ProCurve Networking
HP Innovation

Release Notes:
Version M.08.107 Software
for the ProCurve Series 6400cl Switches

"M" software versions are supported on these switches:

ProCurve Switch	M.08.51 through M.08.95	M.08.99.x and newer	M.08.96, M.08.97, M.10.01 and newer
ProCurve Switch 3400cl-24G (J4905A)	✔		✔
ProCurve Switch 3400cl-48G (J4906A)	✔		✔
ProCurve Switch 6400cl-6XG 10-GbE CX4(J8433A)	✔	✔	
ProCurve Switch 6410cl-6XG 10-GbE X2(J8474A)	✔	✔	

Release M.08.107 supports theseProCurve switches: 6400cl-6XG 10-GbE CX4 (J8433A), and 6410cl-6XG 10-GbE X2 (J8474A)

These release notes include information on the following:

- Downloading switch software and documentation from the Web (page 1)
- Clarification of operating details for certain software features (page 18)
- A listing of software enhancements in this release (page 22)
- A listing of software fixes included in releases M.08.51 through M.08.10x (page 44)

Security Note:
Downloading and booting software release M.08.89 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. For more information, refer to "Enforcing Switch Management Access Security" on page 8 and "Using SNMP To View and Configure Switch Authentication Features" on page 32.

Related Publications
For the latest version of any of the publications listed below, visit **http://www.procurve.com**. Click on **Technical support**, then **Product manuals**.

- Management and Configuration Guide* (part number 5990-6050)
- Advanced Traffic Management Guide* (part number 5990-6051)
- Access Security Guide* (part number 5990-6052)

*Covers the ProCurve Series 5300xl, Series 3400cl, and Series 6400cl switches.

Publication Number

5991-4765
March, 2007

Applicable Product

ProCurve Switch 6400cl-6XG 10-GbE CX4 (J8433A)
ProCurve Switch 6410cl-6XG 10-GbE X2 (J8474A)

Trademark Credits

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

Software Credits

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

http:// www.openssh.com.

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

http://www.openssl.org.

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

Disclaimer

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

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

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

Warranty

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

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

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

Contents

Software Management

Software Updates

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

Downloading 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.

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

   http://www.procurve.com.

2. Click on **Software updates** (in the sidebar).
3. Under **Latest software**, click on **Switches**.

To Download Product Documentation: You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

1. Go to the ProCurve Networking Web site at **http://www.procurve.com**.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation.
4. On the resulting web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Switch

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

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

Note

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

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

TFTP Download from a Server

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

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

For example, to download a software file named M_08_8x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
HPswitch # copy tftp flash 10.28.227.103 M_08_8x.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 shown in figure 1. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:

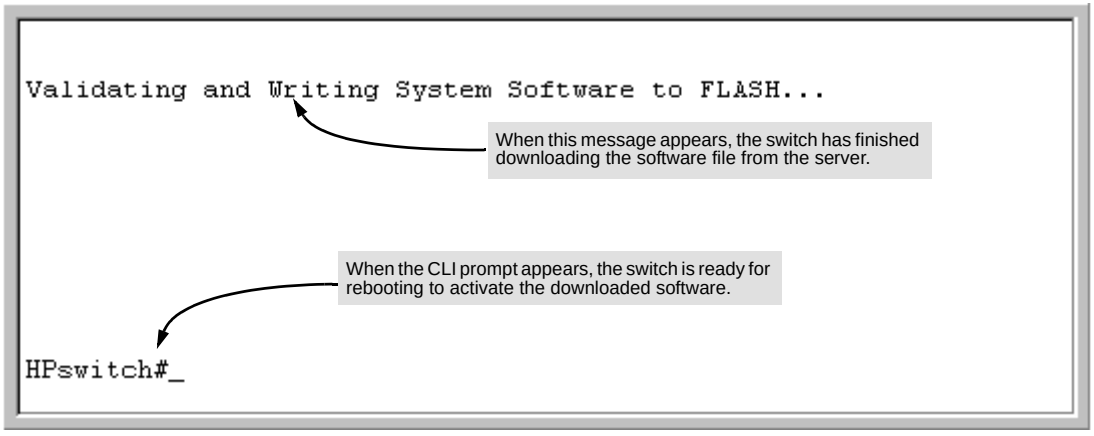

Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

3. Reboot the switch.

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (Refer to the Installation and Getting Started Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch software is stored on a disk drive in the PC.

- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the Send File option in the Transfer dropdown menu.)

Using Xmodem and a terminal emulator, you can download a switch software file to either primary or secondary flashusing 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:

   ```
   HPswitch(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:

   ```
   HPswitch # 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), use the same command to return it to its previous setting. (HP recommends a baud rate of 9600 bits per second for most applications.) Remember to return your terminal emulator to the same baud rate as the switch.)

5. Reboot the switch.

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

Saving Configurations While Using the CLI

The switch operates with two configuration files:

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

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

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

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

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
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, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G)
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
T	Switch 2900 Series (2900-24G, and 2900-48G)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Minimum Software Versions for Series 6400cl Switch Features

For Switch 6400cl Hardware Accessories

ProCurve Device	Minimum Supported Software Version
J8434A ProCurve 10-GbE Copper Module	M.08.62
J8435A ProCurve 10-GbE Media Flex Module	M.08.62
J8436A ProCurve 10-GbE X2-SC SR Optic	M.08.62
J8437A ProCurve 10-GbE X2-SC LR Optic	M.08.62
J8438A ProCurve 10-GbE X2-SC ER Optic	M.08.75
J8439A ProCurve 10-GbE CX4 Media Converter	M.08.54
J8440A ProCurve 10-GbE X2-CX4 Transceiver	M.08.54
J8440B ProCurve 10-GbE X2-CX4 Transceiver	M.08.102

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, SP1	Sun Java 2 Runtime Environment: – Version 1.5.0.02
Windows Server SE 2003 SP1	6.0, SP1	

Enforcing Switch Security

ProCurve switches are designed as "plug and play" devices, allowing quick and easy installation in your network. However, when preparing the switch for network operation, ProCurve strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportunity for access and possible malicious actions. Since security incidents can originate with sources inside as well as outside of an organization, your switch and network access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and uses.

This section provides an overview of switch management and network access security features and applications. For information on specific features, refer to the software manuals provided for your switch model.

Caution:

In its default configuration, the switch is open to unauthorized access of various types. ProCurve recommends that you review this section to help ensure that you recognize the potential for unauthorized switch and network access and are aware of the features available to help prevent such access.

Switch Management Access Security

This section outlines provisions for protecting access to the switch's status information configuration settings. For more detailed information on these features, refer to the indicated manuals.

Default Settings Affecting Security

In the default configuration, switch management access is available through the following methods:

- Telnet
- Web-browser interface (including the ability to launch Telnet access)
- SNMP access
- Front-Panel access (serial port access to the console, plus resets and clearing the password(s) or current configuration)

It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch hardware.

Local Manager Password

In the default configuration, there is no password protection. Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch's web browser and console (CLI and Menu) interfaces. The Manager password can easily be set using the CLI **password manager** command, the Menu interface **Console Passwords** option, or the password options under the **Security** tab in the web browser interface.

Inbound Telnet Access and Web Browser Access

The default remote management protocols enabled on the switch are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL must be used for remote access. This enables you to employ increased access security while still retaining remote client access.

- SSHv2 provides Telnet-like connections through encrypted and authenticated transactions
- SSLv3/TLSv1 provides remote web browser access to the switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.

(For information on SSH and SSL/TLS, refer to the chapters on these topics in the *Advanced Traffic Management Guide* for your switch.)

