers with Option 66 are enabled
- One or more TFTP servers has the desired configuration file.

Caution

This feature must use configuration files generated on the switch to function correctly. If you use configuration files that were not generated on the switch, and then enable this feature, the switch may reboot continuously.

CLI Command

The command to enable the configuration update using Option 66 is:

Syntax: [no] dhcp config-file-update

Enables configuration file update using Option 66.

Default: Enabled

```
ProCurve(config)# dhcp config-file-update
```

Figure 13. Example of Enabling Configuration File Update Using Option 66

Possible Scenarios for Updating the Configuration File

The following table shows various network configurations and how Option 66 is handled.

Scenario	Behavior
Single Server serving Multiple VLANs	• Each DHCP-enabled VLAN interface initiates DHCPDISCOVER message, receives DHCPOFFER from the server, and send DHCPREQUEST to obtain the offered parameters. • If multiple interfaces send DHCPREQUESTs, it's possible that more than one DHCPACK is returned with a valid Option 66. • Evaluating and updating the configuration file occurs only on the primary VLAN. • Option 66 is ignored by any interfaces not belonging to the primary VLAN.
Multiple Servers serving a Single VLAN	• Each DHCP-enabled VLAN interface initiates one DHCPDISCOVER and receives one or more DHCPOFFER messages. • Each interface accepts the best offer. • Option 66 is processed only for the interface belonging to the primary VLAN.
Multiple Servers serving Multiple VLANs	• Each DHCP-enabled VLAN interface initiates DHCPDISCOVER and receives one or more DHCPOFFER messages. • Each interface accepts the best offer. • Option 66 is processed only for the interface belonging to the primary VLAN.
Multi-homed Server serving Multiple VLANs	• The switch perceives the multi-homed server as multiple separate servers. • Each DHCP-enabled VLAN interface initiates DHCPDISCOVER and receives one DHCPOFFER message. • Each interface accepts the offer. • Option 66 is processed only for the interface belonging to the primary VLAN.

Operating Notes

Replacing the Existing Configuration File: After the DHCP client downloads the configuration file, the switch compares the contents of that file with the existing configuration file. If the content is different, the new configuration file replaces the existing file and the switch reboots.

Option 67 and the Configuration File Name: Option 67 includes the name of the configuration file. If the DHCPACK contains this option, it overrides the default name for the configuration file (switch.cfg)

Global DHCP Parameters: Global parameters are processed only if received on the primary VLAN.

Best Offer: The "Best Offer" is the best DHCP or BootP offer sent by the DHCP server in response to the DHCPREQUEST sent by the switch. The criteria for selecting the "Best Offer" are:

- DHCP is preferred over BootP
- If two BootP offers are received, the first one is selected
- For two DHCP offers:
  - The offer from an authoritative server is selected
  - If there is no authoritative server, the offer with the longest lease is selected

Log Messages

The file transfer is implemented by the existing TFTP module. The system logs the following message if an incorrect IP address is received for Option 66:

```
Invalid IP address <ip-address> received for DHCP Option 66
```

- **Enhancement (PR_0000000085) —** The DHCP relay address configuration enhancement provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address.

BOOTP/DHCP Relay Gateway

Overview

Previously, the DHCP relay agent selected the lowest-numbered IP address on the interface to use for DHCP messages. The DHCP server then used this IP address when it assigned client addresses. However, this IP address may not be the same subnet as the one on which the client needs the DHCP Service.

This enhancement provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address.

You must be in VLAN context to use this command, for example:

```
ProCurve# config

ProCurve(config)# vlan 1

ProCurve(vlan-1)#
```

Syntax: ip bootp-gateway <ip-addr>

Allows you to configure an IP address for the DHCP relay agent to use for DHCP requests. The IP address must have been configured on the interface.

Default: Lowest-numbered IP address

If the IP address has not already been configured on the interface (VLAN), you will see the message shown in Figure 14.

```
ProCurve# config
ProCurve(config)# vlan 1
ProCurve(vlan-1)# ip bootp-gateway 10.10.10.1
The IP address 10.10.10.1 is not configured on this VLAN.
```

Figure 14. Example of Trying to Configure an IP Address that is not on this Interface (VLAN)

Displaying the BOOTP Gateway

To display the configured BOOTP gateway for an interface (VLAN) or all interfaces, enter this command. You do not need to be in VLAN context mode.

Syntax: show dhcp-relay bootp-gateway [vlan <vid>]

Displays the configured BOOTP gateway for a specified VLAN (interface). If a specific VLAN ID is not entered, all VLANs and their configured BOOTP gateways display.

Figure 15 shows an IP address being assigned to a gateway for VLAN 22, and then displayed using the **show dhcp-relay bootp-gateway** command.

```
ProCurve(vlan-22)ip bootp-gateway 12.16.18.33
ProCurve(vlan-22)# exit
ProCurve(config)# show dhcp-relay bootp-gateway vlan 22

 BOOTP Gateway Entries

 VLAN                 BOOTP Gateway
 -------------------- --------------
 VLAN 22              12.16.18.33
```

Figure 15. An Example of Assigning a Gateway to an Interface and then Displaying the Information

Operating Notes

- If the configured BOOTP gateway address becomes invalid, DHCP relay agent returns to the default behavior (assigning the lowest-numbered IP address).
- If you try to configure an IP address that is not assigned to that interface, the configuration will fail and the previously configured address (if there is one) or the default address is used.

■ **Enhancement (PR_ 0000000086) —** This enhancement allows rate-limiting of inbound broadcast and multicast traffic on the switch.

Inbound Rate-Limiting for Broadcast and Multicast Traffic

This enhancement allows rate-limiting (throttling) of inbound broadcast and multicast traffic on the switch. The rate-limiting is implemented as a percentage of the total available bandwidth on the port. Rate-limiting inbound broadcast or multicast traffic helps prevent the switch from being disrupted by traffic storms if they occur on the rate-limited port.

You can execute the **rate-limit** command from the global or interface context, for example:

```
ProCurve(config)# interface 3 rate-limit bcast in percent 10
```

or

```
ProCurve(config)# interface 3
ProCurve(eth-3)# rate-limit bcast in percent 10
```

Syntax: rate-limit < bcast | mcast > in percent <0-100>
no rate-limit <bcast | mcast> in

Enables rate-limiting and sets limits for the specified inbound broadcast or multicast traffic. Only the amount of traffic specified by the percent is forwarded.

Default: Disabled

For example, if you want to set a limit of 50 percent on inbound broadcast traffic for port 3, you can first enter interface context for port 3 and then execute the **rate-limit** command, as shown in Figure 1. Only 50 percent of the inbound broadcast traffic will be forwarded.

```
ProCurve(config)# int 3
ProCurve(eth-3)# rate-limit bcast in percent 50

ProCurve 3500(eth-3)# show rate-limit bcast
 Broadcast-Traffic Rate Limit Maximum %

  Port  | Inbound Limit Mode      Radius Override
  ----- + ------------- --------- ---------------
  1     | Disabled      Disabled  No-override
  2     | Disabled      Disabled  No-override
  3     | 50            %         No-override
  4     | Disabled      Disabled  No-override
  5     | Disabled      Disabled  No-override
```

Figure 1. Example of Inbound Broadcast Rate-limiting of 50% on Port 3

If you rate-limit multicast traffic on the same port, the multicast limit is also in effect for that port, as shown in Figure 2. Only 20 percent of the multicast traffic will be forwarded.

```
ProCurve(eth-3)# rate-limit mcast in percent 20
ProCurve(eth-3)# show rate-limit mcast

 Multicast-Traffic Rate Limit Maximum %

  Port  | Inbound Limit Mode      Radius Override
  ----- + ------------- --------- ---------------
  1     | Disabled      Disabled  No-override
  2     | Disabled      Disabled  No-override
  3     | 20            %         No-override
  4     | Disabled      Disabled  No-override
```

Figure 2. Example of Inbound Multicast Rate-limiting of 20% on Port 3

To disable rate-limiting for a port enter the **no** form of the command.

```
ProCurve(eth-3)# no rate-limit mcast in

ProCurve(eth-3)# show rate-limit mcast

 Multicast-Traffic Rate Limit Maximum %

  Port  | Inbound Limit Mode      Radius Override
  ----- + ------------- --------- ---------------
  1     | Disabled      Disabled  No-override
  2     | Disabled      Disabled  No-override
  3     | Disabled      Disabled  No-override
  4     | Disabled      Disabled  No-override
```

Figure 3. Example of Disabling Inbound Multicast Rate-limiting for Port 3

Operating Notes

- This rate-limiting feature does not limit unicast traffic.
- This feature does not include outbound multicast rate-limiting.

For more detailed information about rate-limiting, see the *Multicast and Routing Guide* for your switch.

■ **Enhancement (PR_ 0000000087) —** This enhancement enables a Telnet client to use the histamine in command input.

DNS Capabilities for Telnet

Overview

This enhancement enables a Telnet client to use the hostname in command input.

Syntax: telnet <ipv4-addr | ipv6-addr | hostname | switch-num>

Initiates an outbound telnet session to another network device. The destination can be specified as:

- *IPv4 address*
- *IPv6 address*
- *Hostname*
- *Stack number of a member switch (1-16) if the switch is a commander in a stack and stacking is enabled*

For example, if the host “Labswitch” is in the domain abc.com, you can enter the following command and the destination is resolved to “Labswitch.abc.com”.

```
ProCurve(config)# telnet Labswitch
```

You can also enter the full domain name in the command:

```
ProCurve(config)# telnet Labswitch.abc.com
```

You can use the **show telnet** command to display the resolved IP address.

```
ProCurve(config)# show telnet

 Telnet Activity

 ------------------------------------------------------
 Session  : **  1
 Privilege: Manager
 From     : Console
 To       :

-------------------------------------------------------
 Session  : **  2
 Privilege: Manager
 From     : 12.13.14.10
 To       : 15.33.66.20

-------------------------------------------------------
 Session  : **  3
 Privilege: Operator
 From     : 2001:db7:5:0:203:4ff:fe0a:251
 To       : 2001:db7:5:0:203:4ff1:fddd:12
```

Figure 16. Example of show telnet Command Displaying Resolved IP Addresses

- **Enhancement (PR_ 0000000089) —** The CLI **show modules** command displays additional component information for system support modules and mini-GBICS.

Show Module Enhancement

Overview

With this enhancement, the CLI **show modules** command will display additional component information for the following:

- System Support Modules (SSM) — identification, including serial number
- Mini-GBICS — a list of installed mini-GBICs displaying the type, “J” number, and serial number (when available)

Syntax: show modules [details]

Displays information about the installed modules, including:

- *The slot in which the module is installed*
- *The module description*
- *The serial number*
- *The System Support Module description, serial number, and status (8212zl only)*

Additionally, the part number (J number) and serial number of the chassis is displayed.

```
ProCurve(config)# show modules

 Status and Counters - Module Information

  Chassis: 5406zl J8697A         Serial Number:   SG560TN124
  Slot  Module Description                       Serial Number
  ----- ---------------------------------------- --------------
  A     ProCurve J8706A 24p SFP zl Module        AD722BX88F
  B     ProCurve J8702A 24p Gig-T zl Module      FE999CV77F
  C     ProCurve J8707A 4p 10-Gbe zl Module      FB345DC99D
```

Figure 17. Example of the show modules Command Output

```
ProCurve(config)# show modules details

 Status and Counters - Module Information

  Chassis: 8212zl J8715A        Serial Number:   SG560TN124
  Slot  Module Description                         Serial Number   Status
  ----- ---------------------------------------   --------------  -------
  MM1   ProCurve J9092A Management Module 8200zl   AD722BX88F      Active
  SSM   ProCurve J8784A System Support Module      AF988DC78G      Active
  C     ProCurve J8750A 20p +4 Mini-GBIC Module    446S2BX007      Active
         GBIC 1: J4859B  1GB LX-LC                 4720347DFED734
         GBIC 2: J4859B  1GB LX-LC                 4720347DFED735
```

Figure 18. An Example of the show modules details Command for the 8212zl Showing SSM and Mini-GBIC Information

Note

On ProCurve 3500yl and 6200yl series switches, the mini-GBIC information does not display as the ports are fixed and not part of any module.

- **Enhancement (PR_ 0000000101) —** This enhancement adds a **vrrp** option to the **debug** command.

VRRP Option with Debug Command

This enhancement adds a **vrrp** option to the **debug** command. This option turns on the tracing of the incoming and outgoing VRRP packets. The information in the following table is included in the output.

Syntax: [no] debug vrrp

Displays VRRP debug messages.

Displaying the "Near-Failover" Statistic

There is a new VRRP statistic that will track occurrences of "near failovers" on the Backup VRRP routers. This makes visible any difficulties the VRRP routers are having receiving the "heartbeat" advertisement from the Master router. (A "near failover" is one that is within one missed VRRP advertisement packet of beginning the Master determination process.)

The **show vrrp** command displays this statistic.

```
ProCurve(config)# show vrrp

 VRRP Global Statistics Information

  VRRP Enabled           : Yes
  Protocol Version       : 2
  Invalid VRID Pkts Rx   : 0
  Checksum Error Pkts Rx : 0
  Bad Version Pkts Rx    : 0


 VRRP Virtual Router Statistics Information

  Vlan ID                  : 22
  Virtual Router ID        : 1
  State                    : Initialize
  Up Time                  : 64 mins
  Virtual MAC Address      : 00005e-000101
  Master's IP Address      :
  Associated IP Addr Count : 1          Near Failovers            : 0
  Advertise Pkts Rx        : 0          Become Master             : 0
  Zero Priority Rx         : 0          Zero Priority Tx          : 0
  Bad Length Pkts          : 0          Bad Type Pkts             : 0
  Mismatched Interval Pkts : 0          Mismatched Addr List Pkts : 0
  Mismatched IP TTL Pkts   : 0          Mismatched Auth Type Pkts : 0
```

Figure 19. Example of the show vrrp Command with Statistics

- **Enhancement (PR_0000000420) —** This enhancement provides the **show-tech** option for customizing **copy tftp** output.

Copy Command with Show Tech Option

This enhancement allows the **show-tech** command to execute a series of commands found in a special file stored in flash. If no file is found, the current hard-coded list is used. This feature provides the ability to customize the output.

To upload the customized list, the **copy tftp** command will include the **show-tech** option in the **destination** parameter.

Syntax: copy <source> <destination> [options]

Copy data files to or from the switch.

<source>: *specify the source of the data. It can be tftp, xmodem, command, usb, or any of the following switch data files:*

- running-config
- startup-config
- crash-log [a|b|c|d|e|f|g|h|master]
- crash-data
- event-log
- flash
- command-output <command>

Note: *When using* **command output**, *place the desired CLI command in double quotes, for example, "show system".*

<destination>: *specify the copy target. It can be tftp, xmodem, usb, or one of the following switch data files:*

- startup-config
- command-file
- flash
- pub-key-file
- show-tech

For example:

```
ProCurve(config)# copy tftp show-tech 10.10.10.3 commandfile1
```

Figure 4. Example of Using the show-tech Command to Upload a Customized List

Release K.13.05 through K.13.15 Enhancements

No enhancements; Bug fixes only.

Release K.13.16 Enhancements

Release K.13.16 includes the following enhancements:

- **Enhancement (PR_0000001641)** — This enhancement allows the user to set the console inactivity time out without rebooting the switch.

Console/Telnet Inactivity Timer

This enhancement allows you to configure the inactivity timer and have the new value take effect immediately, without a reboot of the system.

Syntax: console inactivity-timer <minutes>

If the console port has no activity for the number of minutes configured, the switch terminates the session. A value of zero indicates the inactivity timer is disabled.

Default: 0 (zero)

For example:

```
ProCurve(config)# console inactivity-timer 20
```

- **Enhancement (PR_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files.
- **Enhancement (PR_0000001430)** — This enhancement allows the user to configure access methods for IP Authorized Manager entries.

Management Access Security Enhancement

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

- SSH
- Telnet
- Web
- TFTP
- SNMP

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

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

Setting the Management Access Method—CLI

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

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

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

Configures one or more authorized IP addresses.

access [manager | operator]

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

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

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

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

Figure 5. Example of Configuring IP Authorized Manager Access Method SSH

```
ProCurve(config)# show ip authorized-manager

IPV4 Authorized Managers
------------------------

 Address : 10.10.10.10
 Mask    : 255.255.255.255
 Access  : Manager
 Access Method : ssh
```

Figure 6. Example of show authorized-managers Command with Access Method Configured

Setting the Management Access Method—Menu

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

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

```
ProCurve                                                    22-Apr-2008  20:17:53
==========================- CONSOLE - MANAGER MODE -============================
                        Switch Configuration - IP Managers

  Authorized Manager IP          IP Mask          Access Level  Access Method
  ----------------------  ---------------------  ------------  -------------
  10.10.240.2             255.255.255.255         Manager       all
  10.10.245.3             255.255.255.255         Operator      ssh
  10.10.246.200           255.255.255.255         Operator      tftp
  10.10.245.30            255.255.255.0           Operator      ssh









 Actions->   Back     Add     Edit     Delete     Help
```

Figure 7. Example of Menu Showing Authorized Managers with Access Method

```
ProCurve                                                    22-Apr-2008  20:17:53
==========================- CONSOLE - MANAGER MODE -============================
                        Switch Configuration - IP Managers

  Authorized Manager IP: 10.10.245.3
  IP Mask [255.255.255.255]:255.255.255.255
  Access Level:Operator
  Access Method:ssh









 Actions->   Back     Add     Edit     Delete     Help
```

Figure 8. Example of Edit Menu for IP Managers

Setting the Management Access Method—Web Interface

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

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

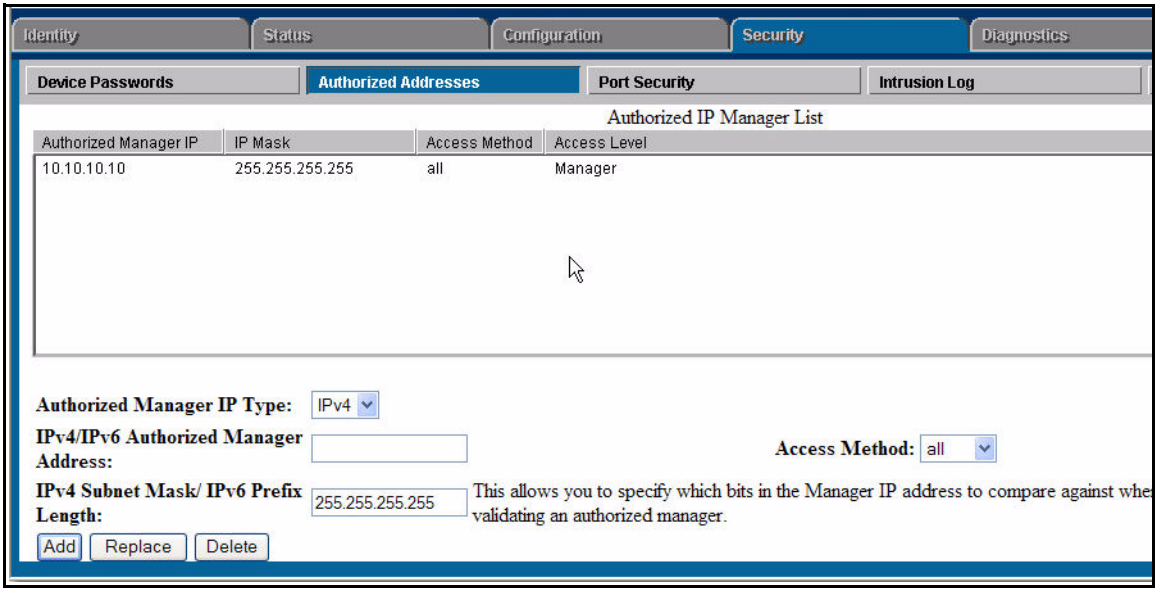

Figure 9. Example of Configuring Authorized Manager Access Method in the Web Interface

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

- **Enhancement (PR_0000000090)** — This enhancement allows you to choose which information to display when you enter the **show interfaces** command.

Show Interfaces Custom

This command enhancement allows you to choose which information to display when you enter the **show interfaces** command. You can create **show** commands displaying the information that you want to see in any order you want.

Syntax: show interfaces custom [port-list] column-list

Select the information that you want to display. Parameters include:

- *port name*
- *type*
- *vlan*
- *intrusion*
- *enabled*
- *status*
- *speed*
- *mdi*
- *flow*

Columns supported are:

Parameter Column	Displays	Examples
port	Port identifier	A2
type	Port type	100/1000T
status	Port status	up or down
speed	Connection speed and duplex	1000FDX
mode	Configured mode	auto, auto-100, 100FDX
mdi	MDI mode	auto, MDIX
flow	Flow control	on or off
name	Friendly port name	
vlanid	The vlan id this port belongs to, or "tagged" if it belongs to more than one vlan	4 tagged
enabled	port is or is not enabled	yes or no
intrusion	Intrusion alert status	no intrusion
bcast	Broadcast limit	0

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

 Status and Counters - Custom Port Status

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

Figure 20. Example of the Custom show interfaces Command

You can specify the column width by entering a colon after the column name, then indicating the number of characters to display. In Figure 20 the Name column only displays the first four characters of the name. All remaining characters are truncated.

Note

Each field has an fixed minimum width to be displayed. If you specify a field width smaller than the minimum width, the information is displayed at the minimum width. For example, if the minimum width for the Name field is 4 characters and you specify Name:2, the Name field displays 4 characters.

Parameters can be entered in any order. There is a limit of 80 characters per line; if you exceed this limit an error displays.

Error Messages

Error	Error Message
Requesting too many fields (total characters exceeds 80)	Total length of selected data exceeds one line
Field name is misspelled	Invalid input: <input>
Mistake in specifying the port list	Module not present for port or invalid port: <input>
The port list is not specified	Incomplete input: custom

Note on Using Pattern Matching with the "Show Interfaces Custom" Command

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

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

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

- **Enhancement (PR_0000000857)** — This enhancement reduces the PIM delay time, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. A delay occurs in PIM when processing IGMP Join messages. This enhancement reduces the delay, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. There are no CLI changes with this enhancement.
- **Enhancement (PR_0000001790)** — This enhancement provides the **no-tag-added** parameter that gives the user the option of not tagging a mirrored copy of an outbound packet.

Mirror Port VLAN Tagging

ProCurve switches can mirror inbound and outbound traffic to local ports on the switch, or to ports on remote switches. Currently, a VLAN tag is added to the mirrored copy of untagged outbound packets to indicate the source VLAN of the packet. However, it is desirable in some situations to have mirrored packets look exactly like the original packet.

This enhancement provides the **no-tag-added** parameter that gives you the option of not tagging a mirrored copy of an outbound packet.