Also, access security on the switch is incomplete without disabling Telnet and the standard web browser access.Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two commands:

- **no telnet-server**: This CLI command blocks inbound Telnet access.
- **no web-management**: This CLI command prevents use of the web browser interface through http (port 80) server access.

If you choose not to disable Telnet and web browser access, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch. Refer to the chapter titled "RADIUS Authentication and Accounting" in the *Access Security Guide* for your switch.

Secure File Transfers

Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices. For more on these features, refer to the section titled "Using Secure Copy and SFTP" in the "File Transfers" appendix of the *Management and Configuration Guide* for your switch.

SNMP Access (Simple Network Management Protocol)

In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing and changing the settings and status data in the switch's MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

General SNMP Access to the Switch. The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options. ProCurve recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation). SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers
- restricting non-SNMPv3 agents to either read-only access or no access
- co-existing with SNMPv1 and v2c if necessary

For more on SNMPV3, refer to the next subsection and to the chapter titled "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

SNMP Access to the Switch's Authentication Configuration MIB . A management station running an SNMP networked device management application such as ProCurve Manager Plus (PCM+) or HP OpenView can access the switch's management information base (MIB) for read access to the switch's status and read/write access to the switch's configuration. In earlier software versions, SNMP access to the switch's authentication configuration (hpSwitchAuth) MIB was not allowed. However, beginning with software release M.08.89, the switch's default configuration allows SNMP access to security settings in hpSwitchAuth. If SNMP access to the hpSwitchAuth MIB is considered a security risk in your network, then you should implement the following security precautions when downloading and booting from software release M.08.89 or greater:

1. If SNMP access to the authentication configuration (hpSwitchAuth) MIB described above and in the section titled "Using SNMP To View and Configure Switch Authentication Features"(page 32) is not desirable for your network, then immediately after downloading and booting from the M.08.89 or greater software for the first time, use the following command to disable this feature:

   snmp-server mib hpswitchauthmib excluded

Caution:

Downloading and booting from the M.08.89 or greater software version for the first time enables SNMP access to the authentication configuration MIB (the default action). If SNMPv3 and other security safeguards are not in place, the switch's authentication configuration MIB is exposed to unprotected SNMP access and you should use the above command to disable this access.

2. If you choose to leave the authentication configuration MIB accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to access the MIB:
   - Configure SNMP version 3 management and access security on the switch.
   - Disable SNMP version 2c on the switch.

Refer to "Using SNMP Tools To Manage the Switch" in the chapter titled "Configuring for Network Management Applications" in the Management and Configuration Guide for your switch. .

Physical Access to the Switch

Physical access to the switch allows the following:

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch's Clear and Reset buttons for these actions:
  - clearing (removing) local password protection
  - rebooting the switch
  - restoring the switch to the factory default configuration (and erasing any nondefault configuration settings)

Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you can do the following:

- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch's factory default settings.
- Disable or re-enable password recovery.

For the commands to implement the above actions, refer to "Front-Panel Security" in the chapter titled "Configuring Usernames and Passwords" in the *Access Security Guide* for your switch.

Other Provisions for Management Access Security

Authorized IP Managers. This feature uses IP addresses and masks to determine whether to allow management access to the switch through the network, and covers access through the following:

- Telnet and other terminal emulation applications
- The switch's web browser interface
- SNMP (with a correct community name)

Refer to the chapter titled "Using Authorized IP Managers" in the *Access Security Guide* for your switch.

Secure Management VLAN. This feature creates an isolated network for managing the ProCurve switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and web browser interface access is restricted to ports configured as members of the VLAN.

Refer to the chapter titled "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

RADIUS Authentication. For each authorized client, RADIUS can be used to authenticate operator or manager access privileges on the switch via the serial port (CLI and Menu interface), Telnet, SSH, and Secure FTP/Secure Copy (SFTP/SCP) access methods.

Refer to the chapter titled "RADIUS Authentication and Accounting" in the *Access Security Guide* for your switch.

TACACS+ Authentication. This application uses a central server to allow or deny access to TACACS-aware devices in your network. TACACS+ uses username/password sets with associated privilege levels to grant or deny access through either the switch's serial (console) port or remotely, with Telnet. If the switch fails to connect to a TACACS+ server for the necessary authentication service, it defaults to its own locally configured passwords for authentication control. TACACS+ allows both login (read-only) and enable (read/write) privilege level access.

Refer to the chapter titled "TACACS+ Authentication" in the *Access Security Guide* for your switch model.

Access Control Lists (ACLs) for Management Access Protection. ACLs can be used to secure access to the management interface of the switch by blocking inbound IP traffic that has the switch itself as the destination address. (Refer also to "Access Control Lists" in the next section.)

Network Access Security

This section outlines provisions for protecting access through the switch to the network. For more detailed information on these features, refer to the indicated manuals.

Access Control Lists (ACLs)

ACLs enable the switch to permit or deny the following:

- any inbound IP traffic on a port
- specific types of TCP or UDP traffic

While ACLs do not provide user or device authentication, or protection from malicious manipulation of data in IP packet transmissions, ACLs can enhance network security by blocking selected IP traffic types. This functionality can be utilized to:

- permit or deny in-band management access by limiting or preventing the use of designated TCP or UDP protocols
- permit or deny unwanted IP traffic to or from specific hosts

Refer to the chapter titled "Access Control Lists (ACLs) for the Series 3400cl and Series 6400cl Switches" in the *Advanced Traffic Management Guide* for your switch model.

Web and MAC Authentication

These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC address for access to the network.

Refer to the chapter titled "Web and MAC Authentication" in the *Access Security Guide* for your switch model.

Secure Shell (SSH)

SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:

- **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 stored public key can gain access to the switch.
- **switch SSH and user password authentication:** this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client's key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.
- **secure copy (SC) and secure FTP (SFTP):** By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information.

Refer to the chapter titled "Configuring Secure Shell (SSH)" in the *Access Security Guide* for your switch model. For more on SC and SFTP, refer to the section titled "Using Secure Copy and SFTP" in the "File Transfers" appendix of the *Management and Configuration Guide* for your switch model.

Secure Socket Layer (SSLv3/TLSv1)

This feature includes use of Transport Layer Security (TLSv1) to provide remote web access to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication.

Refer to the chapter titled "Configuring Secure Socket Layer (SSL) in the *Access Security Guide* for your switch model.

Traffic/Security Filters

These statically configured filters enhance in-band security (and improve control over access to network resources) by forwarding or dropping inbound network traffic according to the configured criteria. Filter options and the devices that support them are listed in the following table:

Switch Model	Source-Port Filters	Protocol Filters	Multicast Filters
Series 6400cl	X	--	--
Series 5400zl	X	X	X
Series 5300xl	X	X	X
Series 4200vl	X	--	--
Series 3500yl	X	X	X
Series 3400cl	X	--	--
Series 2800	X	--	--
Series 2600	X	--	--

- **source-port filters:** Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.
- **multicast filters:** Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports or dropped on a per-port (destination) basis.
- **protocol filters:** Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.

Refer to the chapter titled "Traffic/Security Filters" in the *Access Security Guide* for your switch model.

802.1X Access Control

This feature provides port-based or client-based authentication through a RADIUS server to protect the switch from unauthorized access and to enable the use of RADIUS-based user profiles to control client access to network services. Included in the general features are the following:

- client-based access control supporting up to 32 authenticated clients per-port
- port-based access control allowing authentication by a single client to open the port
- switch operation as a supplicant for point-to-point connections to other 802.1X-aware switches

The following table shows the type of access control available on the various ProCurve switch models:

Access Control Types	6200yl 5400zl 3500yl	5300xl 4200vl	3400cl 6400cl	2800 2600 2600-pwr	4100gl
client-based access control (up to 32 authenticated clients per port)	X	X*	--	--	--
port-based access control (one authenticated client opens the port)	X	X	X	X	X
switch operation as a supplicant	X	X	X	X	X
* On the 5300xl switches, this feature is available with software release E.09.02 and greater.					

Refer to the chapter titled "Configuring Port-Based and Client-Based Access Control" Access Security Guide for your switch model.

Port Security, MAC Lockdown, MAC Lockout, and IP Lockdown

These features provide device-based access security in the following ways:

- **port security:** Enables configuration of each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. Some switch models also include eavesdrop prevention in the port security feature.
- **MAC lockdown:** This "static addressing" feature is used as an alternative to port security for to prevent station movement and MAC address "hijacking" by allowing a given MAC address to use only one assigned port on the switch. MAC lockdown also restricts the client device to a specific VLAN.
- **MAC lockout:** This feature enables blocking of a specific MAC address so that the switch drops all traffic to or from the specified address.
- **IP lockdown:** Available on Series 2600 and 2800 switches only, this feature enables restriction of incoming traffic on a port to a specific IP address/subnet, and denies all other traffic on that port.

Refer to the chapter titled "Configuring and Monitoring Port Security" in the *Access Security Guide* for your switch model.

Key Management System (KMS)

KMS is available in several ProCurve switch models and is designed to configure and maintain key chains for use with KMS-capable routing protocols that use time-dependent or time-independent keys. (A key chain is a set of keys with a timing mechanism for activating and deactivating individual

keys.) KMS provides specific instances of routing protocols with one or more Send or Accept keys that must be active at the time of a request.

Refer to the chapter titled "Key Management System" in the *Access Security Guide* for your switch model.

Connection-Rate Filtering Based On Virus-Throttling Technology

While not specifically a tool for controlling network access, this feature does help to protect the network from attack and is recommeded for use on the network edge. It is primarily focused on the class of worm-like malicious code that tries to replicate itself by taking advantage of weaknesses in network applications behind unsecured ports. In this case, the malicious code tries to create a large number of outbound IP connections on a routed interface in a short time. Connection-Rate filtering detects hosts that are generating routed traffic that exhibits this behavior, and causes the switch to generate warning messages and (optionally) to either throttle routed traffic from the offending hosts or drop all traffic from the offending hosts.

Refer to the chapter titled "Virus Throttling" in the *Access Security Guide* for your switch model.

Identity-Driven Management (IDM)

IDM is a plug-in to ProCurve Manager Plus (PCM+) and uses RADIUS-based technologies to create a user-centric approach to network access management and network activity tracking and monitoring. IDM enables control of access security policy from a central management server, with policy enforcement to the network edge, and protection against both external and internal threats.

Using IDM, a system administrator can configure automatic and dynamic security to operate at the network edge when a user connects to the network. This operation enables the network to distinguish among different users and what each is authorized to do. Guest access can also be configured without compromising internal security. This means that users can be identified and either approved or denied at the edge of the network instead of in the core.

Criteria for enforcing RADIUS-based security for IDM applications includes classifiers such as:

- authorized user identity
- authorized device identity (MAC address)
- software running on the device
- physical location in the network
- time of day

Responses can be configured to support the networking requirements, user (SNMP) community, service needs, and access security level for a given client and device.

For more information on IDM, visit the ProCurve web site at http://www.procurve.com and click on **Products and Solutions**, then **Identity Driven Management** (under **Network Management**).

Clarifications and Updates

Operating Notes for Jumbo Traffic-Handling

In the Management and Configuration Guide, (Oct., 2005 version) on page 14-33 (page 347 of the .pdf file) where it states:

> When a port is not a member of any jumbo-enabled VLAN, it drops all jumbo traffic. If the port is receiving "excessive" inbound jumbo traffic, the port generates an Event Log message to notify you of this condition. This same condition generates a Fault-Finder message in the Alert log of the switch's web browswer interface, and also increments the switch's "Giant Rx" counter.

Note that it is the "Total Rx Errors" counter that is incremented, not the "Giant Rx" counter. On the 3400cl and 6400cl series switches, when the switch applies the jumbo MTU to a VLAN, all frames with jumbo MTU sizes (1523 to 9220 bytes) are incremented to "Total Rx Errors".

Non-Genuine Mini-GBIC Detection and Protection Initiative

Non-genuine ProCurve Transceivers and Mini-GBICs have been offered for sale in the marketplace. To protect customer networks from these unsupported products, ProCurve switch software includes the capability to detect and disable non-genuine transceivers and mini-GBICs discovered in Series 3400cl Switch ports. When a non-genuine device is discovered, the switch disables the port and generates an error message in the Event Log.

Publication Updates

Table 1 lists updates to the manual set dated January, 2005.

Table 1. Publication Updates for Manual Set Dated January, 2005

***Management and Configuration Guide for the 3400cl, 5300xl, & 6400cl Switches,* p/n 5990-6050, January 2005 Edition**	**Update**
Chapter 14: "Configuring for Network Management Applications" Pages 14-44 and 14-49	The **show lldp info stats** is an invalid command. The correct syntax is: **show lldp stats**.

IGMP Command Update

The following information updates and clarifies information in Chapter 4, "Multimedia Traffic Control with IP Multicast (IGMP)" in the *Advanced Traffic Management Guide*—part number 5990-6051, September 2004 edition. Please refer to this chapter for a detailed explanation of IGMP operation.

The 3400cl switches support the following standards and RFCs:

- RFC2236 (IGMP V.2, with backwards support for IGMP V.1)
- Interoperability with RFC3376 (IGMPv3)
- IETF draft for IGMP and MLD snooping switches (for IGMP V1, V2 V3)

The 3400cl switches:

- Provide full IGMPv2 support as well as full support for IGMPv1 Joins.
- Forward packets for the joined group from all sources, including IGMPv3 Joins.
- Do not support IGMPv3 "Exclude Source" or "Include Source" options in the Join Reports.
- Can operate in IGMPv2 Querier mode on VLANs with an IP address.

IGMP is supported in the HP MIB, rather than the standard IGMP MIBs, as the latter reduce Group Membership detail in switched environments.

Using Delayed Group Flush. This feature continues to filter IGMP groups for a specified additional period of time after IGMP leaves have been sent. The delay in flushing the group filter prevents unregistered traffic from being forwarded by the server during the delay period. In practice, this is rarely necessary on switches such as the Series 3400cl switches, which support data-driven IGMP. (Data-Driven IGMP, which is enabled by default, prunes off any unregistered streams detected on the switch.)

Syntax: igmp delayed-flush < *time period* >

Where leaves have been sent for IGMP groups, enables the switch to continue to flush the groups for a specified period of time (0 - 255 seconds). This command is applied globally to all IGMP-configured VLANs on the switch. A setting of **0** *(zero) disables the feature. (Default:* Disabled.)

Syntax: show igmp delayed-flush

Displays the current setting for the switch.

Setting Fast-Leave and Forced Fast-Leave from the CLI. In earlier switch models, including the 5300xl switches, fast-leave and forced fast-leave options for a port were configured with a lengthy **setmib** command. The following commands now allow a port to be configured for fast-leave or forced fast-leave operation with a conventional CLI command instead of the **setmib** command. Note that these commands must be executed in a VLAN context.