Note

A mirror destination for the session must be assigned before a port monitoring source is assigned.

Syntax: [no] interface <port-num | trunk-name | mesh> monitor all <in | out | both> mirror <session-num> [no-tag-added]

Assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the port, trunk, and/or mesh source to use, the direction of traffic to mirror, and the session identifier.

Note: *If configuring a mesh, designate it using the literal string "mesh".*

[no-tag-added] *Prevents tagging of a mirrored copy of an outbound packet*

You can also use the **no-tag-added** parameter with ACL traffic filtering when mirroring IP traffic.

Syntax: [no] interface <port-num | trunk-name | mesh> monitor ip access-group <acl-name> in mirror <session-num> [no-tag-added]

Assigns a mirroring source to a previously configured mirroring session on a source switch. It specifies the ports, trunk name, or mesh to use, the previously configured ACL to use for selecting traffic to mirror, and the session identifier.

Note: *If configuring a mesh, designate it using the literal string "mesh".*

[no-tag-added] *Prevents tagging of a mirrored copy of an outbound packet*

```
ProCurve(config)#interface 3 monitor all in mirror 1 no-tag-added

ProCurve(config)#interface 2 monitor ip access-group A in mirror 2 no-tag-added

ProCurve(config)#interface mesh monitor all both mirror 1 no-tag-added
```

Figure 21. Mirroring Commands with the no-tag-added Option

```
ProCurve# show monitor

Network Monitoring

   Sessions  Status       Type    Sources  ACL
   --------  -----------  -----   -------  ---
   1         active        port   3        no
   2         active        port   2        yes
```

Figure 22. Example of a Currently Configured Mirroring Summary on a Source Switch

```
ProCurve# show monitor 1

Network Monitoring

   Session: 1   Session Name:
   ACL: no ACL relationship exists

      Mirror Destination: 48
      Untagged traffic  : untagged    <-- Indicates the no-tag-added option is configured.
      Monitoring Sources  Direction
      ------------------  ---------
      Port: 3             Both
```

Figure 23. Example of Session Output Showing no-tag-added Option

Note

For more information about traffic mirroring, see "Monitoring and Analyzing Switch Operation" in the *Management and Configuration Guide* for your switch. For more information about ACL filtering, see "Access Control Lists (ACLs)" in the *Access Security Guide* for your switch.

Using SNMP to Configure No-Tag-Added

The MIB object hpicfBridgeDontTagWithVlan is used to implement the no-tag-added option, as shown below:

```
hpicfBridgeDontTagWithVlan OBJECT-TYPE
         SYNTAX INTEGER
             {
             enabled(1),
             disabled(2)
             }
         MAX-ACCESS   read-write
         STATUS       current
         DESCRIPTION
            "This oid mentions whether VLAN tag is part of the
             mirror'ed copy of the packet. The value 'enabled'
             denotes that the VLAN tag shouldn't be part of the
             mirror'ed copy; 'disabled' does put the VLAN tag in the
             mirror'ed copy. Only one logical port is allowed.
             This object is persistent and when written the entity
```

```
        SHOULD save the change to non-volatile storage."
    DEFVAL { 2 }
::= { hpicfBridgeMirrorSessionEntry 2 }
```

Operating Notes

- The specified port can be a physical port, a trunk port, or a mesh port.
- Only a single logical port (physical port or trunk) can be associated with a mirror session when the **no-tag-added** option is specified. No other combination of ACL mirroring, VLAN mirroring, or port mirroring can be associated with the mirror session. If more than one logical port is specified, the following error message is displayed:
- Cannot monitor more than 1 logical port with no-tag-added option
- If a port changes its VLAN membership and/or untagged status within the VLAN, the "untagged port mirroring" associated with that port is updated when the configuration change is processed.
- Only four ports or trunks can be monitored at one time when all four mirror sessions are in use (one logical port per mirror session) without VLAN tags being added to the mirrored copy.
- The no-tag-added option can also be used when mirroring is configured with SNMP.
- A VLAN tag is still added to the untagged packets obtained via VLAN-based mirroring.

■ **Enhancement (PR_1000756562)** — This enhancement provides concurrent Web/MAC and 802.1x authentication.

Concurrent Web and MAC Authentication

This enhancement allows Web and MAC authentication concurrently on the same port. It is assumed that MAC authentication will use an existing MAC address.

Conditions for Concurrent Web and MAC Authentication

The following conditions apply for concurrent Web and MAC authentication on the same port:

- A specific MAC address cannot be authenticated by both Web and MAC authentication at the same time.
- Each new Web/MAC Auth client always initiates a MAC authentication attempt. This same client can also initiate Web authentication at any time before the MAC authentication succeeds. If either authentication succeeds then the other authentication (if in progress) is ended. No further Web/MAC authentication attempts are allowed until the client is de-authenticated.

- Web and MAC authentications are not allowed on the same port if unauthenticated VLAN (that is, a guest VLAN) is enabled for MAC authentication. An unauthenticated VLAN can't be enabled for MAC authentication if Web and MAC authentication are both enabled on the port.
- Hitless re-authentication must be of the same type (MAC) that was used for the initial authentication. Non-hitless re-authentication can be of any type.

The remaining Web/MAC functionality, including interactions with 802.1X, remains the same. Web and MAC authentication can be used for different clients on the same port.

Normally, MAC authentication finishes much sooner than Web authentication. However, if Web authentication should complete first, MAC authentication will cease even though it is possible that MAC authentication could succeed. There is no guarantee that MAC authentication ends before Web authentication begins for the client.

These changes are backward compatible with all existing user configurations.

■ **Enhancement (PR_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI **show** command information enhancements.

SSH Enhancements

Overview

The SSH enhancements are:

- AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection.
- Configurable key
- Message Authentication Code (MAC) configuration. A new configuration option provides the ability to configure which MACs a client is permitted to use.
- Feedback information
- SSH CLI **show** command information enhancements

Specifying the Set of Ciphers

The following command allows you to specific which ciphers are available for a client to use for connection. All ciphers are available by default; use the **no** form of the command to disable specific ciphers.

Syntax: [no] ip ssh [cipher <cipher-type>]

Cipher types that can be used for connection by clients. Valid types are:

- *aes128-cbc*
- *3des-cbc*
- *aes192-cbc*
- *aes256-cbc*
- *rijndael-cbc@lysator.liu.se*
- *aes128-ctr*
- *aes192-ctr*
- *aes256-ctr*

Default: All cipher types are available.

Use the **no** *form of the command to disable a cipher type.*

```
ProCurve(config)# no ip ssh cipher 3des-cbc
```

Figure 24. Example of Disabling a Specific Cipher

Configuring Key Lengths and DSA/RSA Support

This enhancement allows you to specify the type and length of the generated host key. The command is:

Syntax: crypto key generate ssh [dsa | rsa [bits <num-bits>]]

Specify the type and length of the host key that is generated.

You can also generate and use a DSA key as the host key. The size of the host key is platform-dependent as different switches have different amounts of processing power. The size is represented by the *<num-bits>* key word and has the values shown in Table 1. The default value is used if **num-bits** is not specified.

Table 1. RSA/DSA Values for Various ProCurve Switches

Platform	Maximum RSA Key Size (in bits)	DSA Key Size (in bits)
5400/3500/6200/8200/2900	1024, 2048, 3072 Default: 2048	1024
2610	1024, 2048 Default: 1024	1024

Message Authentication Code (MAC) Support

This enhancement allows configuration of the set of MACs that are available for selection.

Syntax: [no] ip ssh [mac <MAC-type>]

Allows configuration of the set of MACs that can be selected. Valid types are:

- *hmac-md5*
- *hmac-sha1*
- *hmac-sha1-96*
- *hmac-md5-96*

Default: All MAC types are available.

Use the **no** *form of the command to disable a MAC type.*

Displaying the SSH Information

The **show ip ssh** command has been enhanced to display information about ciphers, MACs, and key types and sizes.

```
ProCurve(config)# show ip ssh

  SSH Enabled     : No                  Secure Copy Enabled : No
  TCP Port Number : 22                  Timeout (sec)       : 120
  IP Version      : IPv4orIPv6
  Host Key Type   : RSA                 Host Key Size       : 1024

  Ciphers : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc,
            rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
  MACs    : hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96

  Ses Type     | Source IP                                        Port
  --- -------- + ------------------------------------------------ -----
  1   console  |
  2   inactive |
  3   inactive |
  4   inactive |
  5   inactive |
  6   inactive |
```

Figure 25. Example of show ip ssh Command Showing Ciphers, MACs and Key Information

Logging Messages

There are new event log messages when a new key is generated and zeroized for the server:

ssh: New <num-bits> -bit [rsa | dsa] SSH host key installed
ssh: SSH host key zeroized

There are also new messages that indicates when a client public key is installed or removed:

ssh: <num-bits>-bit [rsa | dsa] client public key [installed | removed] ([manager| operator] access) (key_comment)
Note: Only up to 39 characters of the key comment are included in the event log message.

Debug Logging

To add ssh messages to the debug log output, enter this command:

```
ProCurve# debug ssh LOGLEVEL
```

where LOGLEVEL is one of the following (in order of increasing verbosity):

- fatal
- error
- info
- verbose

- debug
- debug2
- debug3

Release K.13.17 Enhancements

No enhancements; Bug fixes only.

Release K.13.18 Enhancements

Release K.13.18 includes the following enhancements:

- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the **show tech** command.

Release K.13.19 Enhancements

Release K.13.19 includes the following enhancements:

- **Enhancement (PR_0000003808)** — This enhancement allows the user to create command aliases for use in place of command names and their options.

Using a Command Alias

You can create a simple command alias to use in place of a command name and its options. Choose an alias name that is *not* an existing CLI command already. Existing CLI commands are searched before looking for an alias command; an alias that is identical to an existing command will not be executed.

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

ProCurve recommends that you configure no more than 128 aliases.

Syntax: [no] alias <*name*> <*command*>

Creates a shortcut alias name to use in place of a commonly used command. The **alias** *command is executed from the current config context.*

name: *Specifies the new command name to use to simplify keystrokes and aid memory.*
command: *Specifies an existing command to be aliased. The command must be enclosed in quotes.*

Use the **no** *form of the command to remove the alias.*

For example, if you use the **show interface custom** command to specify the output, you can configure an alias for the command to simplify execution.

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

 Status and Counters - Custom Port Status

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



ProCurve(config)# alias showintstatus “show int custom 1-4 port name:4 type
vlan intrusion speed enabled mdi”
ProCurve(config)#

ProCurve(config)# showintstatus

Status and Counters - Custom Port Status

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

Figure 26. Example of Using the Alias Command with show int custom

Note

Remember to enclose the command being aliased in quotes.

Command parameters for the aliased command can be added at the end of the alias command string. For example:

```
ProCurve(config)# alias shoconfig "show config"
ProCurve(config)# shoconfig status
```

To change the command that is aliased, re-execute the alias name with new command options. The new options are used when the alias is executed.

To display the alias commands that have been configured, enter the **show alias** command.

```
ProCurve(config)# show alias

    Name                 Command
--------------------  ------------------------------
showint               show int
showintstatus         show int custom 1-4 port name:4 type vlan intrusion
                      speed enabled mdi
```

Figure 27. Example of Alias Commands and Their Configurations

- **Enhancement (PR_0000000818)** — This enhancement allows the user to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch.

Configure Logging via SNMP

Overview

Debug messages generated by the software can be sent to a syslog server. This feature provides the ability to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch. The HP enterprise MIB hpicfSyslog.mib is added to allow the configuration and monitoring of syslog. (RFC 3164 supported)

The CLI has some additional parameters to permit interoperability with SNMP that are explained below.

Note

See the section "Command Differences for the ProCurve Series 2600/2800/3400cl/6400cl Switches" on page 113 for command differences on these switches.

Adding a Description for a Syslog Server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP. The CLI command is:

Syntax: logging <ip-addr> control-descr <text_string>]
no logging <ip-addr> [control-descr]

An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. IPv4 addresses only. Use the **no** *form of the command to remove the description.*
Limit: 255 characters

Note*: To remove the description using SNMP, set the description to an empty string.*

```
ProCurve(config)# logging 10.10.10.2 control-descr syslog_one
```

Figure 10. Example of the Logging Command with a Control Description

Caution

Entering the **no logging** command removes ALL the syslog server addresses without a verification prompt.

Adding a Priority Description

You can add a user-friendly description for the set of syslog filter parameters using the **priority-descr** option. The description can be added with the CLI or SNMP. The CLI command is:

Syntax: logging priority-descr <text_string>
no logging priority-descr

Provides a user-friendly description for the combined filter values of **severity** *and* **system module**. *If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. Use the* **no** *form of the command to remove the description.*
Limit: 255 characters

```
ProCurve(config)# logging priority-descr severe-pri
```

Figure 11. Example of the Logging Command with a Priority Description

Note

A notification is sent to the SNMP agent if there are any changes to the syslog parameters either through the CLI or with SNMP.

Command Differences for the ProCurve Series 2600/2800/3400cl/6400cl Switches

CLI Commands

The ProCurve series 2600/2800/3400cl/6400cl switches do not have the following CLI logging commands:

- **logging severity**
- **logging system-module**

SNMP Commands

The ProCurve series 2600/2800/3400cl/6400cl switches do not support the following SNMP objects:

- hpicfSyslogPrioritySeverity
- hpicfSyslogSystemModule

Operating Notes

- Duplicate IP addresses are not stored in the list of syslog servers.

- If the default severity value is in effect, all messages that have severities greater than the default value are passed to syslog. For example, if the default severity is “debug”, all messages that have severities greater than debug are passed to syslog.
- There is a limit of six syslog servers. All syslog servers are sent the same messages using the same filter parameters.
- An error is generated for an attempt to add more than six syslog servers.

■ **Enhancement (PR_0000003390)** — This enhancement allows the user to customize Web Authentication HTML pages.

Customizing Web Authentication HTML Files

The Web Authentication process displays a series of Web pages and status messages to the user during login. The Web pages that are displayed can be:

- Generic, default pages generated directly by the switch software
- Customized pages hosted on a local Web server.

By creating customized login Web pages, you can improve the “look and feel” of the Web Authentication process to correspond more closely with your network and business needs. For example, you can:

- Identify the network that a client is trying to log into.
- Provide contact information if a client has difficulty connecting to the network.
- Incorporate CSS styles consistent with the appearance of your network.

To implement these “enhanced” Web Authentication pages, you need to:

- Configure and start a Web server on your local network,
- Customize the HTML template files and make them accessible to the Web server
- Configure the switch to display the customized files by using the **aaa port-access web-based** <*port-list*> **ewa-server** command.

The customized Web pages you create can be hosted on up to three Web servers in your network. Implementing multiple Web servers provides redundancy in case access to any of the other servers fail.

Implementing Customized Web-Auth Pages

Guidelines

- Customized Web Authentication pages are configured per switch, so that each Web-Auth enabled port displays the same customized pages at client login.

- You can use up to three Web servers in your network to store and display customized Web pages for Web Authentication login.
- To configure a Web server on your network, follow the instructions in the documentation provided with the server.
- Before you enable custom Web Authentication pages, you should:

  Determine the IP address or host name of the Web server(s) that will host your custom pages.

  Determine the path on the server(s) where the HTML files (including all graphics) used for the login pages are stored.

  Configure and start the Web server(s).

  Create the customized Web pages as described in "Guidelines for Customizing the HTML Templates" on page 115, and store them in the document path on the designated servers.

  Test that they are accessible at the designated URL(s).

Enabling Customized Web Authentication Pages

To enable customized Web-Auth pages on a switch, use the **aaa port-access web-based ewa-server** command to specify the server's IP address or host name and the path to the customized HTML files on the server. See "Commands for Using Custom Web Authentication Pages" on page 128 for syntax details.

Guidelines for Customizing the HTML Templates

When you customize an HTML template, follow these guidelines:

- Do not change the name of any of the HTML files (**index.html**, **accept.html**, and so on).
- Some template pages use Embedded Switch Includes (ESIs) or Active Server Pages. These should not be modified when customizing HTML files. ESIs behave as follows:

i. A client's Web browser sends a request for an HTML file. The switch passes the request to a configured Web server.

ii. The Web server responds by sending a customized HTML page to the switch. Each ESI call in the HTML page is replaced with the value (in plain text) retrieved by the call.

iii. The switch sends the final version of the HTML page to the client's Web browser.

- Store all customized login Web pages (including any graphics) that you create for client login on each Web server at the path you will configure with the **aaa port-access web-based ewa-server** command.

Customizable HTML Templates

The sample HTML files described in the following sections are customizable templates. To help you create your own set HTML files, a set of the templates can be found on the download page for 'K' software.

File Name	Page
index.html	116
accept.html	118
authen.html	119
reject_unauthvlan.html	120
timout.html	122
retry_login.html	123
sslredirect.html	124
rejectnovlan.html	126

User Login Page (index.html)

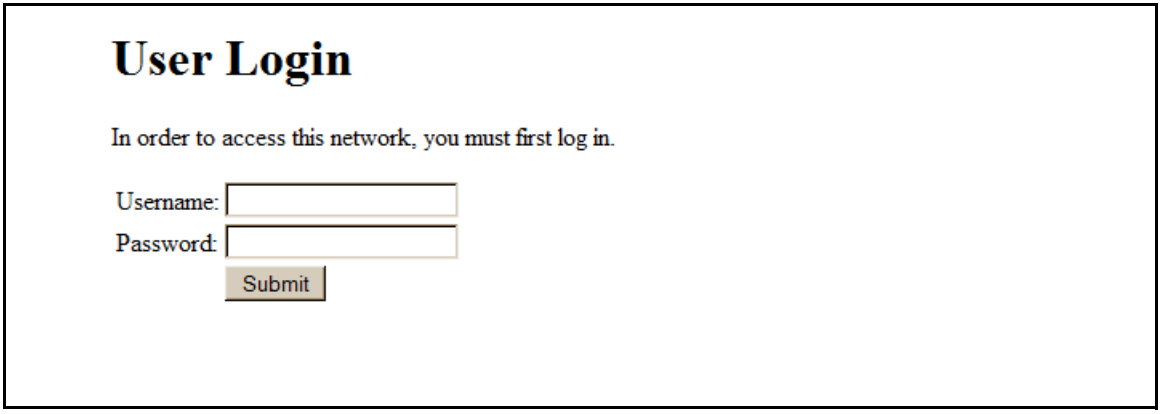

Figure 12. User Login Page

The **index.html** file is the first login page displayed, in which a client requesting access to the network enters a username and password. In the **index.html** Template file, you can customize any part of the source code except for the form that processes the username and password entered by a client.

```
<!--
ProCurve Web Authentication Template
index.html
-->
<html>

   <head>
      <title>User Login</title>
   </head>

   <body>
      <h1>User Login</h1>
      <p>In order to access this network, you must first log in.</p>

      <form action="/webauth/loginprocess" method="POST">
         <table>
            <tr>
               <td>Username: </td>
               <td><input name="user" type="text"/></td>
            </tr>
            <tr>
               <td>Password: </td>
               <td><input name="pass" type="password"/></td>
            </tr>
            <tr>
               <td></td>
               <td><input type="submit" value="Submit"/></td>
            </tr>
         </table>
      </form>

   </body>

</html>
```

Figure 13. HTML Code for User Login Page Template

Access Granted Page (accept.html)

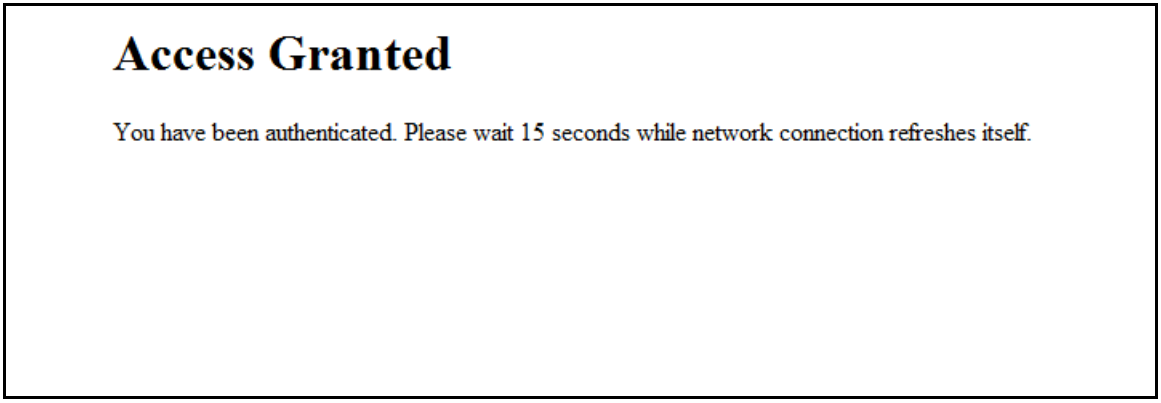

Figure 14. Access Granted Page

The **accept.html** file is the Web page used to confirm a valid client login. This Web page is displayed after a valid username and password are entered and accepted.

The client device is then granted access to the network. To configure the VLAN used by authorized clients, specify a VLAN ID with the **aaa port-access web-based auth-vid** command parameter when you enable Web Authentication.

The **accept.html** file contains the following ESIs, which should not be modified:

- The WAUTHREDIRECTTIMEGET ESI inserts the value for the waiting time used by the switch to redirect an authenticated client while the client renews its IP address and gains access to the network.
- The WAUTHREDIRECTURLGET ESI inserts the URL configured with the **redirect-url** parameter (see page 4-25 in the *Access Security Guide*.) to redirect a client login or the first Web page requested by the client.

```
<!--
ProCurve Web Authentication Template
accept.html
-->
<html>
   <head>
      <title>Access Granted</title>

      <!-- The following line is required to automatically redirect -->
    <meta http-equiv="refresh"content="<!- ESI(WAUTHREDIRECTTIMEGET, 1) ->;URL=<!
ESI(WAUTHREDIRECTURLGET, 1) ->"/>
   </head>

   <body>
      <h1>Access Granted</h1>
      <!--
         The ESI tag below will be replaced with the time in seconds until
         the page redirects.
      -->
     <p>You have been authenticated.  Please wait <!- ESI(WAUTHREDIRECTTIMEGET, 1
-> seconds while network connection refreshes itself.</p>
   </body>

</html>
```

Figure 15. HTML Code for Access Granted Page Template

Authenticating Page (authen.html)

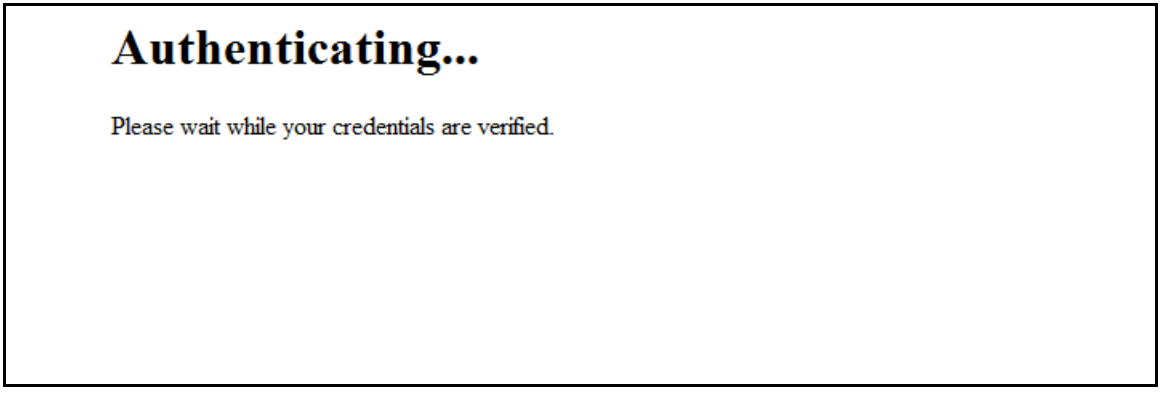

Figure 16. Authenticating Page

The **authen.html** file is the Web page used to process a client login and is refreshed while user credentials are checked and verified.

```
<!--
ProCurve Web Authentication Template
authen.html
-->
<html>

   <head>
      <title>Authenticating</title>

      <!-- The following line is always required -->
      <meta http-equiv="refresh" content="2;URL=/webauth/statusprocess">
   </head>

   <body>
      <h1>Authenticating...</h1>
      <p>Please wait while your credentials are verified.</p>
   </body>

</html>
```

Figure 17. HTML Code for Authenticating Page Template

Invalid Credentials Page (reject_unauthvlan.html)

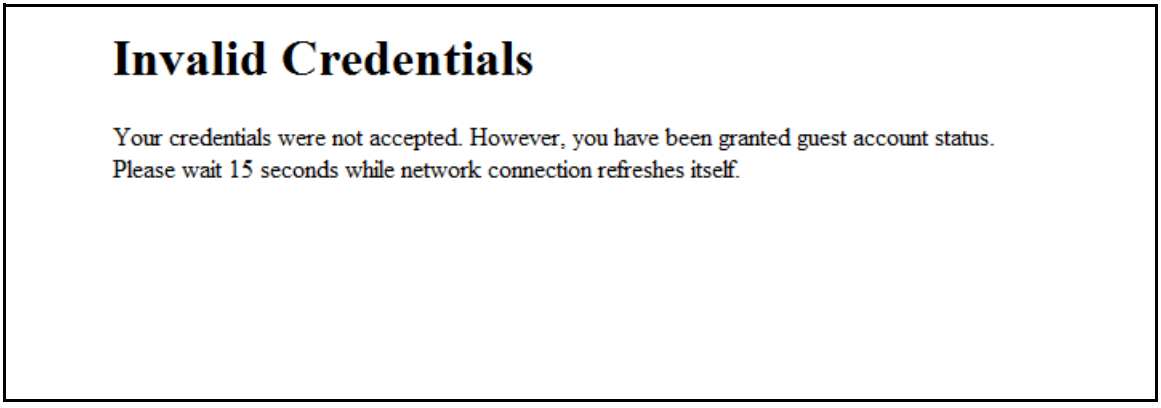

Figure 18. Invalid Credentials Page

The **reject_unauthvlan.html** file is the Web page used to display login failures in which an unauthenticated client is assigned to the VLAN configured for unauthorized client sessions. You can configure the VLAN used by unauthorized clients with the **aaa port-access web-based unauth-vid** command when you enable Web Authentication.

The WAUTHREDIRECTTIMEGET ESI inserts the value for the waiting time used by the switch to redirect an unauthenticated client while the client renews its IP address and gains access to the VLAN for unauthorized clients. This ESI should not be modified.

```
<!--
ProCurve Web Authentication Template
reject_unauthvlan.html
-->
<html>
   <head>
      <title>Invalid Credentials</title>

      <!-- The following line is required to automatically redirect -->
    <meta http-equiv="refresh"content="<!- ESI(WAUTHREDIRECTTIMEGET, 1) ->;URL=<!
ESI(WAUTHREDIRECTURLGET, 1) ->"/>
   </head>

   <body>
      <h1>Invalid Credentials</h1>
      <p>Your credentials were not accepted. However, you have been granted gues
account status. Please wait <!- ESI(WAUTHREDIRECTTIMEGET, 1) -> seconds while networ
connection refreshes itself.</p>
   </body>
</html>
```

Figure 19. HTML Code for Invalid Credentials Page Template

Timeout Page (timeout.html)

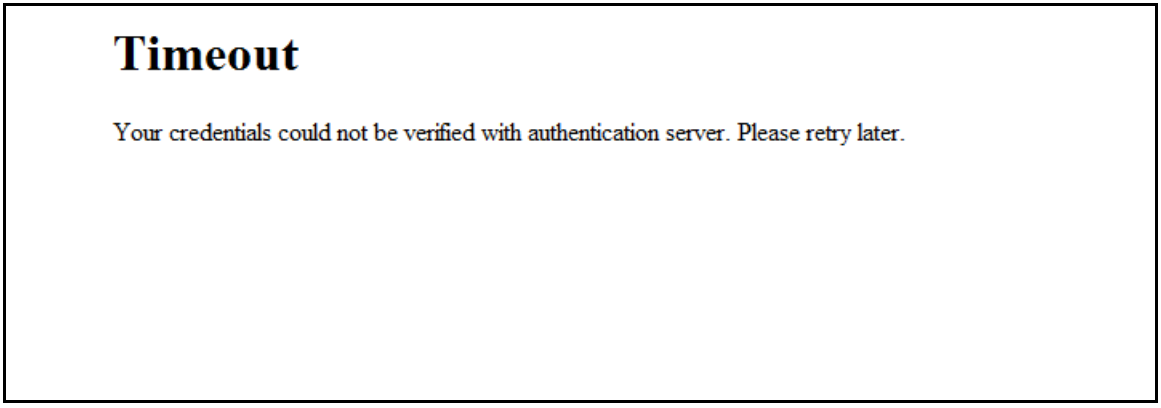

Figure 20. Timeout Page

The **timeout.html** file is the Web page used to return an error message if the RADIUS server is not reachable. You can configure the time period (in seconds) that the switch waits for a response from the RADIUS server used to verify client credentials with the **aaa port-access web-based server-timeout** command when you enable Web Authentication.

```
<!--
ProCurve Web Authentication Template
timeout.html
-->
<html>

   <head>
      <title>Timeout</title>
   </head>

   <body>
      <h1>Timeout</h1>
      <p>Your credentials could not be verified with authentication server.
Please retry later.</p>
   </body>

</html>
```

Figure 21. HTML Code for Timeout Page Template

Retry Login Page (retry_login.html)

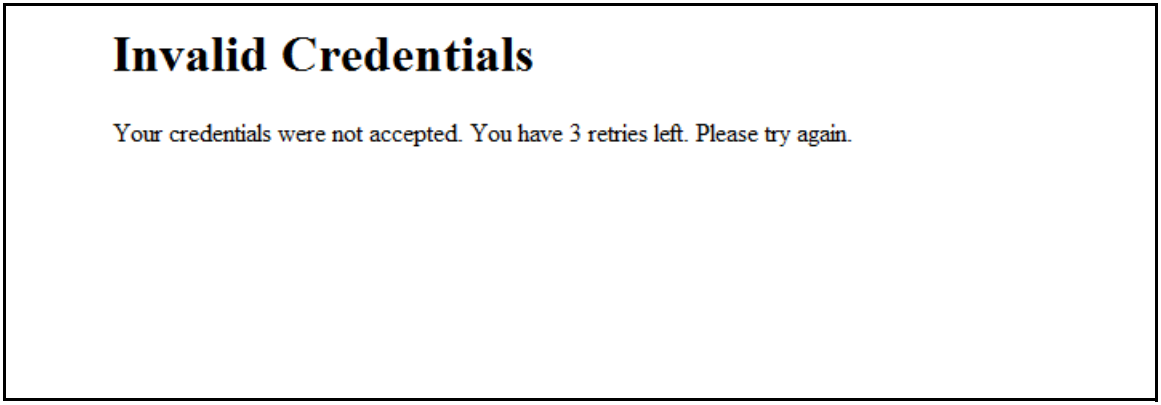

Figure 22. Retry Login Page

The **retry_login.html** file is the Web page displayed to a client that has entered an invalid username and/or password, and is given another opportunity to log in.

The WAUTHRETRIESLEFTGET ESI displays the number of login retries that remain for a client that entered invalid login credentials. You can configure the number of times that a client can enter their user name and password before authentication fails with the **aaa port-access web-based max-retries** commands when you enable Web Authentication. This ESI should not be modified.

```
<!--
ProCurve Web Authentication Template
retry_login.html
-->
<html>

   <head>
      <title>Invalid Credentials</title>

      <!--
         The following line is required to automatically redirect
         the user back to the login page.
      -->
      <meta http-equiv="refresh" content="5;URL=/EWA/index.html">
   </head>

   <body>
      <h1>Invalid Credentials</h1>
     <p>Your credentials were not accepted. You have <!- ESI(WAUTHRETRIESLEFTGET,1
-> retries left. Please try again.</p>
   </body>

</html>
```

Figure 23. HTML Code for Retry Login Page Template

SSL Redirect Page (sslredirect.html)

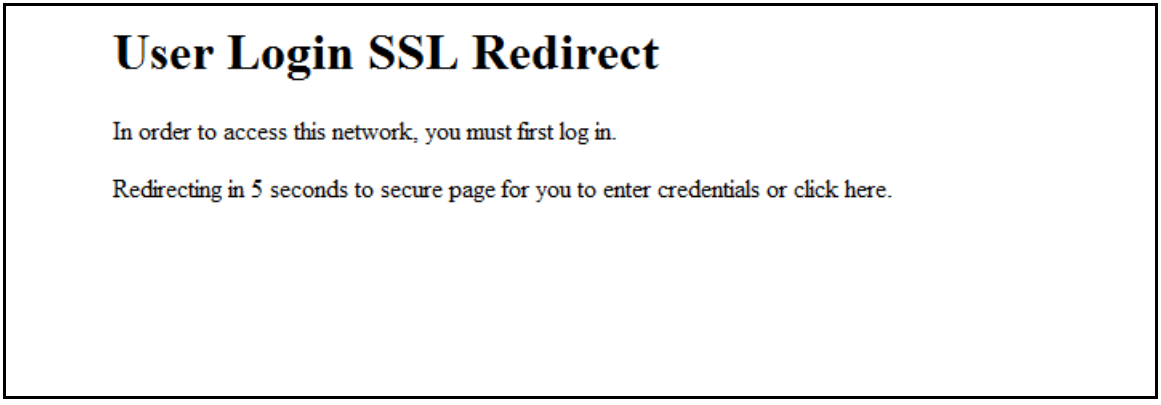

Figure 24. SSL Redirect Page

The **sslredirect** file is the Web page displayed when a client is redirected to an SSL server to enter credentials for Web Authentication. If you have enabled SSL on the switch, you can enable secure SSL-based Web Authentication by entering the **aaa port-access web-based ssl-login** command when you enable Web Authentication.

The WAUTHSSLSRVGET ESI inserts the URL that redirects a client to an SSL-enabled port on a server to verify the client's username and password. This ESI should not be modified.

```
<!--
ProCurve Web Authentication Template
sslredirect.html
-->
<html>

   <head>
      <title>User Login SSL Redirect</title>

      <meta http-equiv="refresh" content="5;URL=https://<!- ESI(WAUTHSSLSRVGET,1
->/EWA/index.html">
   </head>

   <body>
      <h1>User Login SSL Redirect</h1>
      <p>In order to access this network, you must first log in.</p>
     <p>Redirecting in 5 seconds to secure page for you to enter credentials or <
href="https://<!- ESI(WAUTHSSLSRVGET,1) ->/EWA/index.html">click here</a>.</p>
   </body>

</html>
```

Figure 25. HTML Code for SSL Redirect Page Template

Access Denied Page (reject_novlan.html)

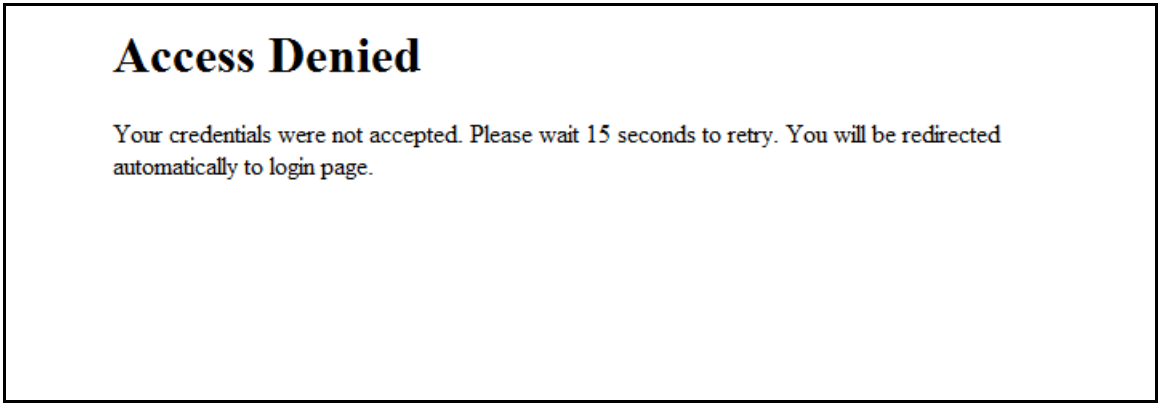

Figure 26. Access Denied Page

The **reject_novlan** file is the Web page displayed after a client login fails and no VLAN is configured for unauthorized clients.

The WAUTHQUIETTIMEGET ESI inserts the time period used to block an unauthorized client from attempting another login. To specify the time period before a new authentication request can be received by the switch, configure a value for the **aaa port-access web-based quiet-period** command when you enable Web Authentication. This ESI should not be modified.

```
<!--
ProCurve Web Authentication Template
reject_novlan.html
-->
<html>

   <head>
      <title>Access Denied</title>

      <!--
         The line below is required to automatically redirect the user
         back to the login page.
      -->
      <meta http-equiv="refresh" content="<!- ESI(WAUTHQUIETTIMEGET,1)
->;URL=/EWA/index.html">
   </head>

   <body>
      <h1>Access Denied</h1>
     <p>Your credentials were not accepted. Please wait <!- ESI(WAUTHQUIETTIMEGET
1) -> seconds to retry. You will be redirected automatically to login page.</p>
   </body>

</html>
```

Figure 27. HTML Code for Access Denied Page Template

Commands for Using Custom Web Authentication Pages

Command	Page
[no] aaa port-access web-based <*port-list*> ewa-server	128
show port-access web-based config <*port-list*>	129

aaa port-access web-based ewa-server

Syntax: aaa port-access web-based [ewa-server <*ipv4-addr* | *hostname*> [<*page-path*>]]

Configures a connection with the Web server at the specified IPv4 address (ipv4-addr) or host name (ipv4-addr) on which customized login Web pages used for Web Authentication are stored. A maximum of 3 Web servers may be configured on the switch.

*The optional <page-path> parameter defines the directory path on the server where all customized login Web pages (graphics, HTML frames, and HTML files) are stored. (Default: The default <page-path> value is "**/**" for root directory. If the Web server is also used for other purposes, you may wish to group the HTML files in their own directory, for example in "**/EWA/**")*

```
ProCurve Switch (config)# aaa port-access web-based 47 ewa-server 10.0.12.179
/EWA
ProCurve Switch (config)# aaa port-access web-based 47 ewa-server 10.0.12.180
/EWA
ProCurve Switch (config)#
```

Figure 29. Adding Web Servers with the aaa port-access web-based ews-server Command

```
ProCurve Switch (config)# aaa port-access web-based 47 ewa-server 10.0.12.181
ProCurve Switch (config)#
```

Figure 31. Removing a Web Server with the aaa port-access web-based ews-server Command

show port-access web-based config

Syntax: show port-access web-based config [<*port-list*>]

Displays the currently configured Web Authentication settings for all ports or specified ports, including web-specific settings for password retries, SSL login status, and a redirect URL, if specified.

```
ProCurve Switch (config)# show port-access web-based 47 config

 Port Access Web-Based Configuration

  DHCP Base Address : 192.168.0.0
  DHCP Subnet Mask  : 255.255.255.0
  DHCP Lease Length : 10
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

  EWA_Server Address | EWA-Server Page Path
  ------------------ + --------------------
  10.0.12.179        | /EWA
  10.0.12.180        | /EWA

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


ProCurve Switch (config)#
```

Figure 33. Example of show port-access Web-based config Command Output

Enhancement (PR_1000460265) — This enhancement provides Dynamic IP Lockdown, which is used to prevent IP source address spoofing on a per-port and per-VLAN basis.

Dynamic IP Lockdown

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

Protection Against IP Source Address Spoofing

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

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

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

Differences Between Switch Platforms

There are some differences in the feature set and operation of Dynamic IP Lockdown, depending on the switch on which it is implemented. These are listed below.

- There is no restriction on GVRP on 3500/5400 switches. On 2600/2800/3400cl switches, Dynamic IP Lockdown is not supported if GVRP is enabled on the switch.
- Dynamic IP Lockdown has the host limits shown in the table below. There is a DHCP snooping limit of 8,000 entries.

Switch	Number of Hosts	Comments
3500/5400	64 bindings per port Up to 4096 bindings per switch	This limit is shared with DHCP snooping because they both use the snooping database.
3400cl/2800	32 bindings per port Up to 32 VLANs with DHCP snooping enabled	This is not guaranteed as the hardware resources are shared with QoS.
2600	8 bindings per port Up to 8 VLANs with DHCP snooping enabled	This is not guaranteed as the hardware resources are shared with QoS.

- A source is considered "trusted" for all VLANs if it is seen on any VLAN without DHCP snooping enabled.
- On the ProCurve switch series 5400 and 3500, dynamic IP lockdown is supported on a port configured for statically configured port-based ACLs.

Prerequisite: DHCP Snooping

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

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

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

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

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

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

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

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

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

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

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

Figure 28. Sample DHCP Snooping Entries

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

IP Address	MAC Address	VLAN ID
10.0.10.1	001122-110011	5

Figure 29. An Example of a Static Configuration Entry

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

```
permit 10.0.8.5 001122-334455 vlan 2

permit 10.0.8.7 001122-334477 vlan 2

permit 10.0.10.3 001122-334433 vlan 5

permit 10.0.10.1 001122-110011 vlan 5

deny any vlan 1-10

permit any
```

Figure 30. Example of Internal Statements used by Dynamic IP Lockdown

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

Enabling Dynamic IP Lockdown

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

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

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

Operating Notes

- Dynamic IP lockdown is enabled at the port configuration level and applies to all bridged or routed IP packets entering the switch. The only IP packets that are exempt from dynamic IP lockdown are broadcast DHCP request packets, which are handled by DHCP snooping.
- DHCP snooping is a prerequisite for Dynamic IP Lockdown operation. The following restrictions apply:
  - DHCP snooping is required for dynamic IP lockdown to operate. To enable DHCP snooping, enter the **dhcp-snooping** command at the global configuration level.
  - Dynamic IP lockdown only filters packets in VLANs that are enabled for DHCP snooping. In order for Dynamic IP lockdown to work on a port, the port must be configured for at least one VLAN that is enabled for DHCP snooping.

    To enable DHCP snooping on a VLAN, enter the **dhcp-snooping vlan [***vlan-id-range***]** command at the global configuration level or the **dhcp-snooping** command at the VLAN configuration level.
  - Dynamic IP lockdown is not supported on a trusted port. (However, note that the DHCP server must be connected to a trusted port when DHCP snooping is enabled.)

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

  For more information on how to configure and use DHCP snooping, refer to the "Configuring Advanced Threat Protection" chapter in the *Access Security Guide*.
- After you enter the **ip source-lockdown** command (enabled globally with the desired ports entered in <*port-list*>), the dynamic IP lockdown feature remains disabled on a port if any of the following conditions exist:
  - If DHCP snooping has not been globally enabled on the switch.
  - If the port is not a member of at least one VLAN that is enabled for DHCP snooping.
  - If the port is configured as a trusted port for DHCP snooping.

  Dynamic IP lockdown is activated on the port only after you make the following configuration changes:
  - Enable DHCP snooping on the switch.
  - Configure the port as a member of a VLAN that has DHCP snooping enabled.

  - Remove the trusted-port configuration.

- You can configure dynamic IP lockdown only from the CLI; this feature cannot be configured from the Web management or menu interface.
- If you enable dynamic IP lockdown on a port, you cannot add the port to a trunk.
- Dynamic IP lockdown must be removed from a trunk before the trunk is removed.

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

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

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

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

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

Potential Issues with Bindings

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

Adding a Static Binding

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

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

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

Note

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

Verifying the Dynamic IP Lockdown Configuration

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

Syntax: show ip source-lockdown status

An example of the **show ip source-lockdown status** command output is shown in Figure 31. Note that the operational status of all switch ports is displayed. This information indicates whether or not dynamic IP lockdown is supported on a port.

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

Global State: Enabled

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

Figure 31. Example of show ip source-lockdown status Command Output

Displaying the Static Configuration of IP-to-MAC Bindings

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

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

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

An example of the **show ip source-lockdown bindings** command output is shown in Figure 32.

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

Dynamic IP Lockdown (DIPLD) Bindings

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

Figure 32. Example of show ip source-lockdown bindings Command Output

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

Debugging Dynamic IP Lockdown

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

Syntax: debug dynamic-ip-lockdown

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

Counters for denied packets are displayed in the **debug dynamic-ip-lockdown** command output. Packet counts are updated every five minutes. An example of the command output is shown in Figure 33.

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

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

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

Figure 33. Example of debug dynamic-ip-lockdown Command Output

Release K.13.20 Enhancements

Release K.13.20 includes the following enhancements:

- **Enhancement (PR_0000004124)** — Support is added for the J9144A ProCurve 10-GbE X2-SC LRM Optic, an X2 form-factor transceiver that supports the 10-Gigabit LRM standard, providing 10-gigabit connectivity for up to 220 meters on legacy multimode fiber.

Release K.13.21 Enhancements

No enhancements; Bug fixes only.

Release K.13.22 Enhancements

No enhancements; Bug fixes only.

Release K.13.23 Enhancements

No enhancements; Bug fixes only.

Release K.13.24 through K.13.25 Enhancements

No enhancements; Bug fixes only.

Release K.13.26 through K.13.39 Enhancements

No enhancements; Software never built.