Syntax: [no] ip igmp fastleave < *port-list* >

Enables IGMP fast-leaves on the specified ports in the selected VLAN. In the Config context, use the VLAN specifier, for example, **vlan < *vid* > ip igmp fastleave < *port-list* >**. *The* **no** *form of the command disables IGMP fast-leave. (Default: Enabled)*

[no] ip igmp forcedfastleave < *port-list* >

Forces IGMP Fast-Leaves on the specified ports in the selected VLAN, even if they are cascaded. (Default: Disabled)

To view a non-default IGMP forced fast-leave configuration on a VLAN, use the **show running-config** command. (The **show running-config** output does not include forced fast-leave if it is set to the default of **0**.)

Note

In a future version of the 3400cl switch software, the **show running-config** command output will include any non-default fast-leave settings configured. However, this information is not included in the output for the M.08.53 software release.

IGMP Operating Notes.

- On the Series 3400cl switches, the delayed group flush feature offers little additional benefit over the IGMP data-driven feature (which is enabled by default).
- Forced fast-leave can be used when there are multiple devices attached to a port.

General Switch Traffic Security Guideline

Where the switch is running multiple security options, it implements network traffic security based on the OSI (Open Systems Interconnection model) precedence of the individual options, from the lowest to the highest. The following list shows the order in which the switch implements configured security features on traffic moving through a given port.

1. Disabled/Enabled physical port
2. MAC lockout (Applies to all ports on the switch.)
3. MAC lockdown

4. Port security
5. Authorized IP Managers
6. Application features at higher levels in the OSI model, such as SSH.

(The above list does not address the mutually exclusive relationship that exists among some security features.)

The Management VLAN IP Address

The optional Management VLAN, if used, must be configured with a manual IP address. It does not operate with DHCP/Bootp configured for the IP address.

Interoperating with 802.1s Multiple Spanning-Tree

The ProCurve implementation of Multiple Spanning-Tree (MSTP) complies with the IEEE 802.1s standard and interoperates with other devices running compliant versions of 802.1s. Note that the ProCurve Series 9300 routing switches do not offer 802.1s-compliant MSTP. Thus, to support a connection between a 9300 routing switch and a 3400cl switch running MSTP, configure the 9300 with either 802.1D (STP) or 802.1w (RSTP). For more information on this topic, refer to the chapter titled "Spanning-Tree Operation" in the *Advanced Traffic Management Guide* for your 3400cl switch. (To download switch documentation, refer to "Software Updates" on page 1.)

Rate-Limiting

The configured rate limit on a port reflects the permitted forwarding rate from the port to the switch fabric, and is visible as the *average* rate of the outbound traffic originating from the rate-limited port. (The most accurate rate-limiting is achieved when using standard 64-byte packet sizes.) Also, rate-limiting reflects the available percentage of a port's entire inbound bandwidth. The rate of inbound flow for traffic of a given priority and the rate of flow from a rate-limited port to a particular queue of an outbound port are not measures of the actual rate limit enforced on a port. Also, rate-limiting is byte-based and is applied to the available bandwidth on a port, and not to any specific applications running through the port. If the total bandwidth requested by all applications together is less than the available, configured maximum rate, then no rate-limit can be applied. This situation occurs with a number of popular throughput-testing software applications, as well as most regular network applications.

As a performance consideration, implementing rate-limiting in heavy traffic situations involving QoS, can affect overall performance. For more information on rate-limiting operation, refer to "Operating Notes for Rate-Limiting" in the chapter titled "Optimizing Traffic Flow with Port Controls, Port Trunking, and Filters" of the *Management and Configuration Guide* for your ProCurve Series 3400cl switch. (To download switch documentation, refer to "Software Updates" on page 1.)

Enhancements

Unless otherwise noted, each new release includes the enhancements added in all previous releases.

Enhancments are listed in chronological order, oldest to newest software release. To review the list of enhancements included since the last general release that was published, begin with "Release M.08.103" on page 42.

Release M.08.69 Enhancements

Release M.08.69 included the following enhancements:

- Support for Web RADIUS authentication with CLI.
- A new scripting mode.
- Source Port Filter user interface, described in Chapter 9. "Traffic/Security Filters" in the *Access Security Guide* for the switch.

Information on these features is included in the current documentation for the switch, available on the web at: **http://www.hp.com/rnd/support/manuals/**.

Release M.08.70 through M.08.72 Enhancements

Software fixes only; no new enhancements.

Release M.08.73 Enhancements

Release M.08.73 included the following enhancements:

- Support for the new I.08.07 Boot ROM version.
  (The 2800/3400/6400 series switches all share the same ROM code)

Release M.08.74 through M.08.77 Enhancements

Software fixes only; no new enhancements.

Release M.08.78 Enhancements

Using Fastboot To Reduce Boot Time

The **fastboot** command allows a boot sequence that skips the internal power-on self-tests, resulting in a faster boot time.

Syntax: [no] fastboot

Used in the global configuration mode to enable the fastboot option. The **no** *version of the command disables* **fastboot** *operation.*

Syntax: show fastboot

Shows the status of the fastboot feature, either enabled or disabled.

For example:

```
ProCurve(config)# show fastboot

    Fast Boot:  Disabled
```

Release M.08.79 Enhancements

CLI Port Rate Display

Beginning with release M.08.79 the CLI "show interface [port list]" command includes the port rate in the display. The rate displayed is the average for a period of 5 minutes, given in bps for 1G ports, or in Kbps for 10G ports. You can also use the CLI command: **show interface port-utilization** to display port-rate over a period of 5 minutes.

The following shows a sample output from this new command.

```
ProCurve# show interface port-utilization

 Port  Mode     |             Rx                          Tx
              |  -------  -------   ------   -------  ------   ------
              |  KBits/s  Pkts/s    Util     KBits/s  Pkts/s   Util
 ----  ----     +  -------  -------   ------   -------  ------   ------
 1     100FDx   |   100000       525       12   100000      400       10
 2     1000FDx  |        0         0        0        0        0        0
 3     100FDx   |      536        44    00.53      504        0    00.50
 4     1000FDx  |        0         0        0        0        0        0
 5     1000FDx  |        0         0        0        0        0        0
 6     1000FDx  |        0         0        0        0        0        0
 7     1000FDx  |        0         5        0        0        0        0
 8     1000FDx  |        0         5        0        0        0        0
 9     100FDx   |        0        30        0        0        0        0
```

Figure 2. Example rate display output for ports

Operating Notes

- For each port on the switch, the command provides a real-time display of the rate at which data is received (Rx) and transmitted (Tx) in terms of kilobits per second (KBits/s), number of packets per second (Pkts/s), and utilization (Util) expressed as a percentage of the total bandwidth available.
- As in previous software versions, the **show interfaces** <port-list> command can be used to display the current link status and the port rate average over a 5 minute period. Port rates are shown in bits per second (bps) for ports up to 1 Gigabit, and are shown in kilobits per second (Kbps) for 10 Gigabit ports.

Release M.08.80 through M.08.83 Enhancements

Software fixes only; no new enhancements.

Release M.08.84 Enhancements

Release M.08.84 includes the following enhancement:

Added the `show tech transceivers` command to allow removable transceiver serial numbers to be read without removal of the transceivers from the switch. :

Release M.08.85 through M.08.88 Enhancements

Software fixes only; no new enhancements.

Release M.08.89 Enhancements

Release M.08.89 includes the following enhancements:

- DNS Resolver for using DNS names for Ping and Traceroute
- RADIUS Configuration via SNMP (see "Using SNMP To View and Configure Switch Authentication Features" on page 32)

DNS Resolver

The Domain Name System (DNS) resolver is designed for use in local network domains where it enables use of a host name or fully qualified domain name to perform **ping** and **traceroute** operations from the switch.

Terminology

Domain Suffix — Includes all labels to the right of the unique host name in a fully qualified domain name assigned to an IP address. For example, in the fully qualified domain name "device53.evergreen.trees.org", the domain suffix is "evergreen.trees.org", while "device53" is the unique (host) name assigned to a specific IP address.