Release K.13.40 Enhancements

Release K.13.40 includes the following enhancements (Never released):

- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable.

LACP and Link Traps Global Disable

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

The new SNMP OIDs are:

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

hpSwitchLACPAllPortsStatus OBJECT-TYPE
   SYNTAX INTEGER {
```

```
                    disabled (1),
                    active (2),
                    passive (3)

                }

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

hpSwitchLinkUpDownTrapAllPortsStatus OBJECT-TYPE
   SYNTAX INTEGER {
                    enable (1),
                    disable (2)
                  }
   ACCESS  read-write
   STATUS current
   DESCRIPTION "Used to either enable/disable the Link Up/Link Down traps
                for all the ports."
   ::= { hpSwitchPortConfig 3 }
```

- **Enhancement (PR_0000003128)** — The ability to clear statistics was added.

Clear Statistics Without Reboot

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

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

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

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

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

Note

The clearing of statistics cannot be uncleared.

- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased.

Increase MAC Lockout to 64

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

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

- **Enhancement (PR_0000007388)** — Crash Log Debug was enhanced.

Configure Logging via SNMP

Debug messages generated by the software can be sent to a syslog server. This feature provides the ability to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch. The HP enterprise MIB hpicfSyslog.mib is added to allow the configuration and monitoring of syslog. (RFC 3164 supported)

The CLI has some additional parameters to permit interoperability with SNMP that are explained below.

Adding a Description for a Syslog Server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP. The CLI command is:

Syntax: logging <*ip-addr*> control-descr <*text_string*>]
no logging <*ip-addr*> [control-descr]

An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. IPv4 addresses only. Use the **no** *form of the command to remove the description.*
Limit: 255 characters

Note*: To remove the description using SNMP, set the description to an empty string.*

```
ProCurve(config)# logging 10.10.10.2 control-descr syslog_one
```

Figure 34. Example of the Logging Command with a Control Description

Caution

Entering the **no logging** command removes ALL the syslog server addresses without a verification prompt.

Adding a Priority Description

You can add a user-friendly description for the set of syslog filter parameters using the **priority-descr** option. The description can be added with the CLI or SNMP. The CLI command is:

Syntax: logging priority-descr <*text_string*>
no logging priority-descr

Provides a user-friendly description for the combined filter values of **severity** *and* **system module***. If no description is entered, this is blank. If <text_string> contains white space, use quotes around the string. Use the* **no** *form of the command to remove the description.*
Limit: 255 characters

```
ProCurve(config)# logging priority-descr severe-pri
```

Figure 35. Example of the Logging Command with a Priority Description

Note

A notification is sent to the SNMP agent if there are any changes to the syslog parameters either through the CLI or with SNMP.

Operating Notes

- Duplicate IP addresses are not stored in the list of syslog servers.
- If the default severity value is in effect, all messages that have severities greater than the default value are passed to syslog. For example, if the default severity is “debug”, all messages that have severities greater than debug are passed to syslog.
- There is a limit of six syslog servers. All syslog servers are sent the same messages using the same filter parameters.
- An error is generated for an attempt to add more than six syslog servers.

Release K.13.41 Enhancements

No enhancements; Bug fixes only. (Not a public release)

Release K.13.42 Enhancements

No enhancements; Bug fixes only. (Never released)

Release K.13.43 Enhancements

Release K.13.43 includes the following enhancements (Not a public release):

- **Enhancement (PR_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added. Note that after being disabled and subsequently re-enabled, the USB port may not function consistently with the PCM USB Autorun features until the switch has been reloaded.

Release K.13.44 Enhancements

No enhancements; Bug fixes only. (Not a public release)

Release K.13.45 Enhancements

The following problems were resolved in release K.13.45.

- **Enhancement (PR_0000010783)** — Support was added for the following products.

  J9099B - ProCurve 100-BX-D SFP-LC Transceiver

  J9100B - ProCurve 100-BX-U SFP-LC Transceiver

  J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC

  J9143B – ProCurve 1000-BX-U SFP-LC Mini-GBIC

Release K.13.46 through K.13.48 Enhancements

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

Release K.13.49 Enhancements

No new enhancements, software fixes only.

Software Fixes in Release K.11.12 - K.13.49

Software fixes are listed in chronological order, oldest to newest.

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.00 code branch with no intervening releases.

The first production software release for the 8212zl switch is K.12.31. Release K.12.57 is the last public release of the K.12.*xx* software. The 3500yl, 6200yl, 5400zl, and 8212zl software code was rolled to the K.13.0*x* code branch with no intervening releases.

Release K.11.12

The following problems were resolved in release K.11.12 (never released)

- **ACL/QoS (PR_1000317233)** — Under some circumstances, the Switch may apply an ACL or QoS configuration setting incorrectly.
- **Configuration/Security (PR_1000316441)** — Operator level can save Manager privilege level changes to the configuration.
- **Crash Log (PR_1000309533)** — Incorrect crash message displayed in the log, "Too many HSL interrupts".
- **Crash (PR_1000317489)** — Changing the QoS/ACL portion of the running configuration may cause a switch module to crash with a message similar to:

  ```
  CL Int status=0x10000000
  ```

- **Gig-T SFP Modules (PR_1000316433)** — The switch accepts a Gig-T SFP dual personality module when it should not accept these modules.w
- **Help file enhancement (PR_1000300491)** — Added support for Help files. Switch can provide a navigation pane on the left side of the screen containing 'Contents' and 'Search' capability.
- **10 Gig Transceiver (PR_1000317965)** — Switch reports incorrect Link status when a defective fiber cable is connected to the Switch.
- **LED (PR_1000316434)** — If a mini-GBIC is installed during switch bootup, that port's link LED will not turn on.

- **MSTP Enhancement (PR_1000310463)** — Implementation of legacy path cost MIB and CLI option for MSTP.
- **RSTP (PR_1000307278)** — Replacing an 802.1D bridge device with an end node (non-STP device) on the same Switch port, can result in the RSTP Switch sending TCNs.
- **Web UI (PR_1000303371)** — In the Web User Interface, the QOS Device Priority window scroll bar does not allow sufficient scrolling to view all entries.
- **Web UI (PR_1000311917)** — When the last port on the last card is configured in a trunk or mesh, and a user browses to a specific location in the Web user interface, the HTTP Web server degrades the switch, causing the Web user interface to hang.

Release K.11.13

The following problems were resolved in release K.11.13 (never released)

- **Routing (PR_1000306239)** — In some cases, the command '**show ip route**' may display incorrect information.
- **Self-test (PR_1000315509)** — The self-test LED does not turn off after bootup of an empty chassis.
- **sFlow (PR_1000317785)** — Using Inmon Traffic Server, traffic will be reported on ports with no traffic present. Other ports may or may not have faulty counter reports.

Release K.11.14

The following problems were resolved in release K.11.14 (never released)

- **SNMP (PR_1000315054)** — SNMP security violations are entering the switch syslog when a valid SNMPv3 'get' operation is initiated.
- **Web (PR_1000302713)** — When using the Web interface and a large amount of stacking interactions occur, portions of the information from the stack commander may no longer appear.

Release K.11.15

The following problems were resolved in release K.11.15 (never released)

- **CLI (PR_1000298299)** — After a reboot, the Switch does not provide warning that the running configuration and startup configuration differ, and does not offer an option to save the running configuration.

- **CLI (PR_1000315256)** — Inconsistent error message, "`Resource unavailable`," when configuring more than the maximum number of allowed static IP routes.
- **Crash (PR_1000322009)**— The Switch may crash with a message similar to:

  ```
  Software exception in ISR at queues.c:123.
  ```

- **Menu (PR_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.

Release K.11.16

The following problems were resolved in release K.11.16 (not a general release)

- **10 GbE module (PR_1000321201)** — At a high temperature and with long cables, the Switch 3500yl X2/CX4 10-GbE module (J8694A) may not work properly.

Release K.11.17

The following problems were resolved in release K.11.17

- **Stacking (PR_1000298299)** - The Stack Commander setting is not written to the configuration file, so Web/Stacking does not work.

Release K.11.32

The following problems were resolved in release K.11.32

- **Authentication (PR_1000334731)** — PEAP/TLS EAP types with IAS Radius Server fail to authenticate.
- **CLI (PR_1000298038)** — The command "**show arp**" displays incomplete information.
- **CLI (PR_1000308346)** — The command "**show tech**" failed to execute.
- **CLI (PR_1000308601)** — The Stack Close Up device view does not display all stack members.
- **CLI (PR_1000329325)** — Unrecognizable characters printed to console on User Authentication timeout when logging in via TACAS server.
- **CLI (PR_1000329977)** — User is unable to edit any SNMPv3 target address entries.
- **Config (PR_1000326255)** — The stacking interval setting does not appear in the startup or running configuration files.
- **Crash (PR_1000228633)** — The Switch may crash with a message similar to:

```
Software exception at ldbal_cost.c:1577 -- in 'eDrvPoll', task ID =
0x1760650-> ASSERT: failed.
```

- **Crash (PR_1000314305)** — The switch may crash with a message similar to:

  ```
  Software exception at ipamMApi.c:1592/1594 -- in 'eRouteCtrl'
  ```

- **Crash (PR_1000323759)** — The Switch may crash with a message similar to:

  ```
  TLB Miss: Virtual Addr=0x00000185 IP=0x8027ae04 Task='mLACPCtrl'
  Task ID=0x81597410 fp:0x00000000 sp:0x815972d0 ra:0x8027aa90
  sr:0x1000fc01.
  ```

- **Crash (PR_1000324041)** — A module may crash due to ACL Parity Interrupt with a message similar to

  ```
  'ACL Int stats=0x1000000 28=0x80000b2'.
  ```

- **Crash (PR_1000325030)** — The Switch may crash with a message similar to:

  ```
  'Software exception at vls_dyn_reconfig.c:1939 -- in 'mLpmgrCtrl', task
  ID = 0xa139a80'.
  ```

- **Crash (PR_1000325540)** — The Switch may crash with a message similar to:

  ```
  Software exception at sw_sem.c:712 -- in 'mSnmpCtrl.
  ```

- **Crash (PR_1000327132)** — The Switch may crash with a message similar to:

  ```
  Software exception in ISR at btmDmaApi.c:304.
  ```

- **Crash (PR_1000329818)** — The Switch may crash with a message similar to:

  ```
  assert in btmDmaApi.c:289 - out of msgs, need to throttle rmon & syslog
  msgs.
  ```

- **Crash (PR_1000330009)** — The Switch may crash with a message similar to:

  ```
  slave assert at bttfSlaveLearn.c:1426 - extended bcast loop condition.
  ```

- **Crash (PR_1000332703)** — The Switch may crash with a message similar to:

  ```
  slave assert at ngDmaRx.c:495 - ease sample outbound received a fragment.
  ```

- **Crash (PR_1000329485)** — Broadcast loop creates additional packets causing throughput traffic to decrease.

- **Crash/ACL (PR_1000332850)** — When authenticating using Radius ACLS, configuring and un-configuring multiple ACLs may cause the Switch to crash.

- **Crash (PR_1000334992)** — The Switch may crash with a message similar to:

  ```
  "Software exception in ISR at btmDmaApi.c:289 -> No resources avail-
  able".
  ```

- **Crash (PR_1000335430)** — The Switch may crash with a message similar to:

  ```
  "Cam range reservation error" crash at aqSlaveRanges.c:172.
  ```

- **Event Log (PR_1000308669)** — After a Switch reset, the event log does not display correct information.
- **Event Log (PR_1000310958)** — Unsupported modules do not produce an event log message in the Switch.
- **Fault LED (PR_1000314005)** — Upon a fan fault, the fault LED does not indicate an error.
- **Flash Memory (PR_1000320941)** — An incorrect error message is displayed when the Switch experiences a Flash memory failure.
- **Flow Control (PR_1000333879)** — Flow Control not functioning properly.
- **Help Menu (PR_1000307772)** — The Help menu text for command "router pim rp-candidate hold-time" displayed incorrect values.
- **Help Menu (PR_1000326670)** — Web User Interface Help file link URLs exceed maximum length.
- **ICMP (PR_1000315805)** — When the Switch receives a UDP packet on a closed port, Switch fails to send an ICMP response message back to the sender.
- **ICMP/Rate Limiting (PR_1000319946)** — Configuring ICMP Rate Limiting on interfaces causes the Switch to create duplicate requests, which affects the total throughput of the blade.
- **LED (PR_1000325259)** — Test LED flashing wrong color when a defective Mini-GBIC is installed.
- **LLDP (PR_1000319356)** — LLDP does not discover CDPv2 devices.
- **MAC Authentication (PR_1000329738)** — Switch may improperly flush the ARP cache when adding or removing an authorized MAC address.
- **MAC Authentication (PR_1000335314)** — While authenticating multiple ports via MAC authentication, the Switch successfully authenticates the port but fails to learn the source MAC address.
- **Meshing (PR_1000325260)** — With meshing enabled, it is possible that packet buffers may get corrupted resulting in a Switch reboot.
- **Module (PR_1000307404)** — With no cable attached, the X2 CX4 transceiver link LED remains on after a switch power up or hot swap of module.
- **Modules (PR_1000314454)** — Blades fail to reboot (retry) after failing a selftest.

- **Module (PR_1000330312)** — Booting up the Switch with an unsupported module installed may cause all existing modules to fail.
- **MSTP Enhancement (PR_1000331792)** — Implementation of Spanning-tree BPDU Filter and SNMP Traps.
- **Power Supply (PR_1000310159)** — After power supply failovers, the Switch incorrectly reports power being available on ports that are actually powered down.
- **QoS/Rate Limiting (PR_1000319946)** — QoS/Rate limiting may stop working or impact unwanted traffic streams.
- **QOS (PR_1000325028)** — Switch may crash after configuring QOS device-priority.
- **SNMPv3 (PR_1000325021)** — SNMPv3 lines may mistakenly be removed from the configuration file.
- **STP (PR_1000333992)** — In a redundant STP network with PIM running, PIM packets may get assigned a higher queue priority than STP packets, which may cause network loops.
- **Switch (PR_1000327506)** — Fixed issue where Switch incorrectly allowed jumbos frames to be configured for 10/100 ports.
- **VLAN (PR_1000334107)** — User is unable to add a port to a VLAN and the Switch responds with an invalid error message.
- **Web UI (PR_1000308213)** — Removed Web Stacking Tab within the Web User Interface for the 5400zl products.
- **Web UI (PR_1000308225)** — When using the Web User Interface, the device view of the Stack Close-up is missing.
- **Web UI (PR_1000311087)** — Serial number for 5400zl products within the Web-UI exceeds the provided rectangle.
- **Web UI (PR_1000322777)** — When using the Web User Interface in the Configuration Tab, a user is unable to modify a port name.
- **Web UI (PR_1000329279)** — When using the Web user interface Commander's Stack Close Up view, some stack members are not displayed.

Release K.11.33

The following problems were resolved in release K.11.33

- **Buffer Leak (PR_1000336963)** — The Switch may run out of packet buffers under certain conditions.
- **Crash/ACL (PR_1000337717)** — The Switch may crash with a message similar to:

```
"Software exception at alloc_free.c:422 -- in 'eDrvPoll'...-> No msg
buffer", when Switch is configured for ACL logging.
```

- **Module J8705A (PR_1000336281)** — The Switch 5400zl 20P 10/100/1000 + 4 mini GBIC module (J8705A) may stop forwarding packets.

Release K.11.34

The following problems were resolved in release K.11.34 (not a general release)

- **CLI (PR_1000323423)** — Entering an incorrect password three times for either the operator or manager levels causes the CLI to display erroneous characters.
- **CLI (PR_1000322029)** — The command "**show vlans**" does not display data correctly in the status field.
- **IDM (PR_1000334365)** — Using EAP/802.1x with IDM ACLs can result in memory leaks.
- **Management (PR_1000337447)** — The switch is unmanageable using Telnet or SNMP.
- **OSPF (PR_1000339542)** — When using the "**show IP route"** or "**show ip route ospf"** commands after configuring an AS External LSA (type 5) with a configured metric, the "show" commands display an incorrect metric value.
- **Web UI (PR_1000331431)** — The QoS Configuration Tab does not work correctly when using the Web User Interface.

Release K.11.35

The following problems were resolved in release K.11.35 (never released)

- **Authentication (PR_1000343377**) — When running the Windows XP 802.1x supplicant and the switch sends a re-authentication, Windows XP prompts the user to re-enter their username and password again.
- **Authentication (PR_1000344961)** — A port with multiple 802.1x users on it will allow traffic to pass for a user after that user's supplicant has been stopped.
- **DHCP (PR_1000323679)** — Client cannot obtain an IP address when two DHCP servers are connected on different local networks.
- **Enhancement (PR_1000336169)** — Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- **Enhancement (PR_1000311957)** — Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.

- **MIB (PR_1000307831)** — The MIB value for **ipAddrTable** is not populated.
- **RIP (PR_1000331536)** — RIP does not send a route poison update in response to a failed route.
- **Show tech (PR_1000294072)** — Show Tech statistics displays incorrect port names for fixed ports.

Release K.11.36

The following problems were resolved in release K.11.36 (never released)

- **10-GbE (PR_1000346107)** — The guaranteed minimum bandwidth feature is not working on 10-GbE ports.

Release K.11.37

The following problems were resolved in release K.11.37 (not a general release)

- **Login (PR_1000347300)** — Login failures do not result in an "Invalid Password" response.

Release K.11.38

The following problems were resolved in release K.11.38 (never released)

- **10-GbE (PR_1000346107)** — The Guaranteed minimum bandwidth feature does not work on 10-GbE ports.
- **CLI (PR_1000305349)** — The command, **no ip router-id**, does not work. Once a router-ID is set, there is no way to remove it.
- **QoS (PR_1000346708)** — IP-Precedence does not set the correct priority if all TOS bits are set to 1.

Release K.11.39

The following problems were resolved in release K.11.39 (never released)

- **Crash (PR_1000344998)** — The switch may crash with a message similar to

```
Software exception at sme.c:103 -- in 'mSess1', task ID = 0x8e05520
-> ASSERT:  failed
```

- **Crash (PR_1000351693)** — The switch may crash with a message similar to

```
Software Exception at rt_table.c.758 --  in 'eRouteCtrl', task ID =
0x8a d6b30 -> Routing Task: Route Destinations exceeded
```

Release K.11.40

The following problems were resolved in release K.11.40 (not a general release)

- **CLI (PR_1000353548)** — Use of the command **show span** incorrectly displays an error,

  ```
  "STP version was changed. To activate the change you must save the
  configuration to flash and reboot the device."
  ```

- **Crash (PR_1000352922)** — The switch may crash with a message similar to

  ```
  mstp_ptx_sm.c:118 -- in 'mMstpCtrl', task ID = 0x8899e70 -> ASSERT:
  failed
  ```

- **Enhancement (PR_1000346164)** — RSTP/MSTP BPDU Protection: When this feature is enabled on a port, the switch will disable (drop the link) a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP TRAP.

Release K.11.41

The following problems were resolved in release K.11.41

- **Enhancement (PR_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **Hang (PR_1000346328)** — Switch hangs during initialization, switch may fail to boot. RMON alarms/events configuration files corrupted.
- **MDI/MDI-X (PR_1000354050)** — Forced MDI and MDIX modes were reversed on the 3500yl - forced MDI was transmitting out pins 3 and 6 instead of 1 and 2, and vice versa.
- **Port Monitoring (PR_1000354067)** — The CLI does not allow users to mirror mesh ports, resulting in "Error setting value monitor for port <n>".
- **SSH (PR_1000350999)** — The SSH login prompts user to "press any key to continue" twice before providing a prompt.
- **Web-UI (PR_1000354104)** — The Web-UI limited the size of the "Common Name" field in the SSL configuration tab to 16 characters

Release K.11.43

Version K.11.42 was never released.

The following problems were resolved in release K.11.43 (not a general release)

- **Crash (PR_1000307842)** — When deleting/removing CLI ACLs, IDM ACLs, management VLAN, or virus throttle lockouts, switch crashes with error similar to:

  ```
  "Delete virtual meter with nonzero rule RefCount".
  ```

- **Crash (PR_1000334982)** — When Web authentication is used with open VLANs, a software exception may occur, with the switch reporting something similar to this.

  ```
  Software exception at wma_vlan_sm.c:289 -- in 'mWebAuth',
  task ID = 0x81e408e0 -> ASSERT: failed
  ```

- **Enhancement (PR_1000358903)** — 802.1X Controlled Directions enhancement. With this change, Administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.

- **VRRP (PR_1000356388)** — VRRP returns the physical MAC address instead of the virtual MAC address when replying with proxy-ARP.

Release K.11.44

The following problems were resolved in release K.11.44 (not a general release)

- **Enhancement (PR_1000361504)** — This enhancement allows STP to detect and block network topology loops on a single port.

Release K.11.46

Version K.11.45 was never released.

The following problems were resolved in release K.11.46 (not a general release)

- **CLI (PR_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.

- **CLI (PR_1000305584)** — The output from the "show power" commands on the ProCurve 3500yl switches references slot letters when it should display port numbers.

- **Crash (PR_1000357083)** — The switch management may run out of packet buffers and crash with a message similar to:

  ```
  Software exception at ngDmaTx.c:722 -- in 'tDevPollTx', task ID = 0x4305c504 ->
  HW DMA DRIVER unable.
  ```

- **Hang (PR_1000359640)** — The switch may hang on initialization and become unresponsive.

Release K.11.47

The following problems were resolved in release K.11.47 (not a general release)

- **Management VLAN (PR_1000299387)** — The management VLAN does not allow connectivity from valid addresses.
- **SNMP (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.

Release K.11.48

The following problems were resolved in release K.11.48 (not a general release)

- **CLI (PR_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **Crash (PR_1000334710)** — When saving changes to the IGMP configuration, the switch may crash with a message similar to this.

```
TLB Miss:  Virtual Addr=0x00000000 IP=0x80591238 Task='mSess1'
```

- **Crash (PR_1000351243)** — The switch may crash at boot-up if more than 1000 VLANs are configured.
- **Enhancement (PR_1000351445)** — The "show tech transceiver" CLI command output now contains the HP part number and revision information for all transceivers on the switch.
- **OSPF (PR_1000363648)** — The "restrict" CLI command in OSPF redistribution does not filter the default route.

Release K.11.49

The following problems were resolved in release K.11.49 (not a general release)

- **802.1X (PR_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports. This fix removes a limitation that requires these steps be done in a specific order.
- **Crash (PR_1000346971)** — When stacking is disabled, the switch may crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x08895e48 HW
Addr=0x39200000 IP=0x007132f8 Task='mSnmpCtrl'
```

- **Enhancement (PR_1000366744)** — DHCP Protection enhancement. For more information about this feature, please watch the ProCurve Web site.

- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.

Release K.11.61

Versions K.11.50 through K.11.59 were never built.

Version K.11.60 was never released.

The following problems were resolved in release K.11.61 (not a general release)

- **802.1X (PR_1000367404)** — Increased the maximum number of 802.1X users per port to 32.
- **Crash (PR_1000366583)** — When a large config is saved using the "write memory" CLI command, the switch may crash with a message similar to:

  ```
  NMI event SW:IP=0x00897870 MSR:0x00029210 LR:0x00100c80 Task='mSess1'
  Task ID=0x8d13fe0.
  ```

Release K.11.62

The following problems were resolved in release K.11.62 (not a general release)

- **ACL (PR_1000368901)** — Outbound access control lists (ACLs) do not function after a reboot.
- **Authorization (PR_1000365285)** — IP Authorized Managers feature behaves incorrectly with regard to Telnet access.
- **CLI (PR_1000313916)** — The CLI output for the "show ip" command is misaligned; the proxy-arp column is shifted over to the left by one.
- **Crash (PR_1000356446)** — When traffic monitoring is in use, the switch may crash with a message similar to this.

  ```
  Data Bus Error: Addr=0x704a6114 Data=0x00000011 flags=0x10000751,
  IP=0x4012eaac Task='mEaseUpdt' TaskID=0x42fef338
  ```

- **Routing (PR_1000350144)** — Adding a VLAN and assigning an IP address to that VLAN through the menu interface takes routing information protocol (RIP) offline in all VLANs.
- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.
- **VLAN (PR_1000356062)** — When configuring from the menu interface, the 3500yl series switches will not allow the following name format for a new VLAN:

  "VLANx" (where "x" is a VLAN number).

Release K.11.63

The following problems were resolved in release K.11.63

- **802.1p QoS (PR_1000368188)** — 802.1p prioritization may not work once a trunk is enabled on a module, unless the user issues the commands "qos type-of service ip-precedence" or "qos type-of service diff-services".
- **Crash (PR_1000368540)** — The switch may crash with a message similar to:

```
Software exception at parser.c:8012 -- in 'mSess2',
task ID = 0x90e10e0 -> ASSERT: failed.
```

- **Menu/Event Log (PR_1000319407)** — Disabling of event log numbers, via the "no log-numbers" CLI command, doesn't work properly when viewing the event log via the Menu. Using the 'next' and 'prev' buttons causes the log numbers to reappear.
- **PCM Traffic Monitoring/Performance Degradation (PR_1000370061)** — The switch is affected by PCM traffic monitoring, causing throughput degradation.
- **RADIUS (PR_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.

Release K.11.64

The following problems were resolved in release K.11.64 (not a general release)

- **Crash (PR_1000372604)** — When multiple of instances of sFlow have been configured via the CLI, the switch may crash with an error similar to:

```
Software exception at sflow.c:1170 -- in 'mEaseCtrl',
task ID = 0x80e5fe0-> ASSERT:  failed.
```

- **Enhancement (PR_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Event Log (PR_1000373796)** — Selecting "Save", within the IP Configuration screen of the Menu causes unnecessary Event Log messages.
- **sFlow/Flow-Control (PR_1000375851)** — To protect performance if Flow-Control is enabled on any one or more ports , egress sFlow sampling will be disabled on all ports and a CLI/Event Log message will be generated.
- **VLAN/CLI (PR_1000368900)** — VLAN names over 12 characters in length cause the output from the command "`show ip route`" to be displayed incorrectly.

Release K.11.65

The following problems were resolved in release K.11.65 (not a general release)

- **Alarms/Log (PR_1000371908)** — The ambient temperature measured by the 5406zl chassis is 4 degrees C too high, causing the generation of false high temperature alarms.
- **CLI (PR_1000377318)** — The output from the CLI command, 'show dhcp-relay' is truncated.
- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Menu/Counters (PR_1000370619)** — The Menu Interface does not reflect changes to SNMP OIDs for "IP Mgmt - Tx/Rx" counters; the counter always reads "0."
- **Syslog (PR_1000379802)** — Forwarding of event log message to a configured syslog server is not disabled when a specific event log message has been disabled via the MIB.
- **VRRP (PR_1000380627)** — VRRP packets are received on a non-VRRP VLAN causing excessive event log/syslog messages.

Release K.11.66

The following problems were resolved in release K.11.66 (not a general release)

- **CLI (PR_1000379455)** — The output from some CLI "show" commands produces incorrectly formatted output on the screen.
- **CLI (PR_1000309983)** — Using the "show tech" command immediately after boot and before the modules have initialized causes the command to fail, and leaves the user in an unsupported CLI state.
- **CLI (PR_1000364628)** — The command output from "show ip rip peer" yields an improperly formatted peer IP address.
- **Meshing (PR_1000386393)** — A 5412zl switch may crash with a bus error, when 4 Port CX4 module (J8708A) in Slot L is configured for Meshing. The crash message is similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x08af5298 HW Addr=0x4b5a697c IP=0x00372ed8
Task='mLdBalCtrl' Task 0 fp: 0x00000018
```

- **sFlow (PR_1000378885)** — The sFlow samplePool for trunks is sometimes unchanged between samples. This may cause inaccurate spikes in traffic monitoring applications that measure the utilization on trunk ports.

- **Web/RADIUS (PR_1000368520)** — Web Authentication doesn't authenticate clients due to a failure to send RADIUS requests to the configured server.
- **WebUI (PR_1000371598)** — Unable to Access Stack Members through Commander WebUI. Use of the WebUI "stack access" drop-down list on the stacking commander returns a "Page not found" error.

Release K.11.67

The following problems were resolved in release K.11.67 (not a general release)

- **MSTP (PR_1000385573)** — MSTP instability when root switch priority is changed. This causes other switches with better priority to assert themselves as root, thus causing a root war to occur.

Release K.11.68

Software never released.

- **CLI/LLDP (PR_1000377191)** — Output from the CLI command, "show lldp info remote-device <port>" shows a blank field for the chassis ID.
- **Crash (PR_1000390591)** — Software exception at sflow.c:3903 after re-starting sflow sampling. Switch may crash with a message similar to:

```
Software exception at sflow.c:3903 -- in 'mSnmpEvt',
task ID = 0x8248e90-> ASSERT: failed
```

- **DHCP (PR_1000386886)** — DHCP-relay uses an inconsistent address when the VLAN is multinetted. This fix forces the lowest IP address to be used for DHCP.
- **Enhancement (PR_1000388709)** — SFlow does not accommodate bursty traffic.
- **ROM update (PR_1000390486)** — ROM update to version K.11.03, required to support the upcoming K.12 software update.
- **Trunking (PR_1000238829)** — Trunks numbered trk10 and greater cause the output from the CLI command "show span" output to be misaligned.

Release K.11.69

The following problems were resolved in release K.11.69

- **Routing (PR_1000392086)** — The switch learns a bogus MAC address when the next hop address is unknown, causing the switch to stop forwarding traffic.

Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0*x* code branch with no intervening releases.

Release K.12.01

The following problems were resolved in release K.12.01

- **ACL (PR_1000393287)** — When the same ACL is applied (in or out) to more than 2 VLANs it does not get applied to the third VLAN or higher.
- **ACL (PR_1000389442)** — Numbering restrictions are not enforced at the CLI; ACLs numbered 200 or higher are considered valid. This fix enforces ACL numbering restrictions and converts existing ACLs numbered 200 or higher into named ACLs. If an invalid name of form XXX is found, it will be converted to "invalidXXX".

  Note:

  If you have ACLs configured with numbers greater than or equal to 200, you need to reconfigure those ACLs with either a valid name or valid number prior to loading K.12.01 software, or it will be tagged as invalid. For example, if you have an ACL called 222 and it is applied to a vlan, the K.12.01 script will convert the 222 ACL to "invalid222" and apply it to the vlan.

- **CLI (PR_1000332352)** — The output of a **show int brief** command should show the negotiated flow control status rather than the flow control configuration setting.
- **Crash (PR_1000385237)** — Applying an access control list with more than 105 entries to a VLAN interface causes the switch to crash with a message similar to:

  ```
  Software exception at enDecode.c:54 -- in 'mSess1',
  task ID = 0x8e7da60 -> out of memory!
  ```

- **Crash (PR_1000392105)** — Specific actions in the port status screen of the menu interface may trigger a crash. Scrolling down to the ports on a module in slot L and pressing [enter] may cause the switch to crash with a message similar to:

  ```
  Software exception at exception.c:424 -- in 'mSess1',
  task ID = 0x8dd1ab0 -> Memory system error at 0x881a480 - memPartFree
  ```

- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out", the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR_1000373226)** — Support was added for the ProCurve 100-FX SFP-LC Transceiver (J9054B).
- **Enhancement (PR_1000376626)** — Enhance CLI **qos dscp-map help** and **show dscp-map** text to warn the user that inbound classification based on DSCP codepoints only occurs if **qos type-of-service diff-services** is also configured.
- **Event Log (PR_1000330310)** — Failed attempts to communicate with an unknown module type fill the event log message buffer.
- **Routing (PR_1000359162)** — When the user configures a static route that overlaps with a local subnet configured on the switch, the router will not respond to packets destined for its own IP address. The packets for its own IP address will be routed using the configured static route.
- **OSPF (PR_1000374003)** — The switch assigns itself a router-id of the neighbor router's in a virtual link.

  Note:

  Existing OSPF virtual link configurations may be lost with the update to K.12.01. Either save the K.11 configuration and reload it once the switch is running K.12, or plan to reconfigure any virtual links at the CLI after booting into the K.12.01 software.

- **SNMP (PR_1000392847)** — RMON alarms that monitor port-specific OIDs are lost if the switch is rebooted.

Release K.12.02

The following problems were resolved in release K.12.02

- **Crash (PR_1000398746)** — The switch may crash with the task "swInitTask". This could result in repeated crashes until the switch configuration is cleared.
- **Crash/Traffic Monitoring (PR_1000396662)** — When Traffic Monitoring is enabled on the switch by a network management station (such as PCM) the switch may crash with a message similar to:

```
Data Bus Error: Addr=0x704a613c Data=0xffffffff flags=0x10000750,
IP=0x4012fa80 Task='tSvcWorkQ' TaskID=0x44b42ad0 cpsr=0x80000013
```

- **Crash (PR_1000392863)** — Switch may crash when **setmib tcpConnState** is used, with a message similar to:

  ```
  NMI event SW:IP=0x0079f4a0 MSR:0x00029210 LR:0x006dca60
  Task='eTelnetd' Task ID=0x8a7cbb0 cr: 0x20000042 sp:0x08a7c870
  ```

- **Daylight savings (PR_1000364740)** — Due to the passage of the Energy Policy Act of 2005, Pub. L. no. 109-58, 119 Stat 594 (2005), starting in March 2007 daylight time in the United States will begin on the second Sunday in March and end on the first Sunday in November.

- **DHCP (PR_1000397753)** — A unicast DHCP request that has already been relayed by another router is sometimes dropped.

- **Hang (PR_1000397964)** — The switch appears to hang where all routing stops, the switch cannot ping anything, even addresses configured locally.

- **Proxy-ARP (PR_1000393571)** — Proxy-ARP sends responses to gratuitous ARPs.

- **Remote Mirroring/Trunking (PR_1000397196)** — Remote mirroring configured on a trunk does not restart after the switch is rebooted. Workaround: after a switch reboot, reconfigure the trunk remote as a mirroring source.

- **RIP (PR_1000393366)** — The switch does not process RIP (v2) responses containing subnets with a classful subnet mask, when the receiving RIP switch has a connected VLSM network defined that would fall within that classful range.

Release K.12.03

The following problems were resolved in release K.12.03 (not a general release)

- **CLI (PR_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.

- **Crash (PR_1000399448)** — Changes to traffic monitoring settings may trigger the switch to crash with a message similar to:

  ```
  Software exception at ease_ctrl.c:575 -- in 'mEaseCtrl',
  task ID = 0x8347161
  ```

- **Crash (PR_1000401664)** — Use of the CLI command **dir** with a very large path name may cause the switch to crash with a message similar to:

  ```
  PC Data Storage (Bus Error) exception vector 0x300:
  Stack Frame=0x08e54928 HW Addr=0x00b3eefc IP=0x0018a740
  Task='mSess2' Task ID=00 fp: 0x00000000 sp:
  ```

- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.

- **Enhancement (PR_1000398393)** — For the **interface *<port-list>* speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.
- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports..

Release K.12.04

Software never released.

- **ACL (PR_1000402901)** — The ACL resequencing feature may discard some ACEs in a random fashion.
- **CLI (PR_1000403104)** — Executing the **erase startup-configuration** command and rebooting does not clean up the RMON 'alarm' table.
- **Crash (PR_1000405465)** — Use of dynamically assigned ACLs may cause the switch to reboot with the following error:

  ```
  Software exception at aclBttfMUtils.c:1208 -- in 'midmCtrl',
  task ID = 0x85f6a60 -> internal error
  ```

- **Enhancement MSTP (PR_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution.

Note

The updated standard provides auto-edge-port operation for MSTP, and supports the automatic detection of edge ports. The port will look for BPDUs for 3 seconds; if there are none, it begins forwarding packets. For more information on selected configuration options and updated MSTP port parameters, see "Release K.12.04 Enhancements" on page 33.

- **Remote Mirroring/SNMP (PR_1000395595)** — Removing a VLAN via SNMP does not remove the related ACL relationship to that VLAN.
- **sFlow (PR_1000408145)** — sFlow samples for routed packets do not occur bidirectionally; inbound packets are dropped and only outbound packets are sampled.
- **Traceroute (PR_1000379199)** — The reported **traceroute** time is inaccurate; it is one decimal place off.

Release K.12.05

The following problems were resolved in release K.12.05.

- **BootROM (PR_1000402707)** — BootROM does not update to latest version when updating code to primary flash.
- **CLI (PR_1000309998)** — Management module is incorrectly displayed as J8627A rather than the correct J8726A product number in response to the **show modules** command.
- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. For more information, see "Release K.12.05 Enhancements" on page 36.
- **Menu (PR_1000392862)** — The menu will allow invalid values (greater than 720 sec) to be entered for the SNTP poll interval.

Release K.12.06

Software never released.

- **Enhancement (PR_1000308332)** — Passwords (hashed) are saved to the configuration file. For more information, see "Release K.12.06 Enhancements" on page 43.

Release K.12.07

The following problems were resolved in release K.12.07.

- **Config (PR_1000405639)** — Various characters in configuration file names (including dash, ampersand, plus, and spaces within quotes) result in truncated names after reboot. This is not just a display issue; the command **erase config <*filename*>** does not remove a file containing the problem characters.
- **Config (PR_1000410790)** — Errors are returned when applying the **interface <*port-list*> speed-duplex auto-10-100** command to interfaces 45 through 48 on a 3500yl-48G-PWR switch.
- **Crash (PR_1000410758)** — When the **interface <*port-list*> speed-duplex auto-10-100** command is issued on a range of ports, the switch may crash with a message similar to:

  ```
  NMI event HW:IP=0x0083f224 MSR:0x00029210 LR:0x0033c3c4
  Task='tDevPollRx' Task ID=0x9137e50 cr: 0x20000022 sp:0x09137d78
  xer:0x20000000
  ```

- **RIP (PR_1000377789)** — RIP restrict filters are not working upon reboot.
- **RMON (PR_1000410885)** — RMON alarms/thresholds set via SNMP are cleared after reboot.

Release K.12.08

Software never released.

- **Enhancement (PR_1000413764)** — Increase the size of the sysLocation and sysContact entries from 48 to 255 characters. For more information, see "Release K.12.08 Enhancements" on page 57.

Release K.12.09

The following problem was resolved in release K.12.09 (Not a general release).

- **Crash (PR_1000385844)** — With sFlow sampling enabled, the switch may crash with a message similar to:

```
Software exception at ngDmaTx.c:729 -- in 'tDevPollTx',
task ID = 0x4305bba8 -> HW DMA DRIVER unable to transmit anymore
```

Release K.12.10

The following problems were resolved in release K.12.10.

- **ARP (PR_1000414347)** — ARP table address learning is slow; once the switch has its ARP table cleared, the clients will be unable to communicate for approximately 30 seconds.
- **Config (PR_1000416508)** — Cannot create alternate startup-config file. Although **show config files** shows an available slot, the switch does not allow copying from an existing config file to create a new config file in the vacant slot.
- **Crash (PR_1000421322)** — Following execution of config-related CLI commands (such as **show running-config** or **show tech**) or when PCM attempts to retrieve the configuration file using TFTP from a switch having a large configuration file, the switch may crash with a message similar to:

```
Software exception at exception.c:373 -- in 'tTftpDmn',
task ID = 0x11cfaa8 -> Memory system error at 0x1175550 - memPartFree
```

  The following related crash message may also be addressed with this fix:

```
PPC Bus Error exception vector 0x300: Stack-frame=0x016778b0
HW Addr=0x667c4c88 IP=0x004dbc88 Task='eChassMgr'
Task ID=0x1677dd8 fp: 0x667c4c88 sp:0x01677970 lrecpgyp
```

- **Enhancement (PR_1000419653)** — The **show vlan** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged/forbidden) for each port. For more information, see "Release K.12.10 Enhancements" on page 58.

- **SNMP (PR_1000374893)** — When retrieving the switch serial number via SNMP, the management module serial number is returned instead of the chassis serial number.
- **SNMP (PR_1000422129)** — HP Fault Finder doesn't send the interface index with the SNMP trap, even though it is listed in the system log.

Release K.12.11

Software never released.

Release K.12.12

The following problems were resolved in release K.12.12 (Not a general release).

- **Crash (PR_1000420709)** — Entering a backslash at the CLI may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x08e66508 HW Addr=0x00b4f2ac IP=0x0018a864
Task='mSess1' Task ID=0x8e67170  fp: 0x3be00000 sp:
```

- **Link LED (PR_1000425143)** — The Small Form-factor Pluggable (SFP) link LED does not work when SFP is hot-swapped into the switch.

Release K.12.13

Software never released.

Release K.12.14

The following problems were resolved in release K.12.14.

- **Authentication (PR_1000422933)** — Issue with local password authentication.
- **CLI/Clear button (PR_1000424194)** — The command **no password manager** deletes the password, but fails to delete the username. Similarly, pressing the clear button deletes the password but not the username.
- **SNMP (PR_1000423362)** — Setting username via SNMP (**hpSwitchAuthMIB**) deletes the password.

- **Hotswap (PR_1000422714)** — Hotswapping a module may result in a false module self-test failure. After hotswapping the module, the following messages may appear in the event log:

```
I 05/27/06 12:06:54 00076 ports: port B23 is now on-line
W 05/27/06 12:07:00 00564 ports: port B23 PD Invalid Signature indication
I 05/27/06 12:32:47 00068 chassis: Slot B Inserted
I 05/27/06 12:32:48 00068 chassis: Slot B Inserted
I 05/27/06 12:32:49 00068 chassis: Slot B Inserted
I 05/27/06 12:32:50 00067 chassis: Slot B Removed
I 05/27/06 12:32:50 00077 ports: port B23 is now off-line
W 05/27/06 12:33:11 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:34 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:57 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:19 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:42 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
I 05/27/06 12:34:44 00179 mgr: SME CONSOLE Session - MANAGER Mode
W 05/27/06 12:35:05 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:35:05 00274 chassis: Slot B self test failure or unsupported
```

  Multiple insertion messages may be included. The errors appear in the log as either a tombstone, HSL failure, or a loss of communications.

Release K.12.15

The following problems were resolved in release K.12.15.

- **Enhancement (PR_1000427592)** — This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.
- **Crash (PR_1000407238)** — Execution of the "show config" command when the startup configuration is different than the running configuration may cause the switch to crash with a message similar to:

```
Software exception at cli_mirror.c:6201 -- in 'mSess1', task ID =
0x8e53690 -> ASSERT: failed
```

- **SNMP (PR_1000406398)** — The URL embedded SNMP traps are not sent as SSL (https) when SSL is enabled, but are sent as plain-text (http) instead. This may result in the trap receiver (such as PCM) being unable to display the URL if SSL is enabled.
- **Enhancement (PR_1000428642)** — The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.
- **Crash (PR_1000427674)** — False positive memory testing may result in an ACL interrupt crash with an event log message similar to:

```
chassis: Slot L ACL Int status=0x2000000 25=0x80000005:
Task=tDevPollRx Task ID=0x4305d314 IP=0x40087044
```

- **Rate-Limiting (PR_1000420720)** — Rate limiting is broken beyond 9.5 Mbps. For any rate limit set to more than 9.5 Mbps, the actual rate drops to 1 Mbps.

Release K.12.16

The following problems were resolved in release K.12.16.