Fully Qualified Domain Name — The sequence of labels in a domain name identifying a specific host (host name) and the domain in which it exists. For example, if a device with an IP address of 10.10.10.101 has a host name of *device53* and resides in the *evergreen.trees.org* domain, then the device's fully qualified domain name is *device53.evergreen.trees.org* and the DNS resolution of this name is 10.10.10.101.

Host Name — The unique, leftmost label in a domain name assigned to a specific IP address in a DNS server configuration. This enables the server to distinguish a device using that IP address from other devices in the same domain. For example, in the *evergreen.trees.org* domain, if an

IP address of 10.10.100.27 is assigned a host name of *accounts015* and another IP address of 10.10.100.33 is assigned a host name of *sales021*, then the switch configured with the domain suffix *evergreen.trees.org* and a DNS server that resolves addresses in that domain can use the host names to reach the devices with **ping** and **traceroute** commands:

```
ping accounts015
traceroute sales021
```

Basic Operation

- When the switch is configured with only the IP address of a DNS server available to the switch, then a **ping** or **traceroute** command, executed with a fully qualified domain name, can reach a device found in any domain accessible through the configured DNS server.
- When the switch is configured with both of the following:
  - the IP address of a DNS server available to the switch
  - the domain suffix of a domain available to the configured DNS server

  then:
  - A **ping** or **traceroute** command that includes the host name of a device in the same domain as the configured domain suffix can reach that device.
  - A **ping** or **traceroute** command that includes a fully qualified domain name can reach a device in any domain that is available to the configured DNS server.

Example. Suppose the switch is configured with the domain suffix **mygroup.procurve.net** and the IP address for an accessible DNS server. If an operator wants to use the switch to ping a host using the DNS name "leader" assigned to an IP address used in that domain, then the operator can use either of the following commands:

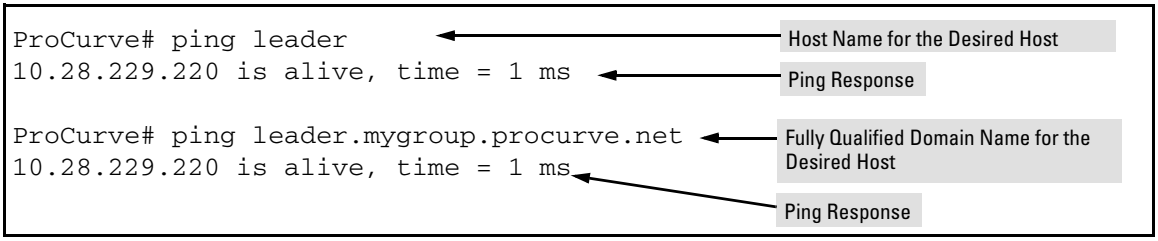

Figure 3. Example of Using Either a Host Name or a Fully Qualified Domain Name

In the preceeding example, if the DNS server's IP address is configured on the switch, but a domain suffix is not configured, then the fully qualified domain name *must* be used.

Note that if the target host is in a domain *other than* the domain configured on the switch, then:

- The host's domain must be reachable from the switch. This requires that the DNS server for the switch must be able to communicate with the DNS server(s) in the path to the domain in which the target host operates.
- The fully qualified domain name must be used, and the domain suffix must correspond to the domain in which the target host operates, regardless of the domain suffix configured in the switch.

Example. Suppose the switch is configured with the domain suffix **mygroup.procurve.net** and the IP address for an accessible DNS server. This time, the operator wants to use the switch to trace the route to a host named "remote-01" in another domain named **common.group.net**. As long as this domain is accessible to the DNS server configured on the switch, a **traceroute** command using the target's fully qualified DNS name should succeed.

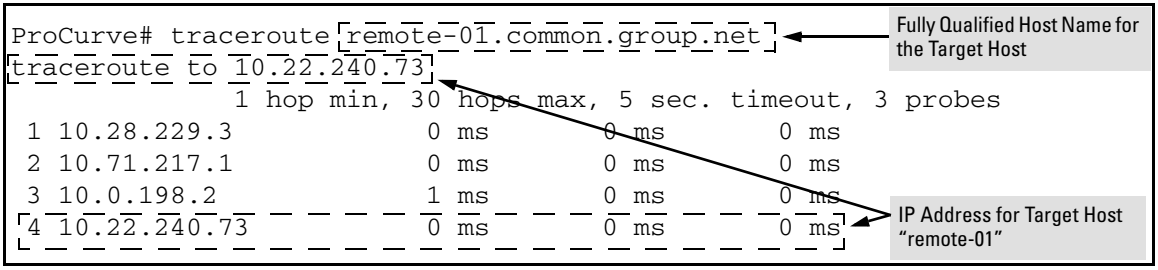

Figure 4. Example Using the Fully Qualified Domain Name for an Accessible Target in Another Domain

Configuring and Using DNS Resolution with Ping and Traceroute Commands

1. Determine the following:
   a. the IP address for a DNS server operating in a domain in your network
   b. the domain name for an accessible domain in which there are hosts you want to reach with **ping** and/or **traceroute** commands. (This is the domain suffix in the fully qualified domain name for a given host operating in the selected domain. Refer to "Terminology" on page 25.) Note that if a domain suffix is not configured, fully qualified domain names can be used to resolve **ping** and **traceroute** commands.
   c. the host names assigned to target IP addresses in the DNS server for the specified domain
2. Use the data from steps 1a and 1b to configure the DNS entry on the switch.
3. Use either **ping** or **traceroute** with the host names for the target devices whose connectivity you are testing or troubleshooting.

Configuring a DNS Entry

The switch allows one DNS server entry, which includes the DNS server IP address and the chosen domain name suffix. Configuring the entry enables the use of **ping** and **traceroute** with a target's host name instead of the target's IP address.

Syntax: [no] ip dns server-address < *ip-addr* >

Configures the IP address of a DNS server accessible to the switch. This setting identifies the server to use for DNS resolution to the target IP address, and must be configured before **ping** *or* **traceroute** *can be executed with host name criteria.*

The switch supports one DNS server entry. Configuring another IP address for this value replaces the current IP address with the new one.

The **no** *form of the command replaces the configured IP address with the null setting, which disables host name resolution. (Default: null)*

Syntax: [no] ip dns domain-name < *domain-name-suffix* >

Configures the domain suffix that is automatically appended to the host name entered with the **ping** *or* **traceroute** *command. When the domain suffix and the DNS server IP address are both configured on the switch, you can execute* **ping** *and* **traceroute** *with only the host name of the desired target within the domain. In either of the following two instances, you must manually provide the domain identification by using a fully qualified DNS name with each* **ping** *and* **traceroute** *command:*

- *If the DNS server IP address is configured on the switch, but the domain suffix is not configured (null)*
- *The domain suffix configured on the switch is not the domain in which the target host exists*

The switch supports one domain suffix entry. Configuring a new entry for this value replaces the current suffix.

The **no** *form of the command replaces the configured domain suffix with the null setting. (Default: null)*

Example Using DNS Names with Ping and Traceroute

In the network illustrated in figure figure 5, the switch at 10.28.192.1 is configured to use DNS names for **ping** and **traceroute** in the *pubs.outdoors.com* domain. The DNS server has been configured to assign the host name *docservr* to the IP address used by the document server (10.28.229.219).