- **Crash (PR_1000415621)** — Removing a VLAN that has OSPF configured may cause the switch to crash with a message similar to:

```
NMI event HW:IP=0x0084a0a4 MSR:0x00029210 LR:0x00513ee4 Task='eRou-
teCtrl' Task ID=0x89658b0'
```

- **Crash (PR_1000428582)** — Typing non-alphanumeric characters at the CLI prompt may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack
Frame=0x08e36878 HW Addr=0x00b4f2ec IP=0x0018a974 Task='mSess1' Task
ID=0x0fp: 0x18020800 sp:
```

Release K.12.17

The following problems were resolved in release K.12.17.

- **STP (PR_1000420442)** — The switch erroneously allows configuration of spanning tree parameters on an interface that is a member of a trunk (link aggregation group), which creates an invalid configuration.
- **CLI (PR_1000429474)** — The "all" parameter is missing from the "password" command.
- **Radius (PR_1000432556)** — When DHCP snooping is enabled on the client VLAN, and the client is on a VLAN other than the default VLAN, the Framed-IP-Address attribute is not added to the RADIUS accounting packet as it should be.
- **Crash (PR_1000416453)** — Execution of the "show tech" command in an SSH session may cause the switch to crash with a message similar to:

```
Software exception - Assert in pmgr_util.c:1155 -- in 'mSess2', task
ID = 0x85adf60
```

Release K.12.18

The following problems were resolved in release K.12.18.

- **CLI (PR_1000419379)** — The “interface” command does not exist in the VLAN context, resulting in an inability to shift to the interface configuration context directly from the VLAN context.
- **Hang (PR_1000434809)** — The switch may hang, causing all the port LEDs to remain lit, and stop transmitting traffic.
- **Enhancement (PR_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method.
- **Crash (PR_1000436274)** — Typing a question mark ("?") at the "multi-line" input prompt (">") may cause the switch to crash. The crash occurs when the switch is trying to print the error message that states:

  ```
  Expansion help not available on multi-line input.
  ```

- **CLI (PR_1000433948)** — When command authorization is in use, the "show tech" command fails at the “show tech buffer” component, even when the permission list indicates that it should be allowed.
- **Enhancement (PR_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 3.2 years).
- **Enhancement (PR_1000438015)** — The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

Release K.12.19

The following problems were resolved in release K.12.19.

- **ACL (PR_1000432563)** — ACLs with the "permit" parameter on L4 ports and using operators ‘gt’/‘lt’/‘range’ do not function as expected. The ACL does not drop traffic with non-permitted L4 ports. Instead, all traffic with L4 ports is forwarded.
- **CLI (PR_1000438486**) — When using the "port-access mac-based" CLI command, the client MAC address is sent in lower case and as the username to the RADIUS server. This fix adds an option so that the MAC address is in uppercase when sent to the RADIUS server. This fix adds additional parameters to the CLI command to support this: "aaa port-access mac-based addr-format."

- **10-GbE Log (PR_1000424384)** — The switch is not checking for the presence of the J8694A ProCurve yl 10G X2-CX4 module early enough in the boot process, triggering a log message when the check is executed.

Release K.12.20

The following problems were resolved in release K.12.20 (Never released.)

Release K.12.21

The following problems were resolved in release K.12.21 (never released).

- **ARP Protection (PR_1000438129)** — ARP and ARP protection data may not display correctly following a CLI or SNMP status query.
- **Enhancement (PR_1000440049)** — Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic.
- **CLI (PR_1000342461)** — If a trunk is configured, output from the CLI command “show lldp info remote <port number>" reports incorrect information for the remote management address. This may result in a failure to discover or map devices connected to these trunks by management applications that use LLDP discovery (e.g. ProCurve Manager).
- **Enhancement (PR_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Crash (PR_1000434888)** — A switch module may crash with a message similar to:

```
ACL Int status=0x10000000 28=0x80002f3a: Task=tDevPollTx Task
ID=0x4305c504 IP=0x400693e8
```

- **Enhancement (PR_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections.
- **VRRP/Meshing (PR_1000435853)** — A MESHed link in the path between a VRRP Owner and VRRP Backup may lead to a situation where both VRRP routers remain in Master state for a VRID after that VRID fails over to the Backup and then the Owner comes back online.

- **Routing (PR_1000432449)** — If the switch is configured with both port security and routing, a physical port transition on the host may cause the switch to stop transmitting routed traffic to that host. Clearing the ARP cache resolves this problem until another port transition occurs.
- **RADIUS (PR_1000442879)** — If RADIUS (or TACACS+) keys are configured, and then the switch is updated to a software revision with the ability to save the security credentials in the configuration file (K.12.06 or later), the RADIUS keys are no longer shown in output from the "show run" or "show config" commands until the "include-credentials" command is issued.

Release K.12.22

The following problems were resolved in release K.12.22.

- **Enhancement (PR_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR_1000444415)** — OSPF Passive Interface support was added.
- **Crash (PR_1000442695)** — Pasting a VRRP configuration into the running configuration via a Telnet session may cause the switch to crash with a message similar to:

```
Software exception at vrrp_statemach.c:205 -- in 'mVrrpCtrl', task
ID = 0x8b154a0-> internal error
```

Release K.12.23

The following problems were resolved in release K.12.23.

- **Crash (PR_1000415534)** — Execution of the "lockout-mac" CLI command, may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x0ab9a738 HW Addr=0x00b3f104 IP=0x00801d2c Task='eDrvPoll'
Task ID=0xab9ad20 fp: 0x0f3808c0 sp
```

- **AAA/CLI (PR_1000445886)** — This changes the syntax of '**aaa authentication** <port-access | mac-based | web-based>' commands which were previously added in PR_1000438486.
- **CLI (PR_1000403478)** — Power over Ethernet (802.3af) CLI commands were removed from platforms that do not support PoE (such as the ProCurve 6200yl switch).
- **Broadcast-limit (PR_1000429594)** — The broadcast limit feature affects multicast traffic. This fix modifies the feature so that it only affects broadcast traffic.

- **MSTP (PR_1000439775)** — The switch generates a topology change when a port goes off-line. With MSTP enabled and all ports left at default (auto-edge-port), when a port transitions to offline, a TC will be generated, and the topology change counter increases.
- **Multicast (PR_1000436118)** — Multicast forwarding with IGMP is slow and causes an unacceptable delay in servicing.
- **Enhancement (PR_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP.
- **Crash (PR_1000444112)** — Downloading a configuration file to the switch may cause a crash with a message similar to:

  ```
  Software exception at cli_config_action.c:5479 -- in 'mftTask'
  ```

- **SNMP (PR_1000448463)** —The SNMP Engine ID Discovery process described in RFC 3414 is not working properly.

Release K.12.24

The following problems were resolved in release K.12.24.

- **Hang (PR_1000448429)** — A bank of ports may fail the self test, crash or stop functioning after several weeks of use. This failure may result in event log messages similar to those listed below.

  ```
  W 06/10/07 08:07:22 00374 chassis: Ports 25-48: Lost Communications detected
  - Heart Beat Lost

  I 06/10/07 08:07:22 00077 ports: port 31 is now off-line

  I 06/10/07 08:07:22 00077 ports: port 40 is now off-line

  I 06/10/07 08:07:29 00375 chassis: Ports 25-48 Downloading

  I 06/10/07 08:07:30 00376 chassis: Ports 25-48 Download Complete

  W 06/10/07 08:08:32 00374 chassis: Ports 25-48 Failed to boot-timeout
  (AGENT_FAILED)
  ```

Release K.12.25

The following problems were resolved in release K.12.25.

- **Config (PR_ 1000451779)** — Software update, TFTP restoration of the configuration or reloading the switch on software version K.12.22 may delete a Mini-GBIC VLAN port assignment.

Release K.12.26 through K.12.29

Software never built.

Release K.12.30

Software never released.

Release K.12.31

The following problems were resolved in release K.12.31.

- **Enhancement** — Support for the following ProCurve product was added.

  J9091A / J8715A (bundle) for the ProCurve switch 8212zl

Release K.12.32

Never released. The following problems were resolved in build K.12.32.

- **Enhancement** — Merged all of the K.12.24 and earlier software fixes and enhancements with the ProCurve switch 8212zl support.

Release K.12.33 through K.12.40

Software never built.

Release K.12.41 through K.12.42

Software never released.

Release K.12.43

The following problems were resolved in release K.12.43.

- **Enhancement** — Support for the following ProCurve products was added.

  J9051A ProCurve Wireless Edge Services zl Module

  J9052A ProCurve Redundant Wireless Edge Services zl Module

For more information, see "Support for the Wireless Edge Services zl Module" on page 18.

Release K.12.44

Not a general release.

- **Enhancement (PR_1000457691)** — This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see "Release K.12.44 Enhancements" on page 65.
- **Enhancement (PR_1000457868)** — Local Proxy ARP enhancement. For more information, see "Release K.12.44 Enhancements" on page 65.
- **Enhancement (PR_1000456271)** — PC attached to telephone. For more information, see "Release K.12.44 Enhancements" on page 65.

Release K.12.45

The following problems were resolved in build K.12.45. (Never Released.)

- **STP (PR_1000449365)** — ARP & MAC tables get out of sync after a spanning tree (MSTP or RSTP) re-convergence. An ARP entry fails to be associated to the port even though the MAC entry exists. This may result in an unexpected ping failure.
- **PIM (PR_1000450431)** — IP Multicast Routing PIM-DM Stops Forwarding Flows, and the event log reports:

  ```
  PIM: Failed alloc[ation] of HW Flow for flow <multicast address>
  ```

- **SSH (PR_1000453226)** — Configuration of SSH login to the manager mode (**aaa authentication ssh enable public-key** <enter>) triggers an error "Not legal combination of authentication methods", but it should be a valid command syntax.
- **Authentication (PR_1000454714)** — Concurrent 802.1X and MAC-authentication does not give the 802.1X value precedence. This fix gives 802.1X VLAN assignment precedence over MAC auth RADIUS VLAN assignment.
- **SNMP (PR_1000389902)** — The switch is not sending an "embedded URL" within the SNMP trap for an FFI event to the PCM server monitoring traps. The embedded URL, if sent, would allow someone looking at the log event on the PCM server to simply click on the URL and be immediately connected to the switch.
- **CLI (PR_1000418891)** — The Connection Rate Filter *ignore* list does not display properly in the output for the show run command; the IP address and mask are incorrectly printed on the next line.

- **SNMP (PR_1000444744)** — An *snmp set* of hpicfDot1xPaePortauth or an *snmp set* hpicfDot1xPaePortSupp of an invalid value may cause the switch to crash with a message similar to the following:

  ```
  ASSERT at aaa8021x_dyn_reconfig.c.
  ```

- **SSH (PR_1000461002) —** Issue with authentication when SSH is configured.

Release K.12.46

The following problems were resolved in build K.12.46. (Never Released.)

- **Mirroring (PR_1000458287) —** Remote mirroring does not work in slots K or L of the 5412zl or 8212zl chassis.
- **Crash (PR_1000456340) —** Switch may crash with a message similar to:

  ```
  No message buffers: alloc_free.c:435.
  ```

  The trigger for this crash is unknown, though it is suspected to be related to sFlow.

- **Module Failure (PR_1000464335) —** Switches running K.12.31 - K.12.43 may experience a problem with modules failing to boot. The system log may report a message similar to the following:

  ```
  W 11/08/05 02:43:14 00374 chassis: Slot D Failed to
  boot-timeout-(AGENT_FAILED)
  I 11/08/05 02:43:19 00375 chassis: Slot D Downloading
  I 11/08/05 02:43:21 00376 chassis: Slot D Download Complete
  W 11/08/05 02:44:21 00274 chassis: Slot D self test failure or
  unsupported module
  ```

- **Telnet hang (PR_1000457765) —** If **Ctrl+S** is typed and then the Telnet window is closed, the Telnet session may become unresponsive, and fail to reset by the **kill** command issued at the console prompt. This may require the switch to be reloaded to become active again.

Release K.12.47

The following problems were resolved in release K.12.47.

- **Enhancement Removed (PR_1000468258) —** The PC attached to IP telephone enhancement was removed. For more information, see "Release K.12.47 Enhancements" on page 66.

Release K.12.48

The following problems were resolved in release K.12.48.

- **Enhancement Removed (PR_1000470136) —** Removal of the enhancement that allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. The initial implementation of this enhancement did not allow smooth migration of pre-existing MSTP configurations. For more information, see "Release K.12.48 Enhancements" on page 66.
- **CLI (PR_1000417447) —** Some of the instrumentation monitoring parameters (e.g. arp reply monitoring) are not functioning.

Release K.12.49

The following problems were resolved in build K.12.49. (Never Released.)

- **Enhancement (PR_10004570598) —** An improved version of the MSTP-VLAN mapping enhancement referenced in PR_1000457691 was added. This enhancement allows the mapping of all theoretically available VLAN IDs (1-4094) to an MSTP instance, even if some of the VLANs are not currently configured on the switch. For more information, see "Release K.12.44 Enhancements" on page 65.
- **MSTP (1000457691) —** MSTP instances are removed from the configuration after an update and reload into software version K.12.47.
- **Enhancement (PR_1000471015) —** Reintroduction of the feature referenced in PR_1000456271, that will allow a PC to connect with its RADIUS-assigned VLAN after an attached IP phone has authenticated on the authenticating port. For more information, see "Release K.12.44 Enhancements" on page 65.

Release K.12.50

The following problems were resolved in build K.12.50. (Never Released.)

- **CLI (PR_1000464787) —** Minor modifications to internal switch functions.

Release K.12.51

The following problems were resolved in release K.12.51.

- **Trunking (PR_1000461440) —** When dynamic ARP protection and DHCP snooping are configured, a trunk's *trust* status cannot be configured from the appropriate interface configuration context.

- **Routing (PR_1000424308) —** A static route that points to a deleted VLAN may cause other routing table errors.
- **CLI (PR_1000473468) —** Removing a VLAN range from an MSTP instance (e.g., no spanning-tree instance 2 vlan 10-20) fails to delete the VLANs. Listing individually the VLANs desired for deletion will correctly remove the VLANs.

Release K.12.52

The following problems were resolved in release K.12.52 (never released).

- **Enhancement (PR_1000458484) —** This enhancement allows the user to set a maximum frame size for jumbo frames at the global level. For more information, see "Release K.12.52 Enhancements" on page 67.
- **Enhancement (PR_1000461576) —** This enhancement introduces PVST Protection and Filtering. For more information, see "Release K.12.52 Enhancements" on page 67.
- **Enhancement (PR_1000462841) —** This enhancement changes the re-authentication process to allow an authenticated client to remain authenticated during re-authentication. For more information, see "Release K.12.52 Enhancements" on page 67.
- **Enhancement (PR_1000462104) —** This enhancement allows the configuration of modules not currently inserted in the switch. For more information, see "Release K.12.52 Enhancements" on page 67.
- **Enhancement (PR_1000462847) —** This enhancement allows the configuration of transceivers not currently inserted in the switch. For more information, see "Release K.12.52 Enhancements" on page 67.

Release K.12.53

The following problems were resolved in release K.12.53.

- **Crash (PR_1000472846) —** Rebooting the switch with an active Telnet session and while remote mirroring is in use may cause the switch to crash with a message similar to the following. There may also be other, unknown triggers that cause this crash.

  ```
  0x4001bf18 in fatal_exception (file=0x400a8b8c "ngDmaRx.c", line=1413,
  errorcode=256, str=0x400a8b7c "ASSERT: failed."
  ```

- **xSTP (PR_1000715227) —** When there is no module and transceiver inserted in the target slot, attempts to set up a unique path cost on the transceiver port results in an `"invalid input"` error.

Release K.12.54

The following problems were resolved in release K.12.54.

- **Connection Rate Filter (PR_1000440871) —** Some types of traffic could result in connection rate filtering (CRF) that blocks the switch management IP address.
- **Connection Rate Filter (PR_1000716601) —** Connection Rate Filtering does not remove throttled entries when filtering is disabled. The throttled host remains permanently blocked.
- **TFTP (PR_1000427390) —** When the configuration of a 6200yl switch is copied to a TFTP server, the config shows a line with the following description: `module 1 type JFIXME`. If that line is removed from the config and then the config is transferred back to the switch, the transfer will fail with the switch reporting, "`corrupted config.`" This fix results in the fixed switch ports being described as: `module 1 type J8992A`.
- **Crash (PR_1000716461) —** Loading a configuration file that uses up all the ACL resources may cause the switch to crash with a message similar to:

  ```
  NMI event SW: IP=0x007c755c MSR: 0x00029210 LR: 0x007c7544
  Task='mftTask' Task ID=0x8a60920cr: 0x24024442 sp: 0x08a5f850 xer:
  0x20000000
  ```

- **Link Speed (PR_1000432419) —** Ports 1-24 on the ProCurve 3500yl-24G-PWR and ports 25-48 on the ProCurve 3500yl-48G-PWR switches may link at 10/100 speeds rather than the gigabit speed they support.
- **TFTP (PR_1000419582) —** The switch CLI counter displays the wrong size of the file being transferred when uploading from switch flash to TFTP server. The file that is actually transferred is the correct size. This CLI display is in error.
- **PIM (PR_1000306675) —** The switch CLI does not allow the commands to remove PIM and IP multicast routing after the removal of a premium license from ProCurve 5400zl or 3500yl Series switches.
- **CLI (PR_1000447529) —** The CLI output of the command **show rate-limit all** is corrupted.
- **Manufacturing (PR_1000740632) —** Upon reload, the manufacturing information is zeroed out.

Release K.12.55

The following problems were resolved in release K.12.55 (never released).

- **DARPP (PR_1000736402) —** The last port on the switch will not be initialized with Dynamic ARP Protection (DARPP) characteristics if the last two ports are DARPP configured. For example, if the switch has 24 ports and ports 23 and 24 have DARPP characteristics, the DARPP characteristics for port 24 will not be initialized. The last port will be initialized in all other cases.
- **CLI (PR_1000340826) —** The CLI output from a **show interface** command truncates counters that have large values.
- **CLI (PR_1000742974) —** The CLI had some initial limitations within the interface context for configuration of uninserted modules and transceivers. This fix addresses the interface context for spanning-tree, aaa port-access, DHCP snooping, loop protection, and a number of other features.

Release K.12.56

The following problems were resolved in release K.12.56.

- **Enhancement (PR_1000464170) —** This feature provides support for adding the LLDP VLAN Name TLV to LLDP advertisements generated by ProCurve switches. For more information, see "Release K.12.56 Enhancements" on page 67.

Release K.12.57

The following problems were resolved in release K.12.57.

- **Enhancement (PR_1000713394) —** Adjustable IGMP Querier interval.
- **Daylight Savings Time (PR_1000467724) —** This change corrects the schedule for Western Europe Time Zone: DST to start the last Sunday in March and DST to end the last Sunday in October.
- **SSH/SCP (PR_1000742969) —** The following issues with using SSH/SCP were fixed.

  1) In **show ip ssh**, sessions 3 & 4 may display "`console`" instead of "`inactive`," when those sessions are not in use.

  2) The switch does not send an appropriate exit-status message to the client. This corrects the symptom that occurs in some applications, which reports a message similar to:

  ```
  Fatal error: Server unexpectedly closed connection.
  ```

3) The SSH client application does not get a command prompt (or equivalent) back from the switch until the OS is verified and burned to flash.

4) The **show flash** command incorrectly shows an OS image present in flash before the OS has completely copied to flash.

- **Routing (PR_1000744325) —** When a PC is using the switch as its default gateway, and that switch is set with a default route to another device on the same VLAN, duplication of packets may occur. Symptoms may include seeing TCP packets out of order due to retransmission.

- **ACL (PR_1000751460) —** Manipulating ACEs on a switch with the ACL applied may result in a switch hang or crash with a message similar to the following.

  ```
  SubSystem 0 went down: 11/05/07 10:16:07 Software exception at
  ipAccessHandle.c:161 -- in 'mSess2', task ID = 0x876ffa0 -> internal
  error
  ```

- **PIM (PR_1000745983) —** PIM-Sparse Mode causes packet drops in protocols that use a destination IP multicast address such as VRRP/OSPF hello packets, and RIPv2 advertisements.

- **802.1X (PR_1000741874) —** Entering invalid 802.1X credentials (triggering failed authentication) and then trying again with valid credentials may cause the switch may crash with a message similar to the following. Symptoms and triggers for this problem may vary.

  ```
  Software exception at aaa8021x_util.c:2290 -- in 'm8021xCtrl', task ID
  = 0x85db0 -> ASSERT: failed.
  ```

- **Manufacturing (PR_1000752302) —** The ESP module does not initialize in the zl switches during the manufacturing process.

- **Connection Rate Filter (PR_1000751758) —** The “low sensitivity” connection rate filter setting was too sensitive. This fix improved the filter accuracy for "low sensitivity" levels.

- **Config (PR_1000749046) —** The running and startup configurations that are copied via TFTP do not match the output from the **show run** or **show config** output for the ProCurve 3500yl and 6200yl switches.

- **Hang (PR_1000752561) —** Multiple SNMP *get* requests over a 10-GbE link leave the switch in a problematic state. In this state one or more of the following may occur.

  1) Some CLI commands may not produce the expected output, or the output will be truncated.

  2) The **reload** command may not properly respond to some parameters.

  3) New Telnet sessions may not be allowed to form.

  4) DHCP requests may be lost by the switch.

  5) The system may need to be reloaded before the issues clear.

Release K.13.02

The following problems were resolved in release K.13.02.

- **Enhancement (PR_1000458124) —** VRRP Preemptive Delay Timer. For more information, see "Release K.13.02 Enhancements" on page 71.
- **CLI (PR_1000307590) —** Tab-help error in the spanning-tree instance `<instance number> vlan <vlan number>` command context.
- **CLI (PR_1000330684) —** Help text in the spanning-tree `<port_id>` context was updated.
- **CLI (PR_1000742426) —** The CLI command **copy usb pub-key-file** doesn't provide all the appropriate options.
- **Event Log (PR_1000751191) —** There is a misspelled event log message: `chassis: Insufficient power supplies`.
- **Event Log (PR_1000757272) —** There may be corruption in PIM log messages.
- **DHCP Snooping (PR_1000757935) —** DHCP Snooping may miss some packets in certain situations.
- **Mirroring (PR_1000758793) —** When a mirror ACL is applied with multiple destinations, only one of those destinations work properly. Beginning with K.13.02 software, there is only one ACL mirror destination supported.
- **Mirroring (PR_1000758803) —** Applying a second mirror ACL using the same access group number adds a conflicting mirror session rather than replacing the existing entry.
- **Mirroring (PR_1000758810) —** When an ACL used as a mirror ACL is modified, the mirror does not get updated.
- **Mirroring (PR_1000758814) —** Applying a mirror ACL may overwrite a standard mirror session (of the same number) rather than triggering an error stating that the mirror session is already in use.
- **Counters (PR_1000758834) —** SFLOW counter-polling samples may be infrequent or they may stop until the switch is rebooted.
- **IGMP (PR_1000739226) —** Some hosts or downstream devices may experience a disruption in multicast data due to the loss of IGMPv3 reports.
- **VRRP (PR_1000401050) —** Turning on IP multicast routing without enabling PIM may cause VRRP starvation.
- **SCP (PR_1000760416) —** Software transferred through SCP upload becomes corrupted; the image is successfully copied via SCP, but when the switch processes the image in copying to flash, the write never completes.

- **CLI (PR_1000455370) —** Commands that display portmaps may yield corrupted output. For example, a single port may be displayed as a port range.
- **RIP (PR_1000751858) —** Some static routes may not be correctly distributed by RIPv1 or RIPv2.
- **PIM (PR_1000714322) —** A new multicast stream may not get forwarded by the switch.
- **Crash (PR_1000759046) —** Using the "\" character with or without other character combinations may cause the switch to crash with a message similar to the following. There may also be different crash messages resulting from the same problem.

```
Software exception at parser.c:2653 — in 'mSess1', task ID =
0x898e6a0-> ASSERT:  failed
```

- **PIM (PR_1000749627) —** A switch with PIM-SM may send a prune to the RP when none is required.
- **Web Management (PR_1000472572) —** The Web Management Interface does not properly allow configuration of port monitoring/mirroring.

Addendum to Release K.13.02:

- **ACL (PR_1000714376/1000760152) —** Attempts to apply an access group to a range of ports will fail after the initial configuration unless a write mem and reload are done in between configuration statements.

Release K.13.03

The following problems were resolved in release K.13.03.