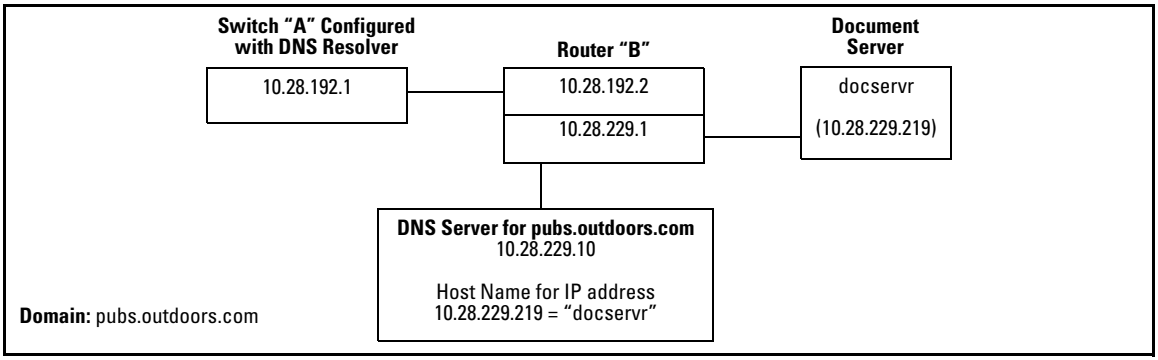

Figure 5. Example Network Domain

Configuring switch "A" with the domain name and the IP address of a DNS server for the domain enables the switch to use host names assigned to IP addresses in the domain to perform **ping** and **traceroute** actions on the devices in the domain. To summarize:

Entity:	Identity:
DNS Server IP Address	10.28.229.10
Domain Name (and Domain Suffix for Hosts in the Domain)	pubs.outdoors.com
Host Name Assigned to 10.28.229.219 by the DNS Server	docservr
Fully Qualified Domain Name for the IP address Used By the Document Server (10.28.229.219)	docservr.pubs.outdoors.com
Switch IP Address	10.28.192.1
Document Server IP Address	10.28.229.219

With the above already configured, the following commands enable **ping** and **traceroute** with the host name **docserver** to reach the document server at 10.28.229.219.

```
ProCurve(config)# ip dns server-address 10.28.229.10
ProCurve(config)# ip dns domain-name pubs.outdoors.com
```

Figure 6. Configuring Switch "A" in Figure figure 5 To Support DNS Resolution

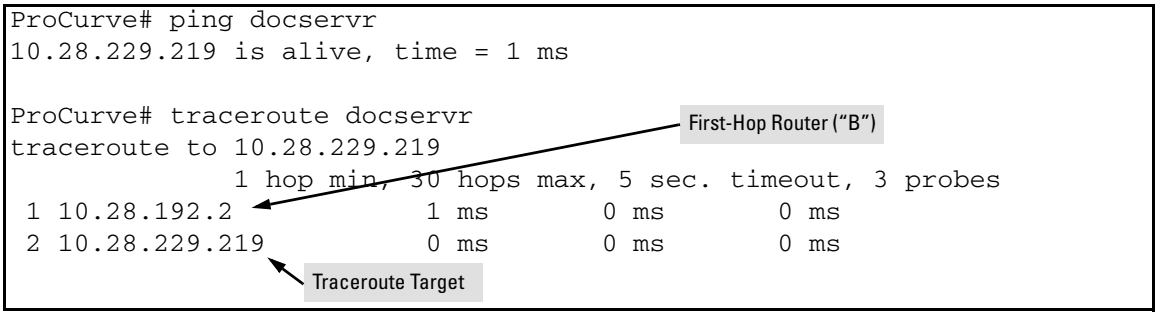

Figure 7. Example of Ping and Traceroute Execution for the Network in Figure figure 5 on Page 29

As mentioned under "Basic Operation" on page 26, if the DNS entry configured in the switch includes only the DNS server's IP address, you must use the target host's fully qualified domain name with **ping** and **traceroute**. For example, using the document server in figure figure 5 as a target:

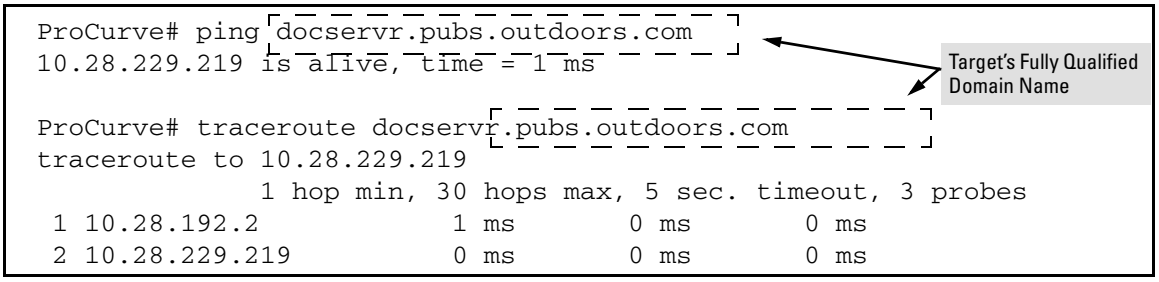

Figure 8. Example of Ping and Traceroute Execution When Only the DNS Server IP Address Is Configured

Viewing the Current DNS Configuration

The **show ip** command displays the current DNS configuration along with other IP configuration information. If the switch configuration currently includes a nondefault (non-null) DNS entry, it will also appear in the **show run** command output.

```
ProCurve# show ip

 Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 10.28.192.2
  Default TTL     : 64
  Arp Age         : 20
  Domain Suffix   : pubs.outdoors.com
  DNS server      : 10.28.229.10

  VLAN         | IP Config  IP Address       Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | Manual     10.28.192.1     255.255.255.0
```

DNS Resolver Configuration in the **show ip** command output

Figure 9. Example of Viewing the Current DNS Configuration

Operating Notes

- The DNS server must be accessible to the switch, but it is not necessary for any intermediate devices between the switch and the DNS server to be configured to support DNS operation.
- A DNS configuration must include the IP address for a DNS server that is able to resolve host names for the desired domain. If a DNS server has limited knowledge of other domains, then its ability to resolve **ping** or **traceroute** requests is also limited.
- If the DNS configuration includes a DNS server IP address but does not also include a domain suffix, then any ping or traceroute command should include the target host's fully qualified domain name. Refer to figure figure 3 on page 26.
- The switch supports one DNS entry; that is, one DNS server IP address and the corresponding domain name suffix.
- Switch-Initiated DNS packets go out through the VLAN having the best route to the DNS server, even if a Management VLAN has been configured.
- The **traceroute** command output shows only IP addresses.
- The DNS server address must be manually input. It is not be automatically determined via DHCP.
- Operation with IPv4 DNS servers has been verified and, while no problems with servers supporting both IPv4 and IPv6 addresses are expected, testing has not been performed with such servers. (IPv6 AAAA-style queries are not supported.)

Event Log Messages

Message	Meaning
DNS server address not configured	The switch does not have an IP address configured for the DNS server.
DNS server not responding	The DNS server failed to respond or is unreachable. An incorrect server IP address can produce this result.
Unknown host < *host-name* >	The host name did not resolve to an IP address. Some reasons for this occurring include: • The host name was not found. • The named domain was not found. • The domain suffix was expected, but has not been configured. (If the server's IP address has been configured in the switch but the domain name has not been configured, then the host's fully qualified domain name must be used.)

Using SNMP To View and Configure Switch Authentication Features

In earlier software releases, SNMP MIB object access has not been available for switch authentication configuration (hpSwitchAuth) features. Beginning with software release M.08.89, the 3400cl and 6400cl switches allow, by default, manager-only SNMP read/write access to a subset of the authentication MIB objects for the following features:

- number of primary and secondary login and enable attempts
- TACACS+ server configuration and status
- RADIUS server configuration
- selected 802.1X settings
- key management subsystem chain configuration
- key management subsystem key configuration
- OSPF interface authentication configuration

With SNMP access to the hpSwitchAuth MIB enabled, a device with management access to the switch can view the configuration for the authentication features listed above (excluding passwords and keys). Using SNMP sets, a management device can change the authentication configuration (*including* changes to passwords and keys). Operator read/write access to the authentication MIB is always denied.