- **Enhancement (PR_1000400991) —** The 802.1X Controlled Directions feature now functions independently of the STP configuration. For more information, see “Release K.13.03 Enhancements” on page 75.
- **IPv6 (PR_1000768670) —** When virus throttling is configured on a port that belongs to an IPv6 enabled VLAN, some IPv6 all nodes (ff02::1) multicast traffic may be dropped.
- **Mirroring (PR_1000768655) —** After a mirror ACL has been modified, some ACL commands that follow may result in an unresponsive CLI session.
- **IDM ACL (PR_1000768727) —** An IDM ACL that uses the syntax, *destination ip "any"* will result in a parsing error, the ACL will not be applied, and the client authentication will fail. Workaround: Instead of the term "any," use “0.0.0.0/0.”
- **VRRP PDT (PR_1000756475) —** If the VRRP preemptive delay timer (PDT) is configured, the virtual router mode (Owner or Backup) cannot be changed unless the PDT configuration is removed.

- **Crash (PR_1000763409) —** When entering and deleting ACLs, the switch may crash with a message similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300: Stack
  Frame=0x087a1ba8 HW Addr=0x1f89d420 IP=0x005e62e0 Task='mSess2' Task
  ID=0x87a3cd0.fp: 0x00000005 sp:0x087a1c68 lr:0x005e6340.
  ```

- **DHCP Relay (PR_1000751623) —** If the IP address on a VLAN interface is changed, any previously configured IP Helper address stops working.

Release K.13.04

The following problems were resolved in release K.13.04 (never released).

- **Self-test/Module (PR_0000000510) —** Inserting a module into a Switch 8212zl may result in the module failing to initialize with one of the following error messages:

  ```
  Self test failure or unsupported module, or
  chassis: Insufficient power supplies to power Slot <x>
  ```

- **Port/Config (PR_1000772652) —** A switch running software version K.12.52 or later only accepts the speed-duplex settings 'auto' or '1000-full' for the dual-personality ports when the configuration file is transferred to the switch via tftp, scp or sftp. Other port settings that should be valid cause the file transfer to abort with a "`corrupted download file`" error.

- **Port/Config (PR_1000778004) —** The switch accepts, via file transfer, a config file with invalid speed/duplex settings on dual-personality ports. Additionally, the 100-FX port settings do not survive a reboot.

- **TFTP/ACL (PR_1000771560) —** The **copy tftp command-file** command rejects ACL remarks if they do not contain the keywords **permit** or **deny**.

- **SNMPv3/Config (PR_1000777656) —** The SNMPv3 configuration is removed from the switch's config file after an update from K.12.xx to K.13.03.

- **SSH/Config (PR_1000777873) —** SSH becomes disabled (an 'ip ssh' entry in the config file becomes a 'no ip ssh' entry in the config file) after an update from K.12.xx to K.13.03.

  In K.12.xx software, SSH is disabled by default. In K.13.xx software, SSH is enabled by default. Since default values are not displayed in the output of **show run** or **show config** commands, this results in a difference in the configuration file output of SSH from K.12.xx to K.13.xx.

- **TFTP/Config (PR_0000000922) —** TFTP client configuration becomes disabled ('`no tftp client`') after an update from K.12.xx to K.13.03.

- **'show tech all/route'/Hang (PR_1000779458) —** When the **show tech all** or **show tech route** commands are used within a remote management session, the switch may hang.

- **Enhancement (PR_ 0000000081) —** The CLI **clear module** command allows you to remove module configuration information from the configuration file. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000082) —** The CLI **track interface** command allows you to configure tracking for a port or list of ports, or a trunk or list of trunks. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000084) —** DHCP Option 66 provides a way to automatically download and initially boot from a configuration that is different from the factory-shipped configuration. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000085) —** The DHCP relay address configuration enhancement provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000086) —** This enhancement allows rate-limiting of inbound broadcast and multicast traffic on the switch. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000087) —** This enhancement enables a Telnet client to use the hostname in command input. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000089) —** The CLI **show modules** command displays additional component information for system support modules and mini-GBICS. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000101) —** This enhancement adds a **vrrp** option to the **debug** command. For more information, see "Release K.13.04 Enhancements" on page 76.
- **Enhancement (PR_ 0000000420) —** This enhancement provides the **show tech** option for customizing **copy tftp** output. For more information, see "Release K.13.04 Enhancements" on page 76.
- **'show tech' (PR_0000000635) —** The **show tech** CLI command will cause an "`Invalid input: power`" error message to be displayed in the ProCurve Switch 6200yl-24G-mGBIC.
- **CLI (PR_0000000358) —** The output from the **show modules** CLI command shows the module serial number as being all zeros, or fails to show any output at all for that value.
- **CLI/sFlow (PR_0000000360) —** The switch administrator is unable to configure sFlow for ports on modules that have not been inserted yet into the switch.

- **CLI (PR_0000000476) —** Various CLI parameters are rejected by the switch as invalid when the administrator is trying to configure ports of transceivers/modules that have not yet been inserted into the switch. Affected commands include **ip source-binding**; **interface** <x> **power**; **interface** <x> **unknown-vlans block**; output from the command, **show vlans**; **interface** <x> **monitor**; and **mirror** <x> **port** <x>.

Release K.13.05

The following problems were resolved in release K.13.05 (not a public release).

- **Link/Config (PR_1000771549) —** On a ProCurve 3500yl Series Switch, a link will not come up after configuring the port mode from MDI to AUTOMDIX (on one side of the link).
- **Static Route/Config (PR_1000785177) —** The VLAN ID for the static route configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **SNMP/Config (PR_1000780506) —** The TFTP transfer of a config file to the switch will fail if the config file contains the command **snmp-server trap-source** `<xx.xx.xx.xx>`.
- **Crash (PR_0000000971) —** Following MAC authentication of a number of users that have a RADIUS ACL, priority, and a number of other parameters applied, the switch may crash with a message similar to:

  ```
  NMI event SW:IP=0x00334dc8 MSR:0x00029210 LR:0x00334e3c Task='mWeb-
  Auth' Task ID=0x8413770. cr: 0x20004044 sp:0x08413260 xer:0x20000000
  ```

- **Crash (PR_1000783817) —** The switch may crash with a message similar to:

  ```
  NMI event SW:IP=0x0010770c MSR:0x00029210 LR:0x00107714

  Task='midmCtrl' Task ID=0x8417f00  cr: 0x24004084 sp:0x08417c08
  xer:0x00000000
  ```

- **SNMP/Config (PR_1000786158) —** The TFTP transfer of a configuration file created on K.12.xx to a switch running K.13.03 will fail if the configuration file contains the command **snmp-server enable traps authentication**.
- **IPv6/Config (PR_1000781026) —** When a configuration file is transferred to the switch and the file contains a VLAN with the '`ipv6 mld`' statement, the switch alters the '`ipv6 mld`' statement to '`no ipv6 mld fastleave 1-A24,=1-Mesh,Trk1-Trk60,Dyn1-Dyn60`'.
- **SNTP/Config (PR_1000786156) —** The TFTP transfer of a configuration file created on K.12.xx to a switch running K.13.03 will fail if the configuration file contains the command **sntp server** `<x.x.x.x>`.
- **VLAN/Config (PR_1000782308) —** Updating from K.12.xx to K.13.03 may result in an incorrect port VLAN assignment.
- **Telnet-Server/Config (PR_0000000946) —** The TFTP transfer of a config file to the switch will fail if the config file contains the command **no telnet-server**.
- **Authorized-Manager/Config (PR_1000789930) —** The update from K.12.xx to K.13.03 does not translate the IP authorized-manager configuration properly.

- **UDLD (PR_0000001433) —** After the switch is rebooted, UDLD may continue to keep switch ports in a blocked state.
- **VLAN Mirroring/Config (PR_0000001240) —** The VLAN Mirroring configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **Bootup/Flash (PR_1000785118) —** During the write-to-flash process, the OS file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk for ProCurve 3500yl, 6200yl, 5400zl Series Switches.
- **Bootup/Flash (PR_1000785113) —** During the write-to-flash process, the configuration file may become truncated if the switch is interrupted (by crash or power outage, for example). This fix minimizes that risk for ProCurve 3500yl, 6200yl, 5400zl Series switches.

Release K.13.06

The following problems were resolved in release K.13.06 (not a public release).

- **Static Route/Config (PR_0000001471) —** Rebooting a switch running K.13.03 may cause the static route configuration to become corrupted.
- **OSPF (PR_1000385566) —** When jumbo frames are enabled on a VLAN configured for OSPF, the state stops at EXCHANGE and EXSTART.
- **UDLD (PR_0000001616 and PR_0000001638) —** After the switch is rebooted, UDLD may continue to keep ports in a blocked state, particularly if the port is in a static LACP trunk.
- **CLI (PR_0000001643) —** The **ip authorized-managers** CLI command does not allow the 10.0.0.0 IP address to be used.

Release K.13.07

The following problems were resolved in release K.13.07 (not a public release).

- **Loopback Interface (PR_1000793862) —** A ping or Telnet session to a loopback address may fail intermittently. A traceroute to the loopback address completes successfully. This may cause some protocol packets to fail to reach the loopback address.
- **Crash (PR_0000001689) —** A switch running software version K.13.04 or higher may crash during configuration of a trunk group from either the CLI or menu interface. Event log messages may be similar to the following.

```
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601
```

```
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601
W 03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications
detected - Heart Beat Lost
I 03/11/06 03:19:00 00375 chassis: Ports 25-48 Downloading
I 03/11/06 03:19:01 00376 chassis: Ports 25-48 Download Complete
I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
```

- **ARP Protect/Config (PR_0000001549) —** The VLAN ID range for the ARP protection configuration is changed from its original value after updating from K.12.xx to K.13.03.
- **Crash/Config Migration (PR_0000001607) —** If VRRP is configured on a switch and the switch is rolled back from K.13.xx to K.12.xx and then updated to K.13.xx again, the switch may get into a continuous crash/reboot state. The crash messages may be similar to the following.

  ```
  NMI event SW:IP=0x0015e960 MSR:0x00029210 LR:0x00229944
  Task='mSess1' Task ID=x86fe5f0  cr: 0x24022488 sp:0x086fd960
  xer:0x00000000

  NMI event SW:IP=0x0083670c MSR:0x00029210 LR:0x007c4e1c
  Task='mIpCtrl' Task ID0x8c0ed90  cr: 0x24004084 sp:0x08c0e4c0
  xer:0x20000000

  Software exception at vrrp_common_lib.c:279 -- in 'swInitTask',
  task ID = 0x917630
  ```

  The fix involves partially removing some of the VRRP configuration and then generating an Event Log message similar to:

  ```
  E 07/14/06 10:14:15 00227 mgr: Partial config deleted for
  subsystem=vrrp;see release notes.
  ```

Release K.13.08

The following problems were resolved in release K.13.08.

- **SNMP/Config (PR_0000001672) —** The **snmp-server** configuration may change during the migration from K.12.xx to K.13.03.
- **Web/MAC Authentication (PR_1000793226) —** Web or MAC authentication to the switch by a client that moves from one port to another may either fail or cause the switch to crash with a message similar to the following.

  ```
  Program exception vector - Task='mWebAuth' Task ID=0x83bc390
  ```

Release K.13.09

The following problems were resolved in release K.13.09.

- **Crash (PR_0000001689a) —** A switch running software version K.13.04 or higher may crash during configuration of broadcast rate limiting. Event log messages may be similar to the following.

```
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601
W 03/11/06 03:18:53 00374 chassis: Ports 25-48 Slave ROM Tombstone:
0x13000601W
03/11/06 03:18:53 00374 chassis: Ports 25-48: Lost Communications
detected - Heart Beat Lost I 03/11/06 03:19:00 00375 chassis: Ports
25-48 Dowloading
I03/11/0603:19:0100376chassis:Ports25-48DownloadComplete
I 03/11/06 03:19:15 00422 chassis: Ports 25-48 Ready
```

- **Web Authentication (PR_0000002047) —** Use of Web authentication with MS-CHAP-v2 to Microsoft IAS may cause the switch to crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'mWebAuth', task ID =
0x8438440 Memory System error at 0x7f56610 - memPartFree
```

- **MAC Authentication (PR_0000002075) —** A client that fails MAC authentication will be blocked by AAA rather than the port being moved, unblocked, into a configured Unauthenticated VLAN.

Release K.13.10

The following problems were resolved in release K.13.10 (never released).

- **VLAN/Config (PR_1000782308)** — Updating from K.12.xx to K.13.03 may result in an incorrect port VLAN assignment.
- **MAC Authentication (0000002318)** — Authenticated MAC Auth clients may intermittently get placed into the unauthenticated VLAN and never come on-line.
- **Port Security (PR_1000777162)** — When Port Security is configured for static MAC address learning, prolonged flooding of unicast traffic may occur under certain conditions.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from K.12.xx to K.13.xx.
- **Wrong Error Message/VRRP (0000000909)** — You may receive an "inconsistent value" error message when attempting to add (max+1) entity for VRRP to track. The correct error message should be "too many entries to track."

- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X-enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **RADIUS (0000001164)** — The switch drops RADIUS messages with EAP-packets larger than 1496 bytes.
- **Auto-TFTP/Config (PR_0000001410)** — The Auto-TFTP configuration is lost during the update from K.12.xx to K.13.03.

Release K.13.11

The following problems were resolved in release K.13.11 (not a public release).

- **TACACS+ (PR_1000764992)** — After authentication to the switch using TACACS+, the switch may crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300:.Stack
Frame=0x08632568 HW Addr=0x30313165 IP=0x008bba1c Task='mTacacsR'
Task ID=0x86329c0.fp: 0x08632750 sp:0x08632628 lr:0x008bba00
```

- **DHCP Snooping (PR_1000469934)** — When DHCP Snooping is enabled and configured, and a client sends a “DHCPINFORM” after receiving address information, the DHCP server response is not forwarded to the client by the switch.
- **Crash (1000790369)** — Use of VRRP may cause the switch to crash with a message similar to the following.

```
Software exception at vrrp_common_lib.c:313 -- in 'mVrrpCtrl', task
ID = 0x8526e20
```

- **Static Route (0000002610)** — After an update/roll-back/update (K.12 to K.13 to K.12 to K.13), static route entries may become corrupted, causing the CLI to hang following execution of the **show ip route** command.

Release K.13.12

The following problems were resolved in release K.13.12 (never released).

- **Crash (PR_0000002347)** — When a VLAN is deleted, all the modules may crash with a message similar to the following.

```
ipamSRtDescr.c Line:289 mIpAdMUpCt0x4484364c ->ASSERT:  failed
```

- **Certificate (PR_1000416167)** — The Web Management interface submission form limits CA-signed certificates to 1800 bytes.

- **802.1X (PR_0000002036)** — 802.1X with Funk Steel Belted RADIUS server causes the switch to fail to assign the VLAN that it was sent with the "Tunnel-Private-Group-Id" parameter.
- **Module Selftest (PR 0000001273)** — After a reboot, ports 1-24 or ports 25-48 on the ProCurve 3500yl, or ports 1-24 on the 6200yl switches, may become unresponsive followed by green and amber port LEDs remaining lit. The ports recover automatically. The log file will show the following messages.

```
chassis: Ports 1-24: Slave ROM Tombstone: 0x13000601
chassis: Ports 1-24: Lost Communications detected - Heart Beat
Lost(4A)
chassis: Ports 1-24 Downloading
chassis: Ports 1-24 Download Complete
chassis: Ports 1-24 Ready
```

- **SNMP (PR_1000772026)** — The wrong OID is set for a redundant power supply (RPS) failure.
- **CLI (PR_0000002177)** — When a ProCurve switch yl 10-GbE module (J8694A) is inserted into a 3500yl or 6200yl switch, the switch may prompt, "Do you want to save the config?," even when no changes to the config have been made.
- **Loopback Interface (PR_0000002165)** — A ping or Telnet session to a loopback address may fail intermittently. A traceroute to the loopback address completes successfully. This may cause some protocol packets to fail to reach the loopback address.
- **CLI (PR_1000745509)** — Output from the CLI command **show ipv6 neighbors vlan** <x> is not displaying the correct age, and it may erroneously display the State Age as "stale" after a recent learn.
- **ICMP (PR_1000764033)** — ICMP TTL expired messages are being sent with a source address of the interface from which the message is sent rather than the from the interface that receives the expired packet.
- **Web (PR_1000761014)** — The Web interface truncates 16 character passwords to 15 characters.
- **MIB (PR_1000770084)** — Several OIDs in MIB violate RFC 2737 and RFC 4133. The affected OIDs are:

```
.iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysic
al.entPhysicalTable.entPhysicalEntry.entPhysicalHardwareRev
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys
calEntry.entPhysicalFirmwareRev
```

```
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys
calEntry.entPhysicalSerialNum
  .iso.org.dod.internet.mgmt.mib-
2.entityMIB.entityMIBObjects.entityPhysical.entPhysicalTable.entPhys
calEntry.entPhysicalModelName
```

Release K.13.13

The following problems were resolved in release K.13.13 (never released).

- **802.1X (PR_1000446227)** — Switch 802.1X authentication running over PAP does not work if the RADIUS message authenticator attribute is required. This fix added the message authenticator attribute to non-EAP RADIUS responses.
- **VLAN/MSTP (PR_0000002103)** — The alteration of the VLAN/MSTP instance mapping in the pending configuration is not properly functioning. Any attempt to remove a single VLAN ID (VID) from one MSTP instance and then assign it to another MSTP instance fails, though specifying a VID range succeeds.
- **SSH (PR_0000001296)** — Upon reboot, if no key is present, a 1024-bit dsa ssh host key is installed rather than the previous default host key type of a 2048-bit rsa key.
- **CLI (PR_1000430534)** — Output from the show port-access mac-based CLI command may omit connected clients.
- **Static Routes/Config (0000001461)** — Static routes mapped to VLANs are incorrectly migrated during the update from K.12.xx to K.13.xx. This is a further improvement to the fix originally implemented in K.13.10.
- **DHCP (PR_0000002888)** — A client may not be able to get a DHCP address when the Management VLAN is configured on the switch.

Release K.13.14

The following problems were resolved in release K.13.14 (not a public release).

- **OSPF (PR_0000003395)** — If a transceiver or mini-GBIC is inserted (hotswapped) on a port that is a member of a VLAN configured for jumbo frames and OSPF, the OSPF state stops at EXCHANGE and EXSTART.

Release K.13.15

The following problems were resolved in release K.13.15 (never released).

No enhancements; No bug fixes.

Release K.13.16

The following problems were resolved in release K.13.16 (not a public release).

- **Enhancement (PR_0000001641)** — This enhancement allows the user to set the console inactivity time out without reboot. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_1000780247)** — This enhancement provides hpicf Download MIB support for transferring configuration files both to and from a TFTP server. Prior to this enhancement, MIB support was limited to downloading and uploading software files. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_0000001430)** — This enhancement allows the user to configure access methods for IP Authorized Manager entries. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_0000000090)** — This enhancement allows you to choose which information to display when you enter the **show interfaces** command. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_0000000857)** — This enhancement reduces the PIM delay time, thereby reducing the amount of time it takes for a packet to arrive at its destination when an IGMP Join is issued. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_0000001790)** — This enhancement provides the **no-tag-added** parameter that gives the user the option of not tagging a mirrored copy of an outbound packet. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_1000756562)** — This enhancement provides concurrent Web/MAC and 802.1x authentication. For more information, see "Release K.13.16 Enhancements" on page 94.
- **Enhancement (PR_0000000088)** — This enhancement provides new features for use with SSH. The SSH enhancements are: AES encryption (included in the K.13.02 release). A new configuration option is added to allow the server to specify the set of ciphers available for client connection; A configurable key; Message Authentication Code (MAC) configuration.

A new configuration option provides the ability to configure which MACs a client is permitted to use; Feedback information; and, SSH CLI **show** command information enhancements. For more information, see "Release K.13.16 Enhancements" on page 94.

- **Config (PR_0000000741)** — When the rate limit for broadcast or multicast inbound is set to 0% (i.e. blocking all traffic), output from the CLI command show running config doesn't display any rate limit information. If the rate limit is set to 100% (i.e. allow all traffic – the default), show running config shows that rate-limiting is set to 100%. The correct behavior is for non-default values to be displayed in the configuration.

Release K.13.17

The following problems were resolved in release K.13.17 (not a public release).

- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **Protocol Starvation (PR_0000003814)** — If the switch is configured for routing, certain packets may cause a packet buffer leak, resulting in some or all of the following symptoms:
  - OSPF neighbor relationships and route information are lost
  - PIM neighbor relationships are lost
  - Telnet, Ping, and SNMP become unresponsive

  Authorized Managers (PR_1000806039) — ProCurve Manager may delete Authorized Managers that have been configured on the switch.
- **Crash (PR_0000001756)** — Configuration of VLANs and VLAN port assignment using SNMP may cause the switch may crash with a message similar to the following.

  ```
  Software exception at bcmHwVlans.c:149 -- in 'mAdMgrCtrl', task ID
  = 0x18636e8 -> ASIC call failed: Entry not found.
  ```
- **Crash (PR_1000715077)** — When RADIUS Accounting is configured, the switch may crash with a message similar to the following.

  ```
  NMI event SW:IP=0x002bd6c4 MSR:0x00029210 LR:0x002bc6a8
  Task='mAcctCtrl' Task ID=0x85e9f10 cr: 0x48000084 sp:0x085e9e38
  xer:0x20000000
  ```
- **Static Route/Config (PR_0000003962)** — Updating from K.13.03 - K.13.09 to K.13.10 - K.13.16 can cause static routes configured with a VLAN as the next hop (vs. an IP address) do not translate correctly.

- **SNMP (PR_1000761379)** — When an SNMP get is used to gather statistics, the interface B1 on a J8702A module only updates its SNMP counters on every other query.
- **SNMP (PR_0000001807)** — Use of a correctly configured third party utility to connect to the switch via SNMPv3 may result in the following event log message.

```
SNMP Security access violation from <ip address>
```

- **PIM/Config (PR_0000002040)** — PIM configurations mapped to VLANs are incorrectly mapped after updating from K.12.xx to K.13.xx. Note that while this fix addresses the way the configuration is updated, rolling back the software while using the same configuration can still result in corruption in PIM configurations mapped to VLANs.

Release K.13.18

The following problems were resolved in release K.13.18 (never released).

- **UDLD (PR_0000002473)** — UDLD protocol packets received on a (non-UDLD) trunk port are incorrectly forwarded out of same port they are received on, resulting in high CPU usage on the switch.
- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the "show tech" command. For more information, see “Release K.13.18 Enhancements” on page 109.
- **SSH (PR_0000002946)** — ProCurve 8212zl switches do not automatically create the SSH folder on /cfa0; the result is that attempts to generate a crypto key may result in the following error.

```
Installing new RSA key.  If the key/entropy cache is depleted, this
could take up to a minute.
Operation aborted.
```

- **ACL (PR_0000004860)** — Mirrored ACL packets that match deny statements, are mirrored; the correct behavior is that only packets matching permit statements should be mirrored.
- **Crash (PR_0000004166)** — When the PIM Sparse Mode "trap all" parameter is configured and the link to PIM neighbor is disabled, the switch will crash and may report a message similar to the following.