Security Notes

Passwords and keys configured in the hpSwitchAuth MIB are not returned via SNMP, and the response to SNMP queries for such information is a null string. However, SNMP sets can be used to configure password and key MIB objects.

To help prevent unauthorized access to the switch's authentication MIB, ProCurve recommends enhancing security according to the guidelines under "Enforcing Switch Security" on page 8.

If you do not want to use SNMP access to the switch's authentication configuration MIB, then you should use the **snmp-server mib hpswitchauthmib excluded** command to disable this access, as described in the next section.

If you choose to leave SNMP access to the security MIB open (the default setting), ProCurve recommends that you configure the switch with the SNMP version 3 management and access security feature, and disable SNMP version 2c access. (Refer to "Enforcing Switch Security" on page 8.)

Changing and Viewing the SNMP Access Configuration

Syntax: snmp-server mib hpswitchauthmib < excluded | included >

included: *Enables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB.*
excluded: *Disables manager-level SNMP read/write access to the switch's authentication configuration (hpSwitchAuth) MIB.*
(Default: **included** *)*

Syntax: show snmp-server

The output for this command has been enhanced to display the current access status of the switch's authentication configuration MIB in the **Excluded MIBs** *field.*

For example, to disable SNMP access to the switch's authentication MIB and then display the result in the Excluded MIB field, you would execute the following two commands.

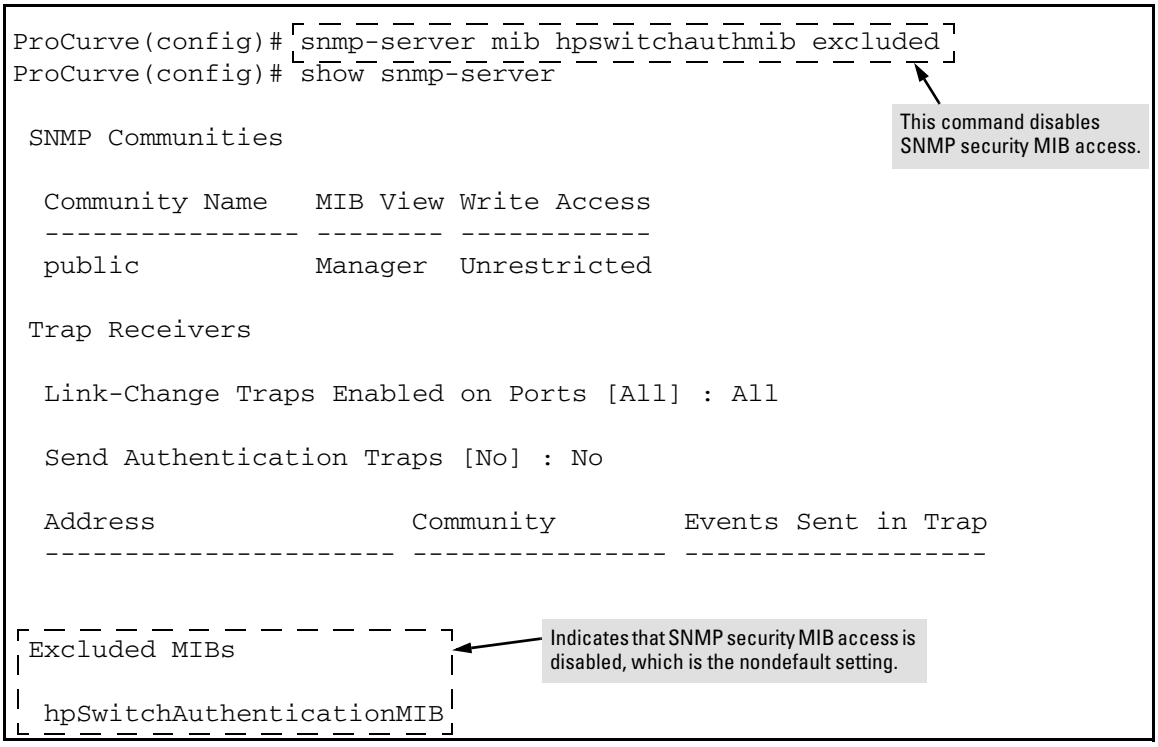

Figure 10. Disabling SNMP Access to the Authentication MIB and Displaying the Result

An alternate method of determining the current Authentication MIB access state is to use the **show run** command.

```
ProCurve(config)# show run

Running configuration:

; J4905A Configuration Editor; Created on release #M.10.05

hostname "ProCurve"
snmp-server mib hpSwitchAuthMIB excluded
ip default-gateway 10.10.24.55
snmp-server community "public" Operator
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-26
   ip address 10.10.24.100 255.255.255.0
   exit
password manager
```

Indicates that SNMP access to the authentication configuration MIB (hpSwitchAuth) is disabled.

Figure 11. Using the show run Command to View the Current Authentication MIB Access State

Releases M.08.90 and M.08.91

Releases M.08.90 and M.08.91 include the following enhancements:

- The MSTP enhancement implementing the CLI command for spanning-tree legacy-path-cost was included in releaseM.08.90
- The MSTP enhancement implementing the CLI command for spanning-tree legacy-mode was included in release M.08.91
- QoS Pass-Through Mode enhancement, a new command that allows the configuration of the Quality of Service (QoS) queues to be selected.

MSTP Default Path Cost Controls

Summary: 802.1D and 802.1t specify different default path-cost values (based on interface speed). These are used if the user hasn't configured a "custom" path-cost for the interface. The default of this toggle is to use 802.1t values. The reason one might set this control to 802.1D would be for better interoperability with legacy 802.1D STP (Spanning Tree Protocol) bridges.

To support legacy STP bridges, the following commands (options) have been added to CLI:

spanning-tree legacy-path-cost – Use 802.1D values for default path-cost

no spanning-tree legacy-path-cost – Use 802.1t values for default path-cost (default setting)

The “legacy-path-cost” CLI command does not affect or replace functionality of the “spanning-tree force-version” command. The “spanning-tree force-version” controls whether MSTP will send and process 802.1w RSTP, or 802.1D STP BPDUs. Regardless of what the “legacy-path-cost” parameter is set to, MSTP will interoperate with legacy STP bridges (send/receive Config and TCN BPDUs).

spanning-tree legacy-mode - A “macro” that is the equivalent of executing the “spanning-tree legacy-path-cost” and “spanning-tree force-version stp-compatible” commands.

no spanning-tree legacy-mode - A “macro” that is the equivalent of executing the “no spanning-tree legacy-path-cost” and “spanning-tree force-version mstp-compatible” commands.

When either legacy-mode or legacy-path-cost control is toggled, all default path costs will be recalculated to correspond to the new setting, and spanning tree is recalculated if needed.

QoS Pass-Through Mode

Release M.08.91 introduced a new command that allows the configuration of the Quality of Service (QoS) queues to be selected. By better matching the configuration of the QoS queues to the amount of prioritized and non-prioritized traffic being transferred, performance can be improved and packet loss due to over-subscription can be minimized.