```
Software exception at exception.c:501 -- in 'mPimsmCtrl', task ID =
0x8215d30 Memory system error at 0x7c838f0 – memPartFree
```

- **Mirror/CLI (PR_0000003269)** — The CLI incorrectly configures the option "no-tag-added" across multiple mirror sessions, resulting in the wrong output saved to the config file.

- **Wake-On-LAN (PR_0000004794)** — Wake-On-LAN does not always work successfully.
- **IP Phone (PR_0000004803)** — A tandem IP phone may stop talking to the switch after a connected PC login failure and reboot.
- **PIM-SM (PR_0000005219)** — When the switch sends a “Register-Stop” message, it will use an incorrect source IP address in the packet header of the message. Rather than using the IP address configured for the PIM RP, the switch uses the VLAN IP address.
- **Mirroring (PR_0000002926)** — When mirroring on a mesh or trunk port, the mirror session is not cleared after the mesh or trunk configuration is deleted.

Release K.13.19

The following problems were resolved in release K.13.19 (not a public release).

- **Enhancement (PR_0000003808)** — This enhancement allows the user to create command aliases for use in place of command names and their options. For more information, see “Release K.13.19 Enhancements” on page 109.
- **Enhancement (PR_0000000818)** — This enhancement allows the user to enter addresses and filter parameters for syslog using SNMP, which allows more options for remote access and management of the switch. For more information, see “Release K.13.19 Enhancements” on page 109.
- **Enhancement (PR_0000003390)** — This enhancement allows the user to customize Web Authentication HTML pages. For more information, see “Release K.13.19 Enhancements” on page 109.
- **Enhancement (PR_1000460265)** — This enhancement provides the user with Dynamic IP Lockdown, which is used to prevent IP source address spoofing on a per-port and per-VLAN basis. For more information, see “Release K.13.19 Enhancements” on page 109.

Release K.13.20

The following problems were resolved in release K.13.20 (not a public release).

- **Enhancement (PR_0000004124)** — Support was added for the J9144A ProCurve 10-GbE X2-SC LRM Optic. For more information, see “Release K.13.20 Enhancements” on page 138.
- **10-GbE (PR_0000001701)** — Sometimes, the LRM optic is misidentified as an LR optic.
- **CLI (PR_0000001528)** — 10-GbE X2 transceivers do not report their part numbers in response to the CLI command **show tech transceivers**.

- **X2 Transceivers (PR_0000004758)** — Some ProCurve SR and ER X2-10GbE (J8436A, J8437A) transceivers have a timing issue that prevents the transceivers from being correctly identified either when hot swapped or during a cold boot.
- **LEDs (PR_0000005623)** — Upon insertion of a removable transceiver – either X2 or SFP - the link LED fails to light for the 2 second-long indication of insertion confirmation.
- **Event Log (PR_0000005624)** — A failed "removable" transceiver results in two event log messages rather than just one.
- **Authentication (PR_0000005582)** — Sometimes PC in the PC-phone tandem authentication does not get authorized on its untagged VLAN.

Release K.13.21

The following problems were resolved in release K.13.21 (never released).

- **CLI (PR_1000760929)** — Output from the CLI command **show name int <***port list***>** fails to display the port number for interfaces with numbers larger than 9.
- **Config (PR_0000003638)** — Fastboot can be configured, but then it cannot be disabled.
- **Multicast Filter (PR_0000002988)** — Multicast filters may become corrupted following their initial configuration, save and subsequent switch reload.
- **Self-Test (PR_0000001406)** — The failure of a single module within a Switch 8212zl or 5400zl chassis may cause false self-test failures for other installed modules.
- **CLI (PR_0000005300)** — The displayed output of the CLI command **show ip pim rp-set** is not properly formatted.
- **CLI (PR_0000005302)** — The displayed output of the CLI command **show ip pim pending** is not properly formatted.
- **CLI (PR_1000782972)** — An incorrect line voltage value may be displayed in the output of the **show system power** CLI command.
- **CLI (PR_0000005381)** — Attempts to perform a **copy flash <primary|secondary>** at the CLI of a 8212zl switch running K.13.05 or higher will fail with the following error.

```
Flash-to-flash copy of product code failed
```

- **Config (PR_1000781011)** — Copying a config onto a switch allows the appearance of an invalid flow control setting (enabled) on half duplex ports.
- **Config (PR_1000781015)** — When the MDIX-mode is configured for dual-personality ports, copying a config onto a switch fails and produces a message about config file corruption.

- **Config (PR_1000781031)** — When the valid port setting 'auto-1000' is configured for any 10/100/1000 interface in an external configuration file and the configuration file is copied to the switch, the system returns the port setting to the default value, changing 'auto-1000' to 'auto.'
- **CLI (PR_0000004687)** — The CLI command **ip access-list resequence <name-str>** does not accept a number for the ACL title as it should.
- **PIM-SM (PR_0000006180)** — PIM Sparse Mode may choose an incorrect rendezvous point (RP), causing interoperability problems. This fix changes the way a RP is chosen such that ALL the devices running "K" versions of software must be on either pre- or post-fix software version in order to use the same criteria to choose the PIM RP.
- **Event Log (PR_1000755803)** — ProCurve Manager is unable to display a link to the switch Web Interface in events generated by Fault Finder.

Release K.13.22

The following problems were resolved in release K.13.22 (not a public release).

- **CLI (PR_0000002856/1000769143)** — The switch is unable to execute the CLI command **show tech** while in QinQ svlan mode.
- **OSPF (PR_0000006183)** — OSPF ECMP may drop up to 50% of the traffic destined for its next hop.
- **Mini-GBIC (PR_0000006298)** — Mini-GBICs in dual-personality ports fail self-test when the switch is running K.13.20-K.13.21. Workaround: Configure fastboot.
- **Licensing (PR_0000006554)** — An invalid hardware ID (required for Premium Licensing in 3500yl and 5400zl switches) is created by switches running K.13.15 - K.13.21.

Release K.13.23

The following problems were resolved in release K.13.23.

- **Crash (PR_0000006624)** — When using the Web Management Interface on software version K.13.17 and higher, the switch may crash if the "Configuration" and then "IP Configuration" tabs are clicked. There may be other triggers for this crash. The switch will display a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x0815da48 HW Addr=0xa2d3e193 IP=0x00169178
Task='tHttpd' Task ID=0x fp: 0x00a650c4 sp:
```

- **Authentication (PR_0000007209)** — A PC behind a tandem IP phone is not able to authenticate.

Release K.13.24

The following problems were resolved in release K.13.24 (not a public release).

- **OSPF (PR_0000006183a)** — OSPF ECMP may drop up to 50% of the traffic destined for its next hop. This fix adds to that implemented in K.13.22 via the same PR.
- **Crash (PR_0000003949)** — Implementation of OSPF ECMP route changes may cause the switch to crash with a message similar to the following.

```
Software exception at exception.c:501 -- in 'eRouteCtrl', task ID =
0x83da3f0 -> Memory system error at 0x7bd9540 - memPartFree
```

- **802.1X (PR_ 0000007259)** — Configuring 802.1X without activating it does not function as expected, resulting in blocking of the port.

Release K.13.25

The following problems were resolved in release K.13.25.

- **SSH (PR_0000002934)** — Copying the client's public SSH keys from the switch fails with the following error.

```
Couldn't read from remote file "/ssh/mgr_keys/authorized_keys
```

- **Crash (PR_0000004023)** — Repeated PCM configuration scans may cause the switch to crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x07af44c0
HW Addr=0x6520463a IP=0x00965a88 Task='tSsh0' Task ID=0x7af4810fp:
0x013d97cc sp:0
```

- **Management Module (PR_0000005902)** — The management module may become unresponsive, resulting in loss of Telnet, Web Management, and console access functionality of the switch.
- **802.1X Authentication (PR_0000002695)** — When an 802.1X enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. This allows the RADIUS server to reply with a large fragment which the switch does not process, causing the authentication to fail. This is an additional fix for the issue described in K.13.17 via PR_1000779048.

- **GVRP/RADIUS (PR_0000006051)** — RADIUS-assigned VLANs are not propagated correctly in GVRP. Please see "Note: This fix is associated with some new switch behavior: " for a description of the behavior change with this fix.

  Note: This fix is associated with some new switch behavior:

  When only one port has learned of a dynamic VLAN, it will advertise that VLAN if an auth port has been RADIUS-assigned that dynamic VLAN, regardless of the unknown-VLANs configuration of that port. The fix accommodates RADIUS-assigned (and hpicfUsrProf MIB-assigned) tagged VLANs as well as untagged VLANs. These changes are enabled by default and are not configurable. This fix does not modify any other GVRP behavior.

- **Assert (PR_0000001836)** — VRRP configuration conversion from K.12.xx to K.13.xx software may experience a crash (assert) in ConfigRecIndex().

- **Assert (PR_0000005208)** — Entering **no ipv6 enable** at the CLI may result in a crash with a message similar to the following.

  ```
  Software exception at ConfigRecIndex.cc:421 -- in 'mSess1', task ID
  = 0x58c1c38-> ASSERT:  failed.
  ```

- **Config (PR_0000002620)** — A MAC-lockdown command that includes VLAN information may fail when it is copied to the default configuration.

Release K.13.26 through K.13.39

Software never built.

Release K.13.40

The following problems were resolved in release K.13.40 (Never released).

- **Enhancement (PR_0000003127)** — Link Trap and LACP Global Enable/Disable. For more information, see "Release K.13.40 Enhancements" on page 139.

- **Enhancement (PR_0000003128)** — The ability to clear statistics was added. For more information, see "Release K.13.40 Enhancements" on page 139.

- **Enhancement (PR_0000003718)** — The MAC Lockout limit was increased. For more information, see "Release K.13.40 Enhancements" on page 139.

- **Enhancement (PR_0000007388)** — Crash Log Debug. For more information, see "Release K.13.40 Enhancements" on page 139.

- **Crash (PR_0000003597)** — Configuring a kbps based rate-limit on 10Gig port may trigger a crash in the area of `bttfHwRateLimits.c:2191`.

Release K.13.41

The following problems were resolved in release K.13.41 (Not a public release).

- **AAA (PR_0000008409)** — The CLI commands **aaa authentication** and **aaa accounting** return a `resource unavailable` error.
- **PCM (PR_0000008113)** — Repeated ProCurve Manager Config Scans may trigger subsequent Config Scan failure.

Release K.13.42

The following problems were resolved in release K.13.42 (Never released).

- **Config (PR_0000007953)** — The config line **spanning-tree instance <n> vlan <vid>** is truncated in some cases, causing loss of configuration after reload of the config file.
- **CLI (PR_0000000912)** — The CLI command **copy tftp show-tech** fails, resulting in failure to create a custom show-tech file on the switch.
- **TFTP (PR_0000008559)** — The switch administrator is unable to download a new image file after executing the CLI command **erase primary flash**; a `corrupted download file` error is reported.
- **ARP (PR_0000008011)** — When port-security is configured, the switch sends ARP requests twice for an unknown DA, making the switch appear to be slow.
- **SFTP/SCP (PR_0000008270)** — Beginning with software version K.13.25, SFTP/SCP will not close the "client" session after the file transfer. The client session will need to be manually closed.
- **RADIUS (PR_0000007278)** — MAC-based authentication doesn't work with a secondary RADIUS server unless the primary and secondary RADIUS server keys are identically configured.
- **Crash (PR_0000006476)** — Some configuration commands entered at the CLI (e.g. **web**, or **no web**) may cause the switch to crash with a message similar to the following:

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack
Frame=0x088befe8HW Addr=0x00cff108 IP=0x0096ca4c Task='mSnmpCtrl'
Task ID=0x88bf320 fp: 0x0845a7e0
```

- **Crash (PR_0000005940)** — An attempt at tab completion for some configuration tasks in the PIM context may cause the switch to crash with a message similar to the following:

```
Software exception at parser.c:6291 -- in 'mSess1', task ID =
0x82ab3b0
```

- **CLI (PR_0000004042)** — The CLI command **snmp-server response-source dst-ip-of-request** does not work as expected when the destination IP address of the *SNMP Request* is the Loopback IP. The source IP address of the *SNMP Response* should be the destination IP of the *SNMP Request*, but instead the switch uses the IP address of the active interface from which the *SNMP Response* was sent.
- **CLI (PR_0000007686)** — The switch does not allow IP authorized-manager configuration of 10.0.0.0.
- **TACACS+ (PR_0000003839)** — The TACACS server configuration parameter accepts an address from an invalid/reserved IP range: 0.0.0.1 to 0.255.255.255.
- **Boot Log (PR_0000009434)** — The switch doesn't create an event log message after deleting an invalid TACACS server host config entry upon bootup following an update from K.12.xx to K.13.xx

Release K.13.43

The following problems were resolved in release K.13.43 (Not a public release).

- **CLI (PR_0000005759)** — There may be odd CLI output in response to a **show modules** command, if that command is executed during module initialization.
- **SNMP (PR_0000001926)** — An SNMP query for the MIB **ifInUnknownProtos** returns incorrect and varying results.
- **Enhancement (PR_0000003557)** — The ability to enable/disable the USB port via CLI and SNMP was added. Note that after being disabled and subsequently re-enabled, the USB port may not function consistently with the PCM USB Autorun features until the switch has been reloaded. For more information, see "Release K.13.43 Enhancements" on page 143.

Release K.13.44

The following problems were resolved in release K.13.44 (Not a public release).

- **ICMP Redirects (PR_0000004534)** — With the next hop router is in the same VLAN as the host machine, the switch does not generate ICMP redirects.
- **Crash (PR_0000009736)** — In some situations, ICMP redirects may cause the switch to crash with a message similar to the following.

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x084f2e40

HW Addr=0x00cff108 IP=0x00870e5c Task='mIpPktRecv' Task ID=0x84f3140
fp: 0x0a84d994
```

- **CLI (PR_1000803731)** — If the "|" character exists in the banner text of a configuration file downloaded via TFTP transfer, the banner text may become corrupted, or the TFTP transfer may fail with a `corrupted download file` error message.
- **Hang (PR_0000007806)** — Using the CLI command **no arp** on ARP entries that do not exist may cause the switch to hang.
- **CLI (PR_0000008617)** — The **copy** command for USB options has incorrect optional parameters for plain text files.
- **RADIUS Accounting (PR_0000004139)** — Procurve switches do not send the accounting-request to a RADIUS server upon execution of the **reload** CLI command.
- **RADIUS Accounting (PR_0000004145)** — An incomplete "Calling-Station-ID" field is sent in the accounting-request to the RADIUS server upon execution of the **boot system** CLI command.
- **RADIUS Accounting (PR_0000004141)** — The "Acct-Status-Type" attribute is missing in the accounting-request to RADIUS server upon execution of the **boot system** CLI command.
- **Terminal Display** (PR_0000008238) — The default boot message is displayed with the wrong formatting if the terminal width is changed.
- **CLI (PR_0000008236)** — The **enable** CLI command is listed in enable-mode help.
- **UDLD (PR_0000009505)** — UDLD misconfiguration (where UDLD is enabled on one side and disabled on the other) could lead to a unicast packet storm which results in MSTP is running with multiple roots.
- **CLI (PR_0000008217)** — The **copy flash** CLI command does not allow the user to specify a source OS location (primary/secondary).

Release K.13.45

The following problems were resolved in release K.13.45.

- **STP (PR_0000010815)** — When a switch configured with BPDU protection is added to a network, if the MSTP configuration of the uplink port is changed from **auto-edge** to **no auto-edge** there is a topology change event that takes place as the switch asserts itself as a new root.
- **Enhancement (PR_0000010783)** — Support was added for the following products.

  J9099B - ProCurve 100-BX-D SFP-LC Transceiver

  J9100B - ProCurve 100-BX-U SFP-LC Transceiver

  J9142B - ProCurve 1000-BX-D SFP-LC Mini-GBIC

J9143B – ProCurve 1000-BX-U SFP-LC Mini-GBIC

For more information, see "Release K.13.45 Enhancements" on page 144.

- **Transceivers (PR_0000010525) —** Intermittent self test failure may occur if transceivers are hot-swapped in and out of the switch in too short a time frame. Note that even with this fix, transceivers should always be allowed to initialize fully prior to removal and subsequent re-insertion.

  Best Practice Tip: Upon hot insertion of a transceiver, the Mode LED will come on for two seconds while the transceiver is initialized. Once the Mode LED has extinguished, it is safe to remove the transceiver.

- **Selftest Failure (PR_0000010937)** — Rarely, the switch may experience self test failure of all the modules. Messages like the following will be visible in the event log. Re-seating the modules may allow successful self-test to occur.

  ```
  W <date/time stamp> 00374 chassis: Slot # Failed to
  boot-timeout-(SELFTEST)
  ```

Release K.13.46

The following problems were resolved in release K.13.46. (Never released.)

- **sFlow (PR_0000003723)** — The switch uses the loopback as the sFlow agent address, even after explicit configuration of the VLAN IP address and the collector receiving the sFlow packets.

- **SCP/SFTP (PR_0000009174)** — Failure to upload a configuration via SFTP/SCP may occur. As a result, it is possible that the switch may become unresponsive or crash with a message similar to the following.

  ```
  Software exception at cfg_edit.cc:313 – in 'swinitTask', task ID =
  0xa9bbcc0
  ```

- **SCP (PR_0000011488)** — The switch does not return the scp/sftp session after new software is uploaded.

- **CLI (PR_0000009997)** — The CLI response to the **boot set-default flash <primary | secondary>** configuration setting is inconsistent between the zl (5400zl/8212zl) and yl (3500yl/6200yl) switches, potentially causing issues for customers running scripts.

- **Password Encryption (PR_0000011828)** — The Password Manager portion of the Include Credentials feature is using SHA-0 Instead of SHA-1 for creation of the hash value. In order to accommodate customers that have worked around this issue, this fix will translate the configuration and correctly report the use of SHA-0 in the config after a software update containing this fix.

  Example line from password encryption config prior to the fix:

```
password operator sha-1 "lsadkjlkjfsd..."
```

Example of what that line might look like after the fix:

```
password operator sha0 "lsadkjlkjfsd..."
```

No switch administrator intervention is required for the forward configuration translation to occur.

Support Note: This fix has implications for rolling back the software. If password encryption is configured and a switch running software with the fix is rolled back to a software version prior to the fix using the same config file, the config loading will fail, and error messages for each line containing "sha0" or "sha1" will be displayed on the switch terminal. In the following example, sha1 was line 14 in the config, and sha0 was on line 15 of the config.

```
Line:14. Invalid input: *sha1*
Line:15. Invalid input: *sha0*
```

To avoid configuration compatibility issues, please follow the instructions in the "Best Practices for Major Software Updates" on page 7. If roll back to a pre-fix software version occurs without following the Best Practice suggestion (association of a compatible config file with a software version), the switch administrator should gain access to the switch by hitting <enter> at the password prompt, and must then reconfigure the password encryption with valid parameters (the pre-fix CLI syntax is **SHA-1,** versus the post-fix CLI use of **SHA0** or **SHA1**).

The default hash value for newly configured password encryption on a software version with this fix is **SHA1**.

- **CLI (PR_0000009860)** — Output from the CLI command **show module** erroneously reports the 8212zl System Support Module (SSM) product number as J8784A instead of J9095A.
- **Crash (PR_0000011049**) — Copying a configuration with mirroring enabled from USB to switch may trigger a software exception with a message similar to the following.

  ```
  Software exception at cli_mirror.c:9953 -- in 'mftTask', task ID
  = 0xa932bc0
  ```

- **VRRP (PR_0000003634)** — When the VRRP Owner router (with preempt-delay-time configured) is rebooting, the VRRP Backup router momentarily gives up Master role (but does resume it) before the VRRP Owner is back online. This may cause an unexpected outage.
- **DHCP Relay (PR_0000011726)** — When the VRRP backup router is the master for the network, DHCP Discover packets are relayed with a corrupted IP address for the Relay Agent. This causes the server to look up a client address range for an invalid network segment, and ultimately fail to communicate with the DHCP Server.
- **PC/Phone Authentication (PR_0000010104)** — When using an IP phone in tandem with a PC, sometimes the post-authentication VLAN assignment of the PC is delayed.

Release K.13.47

The following problems were resolved in release K.13.47. (Never released.)

- **OSPF ECMP (PR_0000004798)** — Some IP subnets which are multiple hops away are not reachable from certain clients despite the presence of the target subnet in the switch routing table. Workaround: Initiate a traceroute from the switch to the client PC.

Release K.13.48

The following problems were resolved in release K.13.48. (Never released.)

- **DHCP Relay (PR_0000013661/000008196)** — After adding a second IP Address to a VLAN with IP Helper configured, the switch Relay Agent IP Address gets corrupted such that the DHCP server does not recognize the request as part of a configured scope, and drops the request. Workaround: Save the configuration and reload the switch after configuration of an IP Helper address and DHCP Relay.

- **Module/Fabric Errors (PR_0000012418)** — Switches running system software version K.12.45 or higher may see one or more of the following errors in the event log, potentially causing false self-test failures.

```
W 12/02/08 14:24:59 00374 chassis: HSL Non-Fatal F0: SLOT D HSL
#11 - HSL status FF002000
W 12/02/08 14:25:25 00374 chassis: Slot D: Msg loss detected - no
ack for seq # 37
W 12/02/08 14:25:38 00374 chassis: Slot D Slave ROM Tombstone:
0x13000601
W 12/02/08 14:25:38 00374 chassis: Slot D: Lost Communications
detected – Source Message System(59)
W 12/02/08 14:25:58 00374 chassis: HSL Non-Fatal F0: SLOT D HSL   #11
- HSL status FF002000 W 12/02/08 14:26:17 00374 chassis: Slot D: Msg
loss detected - no       ack for seq # 40
W 12/02/08 14:27:28 00374 chassis: Slot D Failed to
boot-timeout-     (SELFTEST)
```

- **OSPF ECMP (PR_0000013777)** — When the switch is acting as an ECMP router with multiple next hops available, sometimes it fails to route packets received on a local VLAN to hosts that are reachable via ECMP routes. The result is intermittent connectivity to hosts on the other side of ECMP routes.

- **Boot ROM (PR_0000014318)** — This build introduces the new K.12.14 boot ROM, a prerequisite for future updates. Please do not interrupt power to the switch during the software/boot ROM update!

Release K.13.49

The following problems were resolved in release K.13.49.

- **Auto-TFTP (PR_0000014646/0000013552)** — Certain software file names may trigger auto-tftp to reload the same software file repeatedly.

© 2006 - 2008 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

January 2009
Manual Part Number
5991-4720