In previous software versions, the 3400cl and the 6400cl switches had four QoS queues of equal size. Depending on the mix of prioritized and non-prioritized traffic, this configuration might not always optimize performance and could result in dropped packets when resources were over-subscribed. Starting with this software version, four QoS Pass-Through modes are available for use. The number of queues and the size of the memory buffer used by each queue differs in each mode. Table 2 below summarizes the QoS queue configuration of each mode

Table 2. QoS Pass-Through Modes

QoS Pass-Through Mode	Number of Queues	QoS Queue Memory Buffer Configuration	Description
typical (default)	4	One large queue for Priority 0 and 3 traffic and three other queues for the remaining traffic.	A mix of prioritized and non-prioritized traffic. This is the default mode, used when QoS Pass-Through is disabled.
balanced	4	All queues are the same size.	Equal amounts of prioritized and non-prioritized traffic. This is the same mode used in pre-M.08.78 software versions.
one-queue	1	One large queue.[1]	No traffic is prioritized.
optimized	2	One small queue for Priority 6 and 7 traffic; one large queue for all other traffic.	Most traffic is not prioritized.

[1]This mode has a small queue used exclusively for Priority 7 management and control traffic.

Note

Changing the QoS Pass-Through Mode can be done without rebooting the switch. However, the switch ports are toggled down and back up, allowing the QoS queues to be reconfigured. This may affect routing and spanning tree operation. ProCurve Networking recommends that QoS queues be reconfigured during periods of non-peak traffic.

Configuring QoS Pass-Through Mode

Syntax: qos-passthrough-mode [balanced | one-queue | optimized | typical]

Specifies the QoS queue mode to be used by the switch. The number of queues and the size of each queue is determined by the mode selected. If no mode is specified the **optimized** *mode is used. QoS Pass-Through is disabled using the* **no qos-pass-through** *command.*

balanced: *Configures four QoS queues of the same size. This configuration is the same as was used by software versions prior to M.08.78.*

one-queue: *Configures one QoS queue. By consolidating packet buffer memory, line-rate flows with no loss of data may be achieved.*

Note: *This mode has a small queue used exclusively by Priority 7 management and control packets.*

optimized: *Configures two QoS queues: a small queue for Priority 6 and 7 traffic and a large queue for all other traffic.*

typical: *Configures four QoS queues: a large queue for Priority 0 and 3 traffic, and three other queues for the remaining traffic. This is the default configuration on the switch and is used when QoS Pass-Through is disabled.*

Syntax: [no] qos-passthrough-mode

Specifies the **optimized** *QoS queue mode for the switch.*

The **no qos-pass-through** *command returns the QoS queue mode to* **typical**, *the default setting.*

Configuring QoS Pass-Through Mode Through the CLI. The following example changes the QoS Pass-Through Mode to **balanced**. A **show** command verifies the new mode.

```
ProCurve(config)# qos-passthrough-mode balanced
This requires a temporary shut-down of logical ports. Continue (y/n) y
ProCurve(config)# show qos-passthrough-mode

  Qos passthrough mode : balanced

ProCurve(config)#
```

Reconfiguring the QoS queues toggles the switch ports, which may affect routing and spanning tree operation. Choose **n** to cancel this operation.

Figure 1. Example Showing QoS Pass-Through Mode Set Using the CLI

QoS Pass-Through Mode SNMP MIB Object. A read-write MIB object, 1.3.6.1.4.1.11.2.14.11.5.1.7.1.24.1, has been added to the ProCurve switch MIB. The QoS Pass-Through Mode can be changed using either an SNMP network management application or the CLI **setmib** command.

Syntax: setMIB hpSwitchQosPassThroughModeConfig.0 -i [1 | 2 | 3 | 4]

Specifies the QoS queue mode to be used by the switch. The number of queues and the size of each queue is determined by the mode selected.

- **1** **optimized:** *Configures two QoS queues: a small queue for Priority 6 and 7 traffic and a large queue for all other traffic.*
- **2** **typical:** *Configures four QoS queues: a large queue for Priority 0 and 3 traffic, and three other queues for the remaining traffic. This is the default configuration on the switch and is used when QoS Pass-Through is disabled.*
- **3** **balanced:** *Configures four QoS queues of the same size. This configuration is the same as was used by software versions prior to M.08.xx.*
- **4** **one-queue:** *Configures one QoS queue. By consolidating packet buffer memory, line-rate flows with no loss of data may be achieved.*
  Note: *This mode has a small queue used exclusively by Priority 7 management and control packets.*

The following example changes the QoS Pass-Through Mode to **one-queue**. A **show** command verifies the new mode.

```
ProCurve(config)# setMIB hpSwitchQosPassThroughModeConfig.0 -i 4
hpSwitchQosPassThroughModeConfig.0 = 4
ProCurve(config)# show qos-passthrough-mode

  Qos passthrough mode : one-queue

ProCurve(config)#
```

Figure 2. Example Showing QoS Pass-Through Mode Set Using the setMIB Command

Displaying the Current QoS Pass-Through Mode on the Switch

The following command indicates the current QoS Pass-Through Mode on the switch.

Syntax: show qos-passthrough-mode

This command displays the current QoS Pass-Through Mode configured on the switch. The default mode is **typical**.

The current QoS Pass-Through Mode also is displayed in the **show running-config** command output.

Operating Notes

- To use the same QoS queue structure used in pre-M.08.78 software, set the QoS Pass-Through Mode to **balanced**.
- The **optimized** mode matches the QoS Pass-through mode on the ProCurve Series 2800 switches. This mode is used when the QoS Pass-Through Mode command is entered with no arguments, **qos-passthrough-mode**.

Release M.08.94

Release M.08.94 includes the following enhancements:

- Added DHCP Option 82 functionality for 3400cl series.
- UDP broadcast forwarding feature is now supported on the 3400cl series.

DHCP Option 82: Using the Management VLAN IP Address for the Remote ID

This section describes the Management VLAN enhancement to the DHCP option 82 feature. For more information on DHCP option 82 operation, refer to "Configuring DHCP Relay" in the chapter titled "IP Routing Features" in the *Advanced Traffic Management Guide*.

When the routing switch is used as a DHCP relay agent with Option 82 enabled, it inserts a relay agent information option into client-originated DHCP packets being forwarded to a DHCP server. The option automatically includes two suboptions:

- Circuit ID: the identity of the port through which the DHCP request entered the relay agent
- Remote ID: the identity (IP address) of the DHCP relay agent

Using earlier software releases, the remote ID can be either the routing switch's MAC address (the default option) or the IP address of the VLAN or subnet on which the client DHCP request was received. Beginning with software release M.08.xx, if a Management VLAN is configured on the routing switch, then the Management VLAN IP address can be used as the remote ID.

Syntax: dhcp-relay option 82 < append | replace | drop > [validate] [ip | mac | mgmt-vlan]

[ip | mac | mgmt-vlan] : *Specifies the remote ID suboption the routing switch will use in Option 82 fields added or appended to DHCP client packets. The choice depends on how you want to define DHCP policy areas in the client requests sent to the DHCP server. If a remote ID suboption is not configured, then the routing switch defaults to the* **mac** *option.*

mgmt-vlan: *Specifies the IP address of the (optional) Management VLAN configured on the routing switch. Requires that a Management VLAN is already configured on the switch. If the Management VLAN is multinetted, then the primary IP address configured for the Management VLAN is used for the remote ID.*

ip: *Specifies the IP address of the VLAN on which the client DHCP packet enters the routing switch. In the case of a multinetted VLAN, the remote ID suboption uses the IP address of the subnet on which the client request packet is received.*

mac: *Specifies the routing switch's MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.)*

(Default: **mac***)*

Example

In the routing switch shown below, option 82 has been configured with **mgmt-vlan** for the Remote ID.

```
ProCurve(config)# dhcp-relay option 82 append mgmt-vlan
```

The resulting effect on DHCP operation for clients X, Y, and Z is shown in table 3.

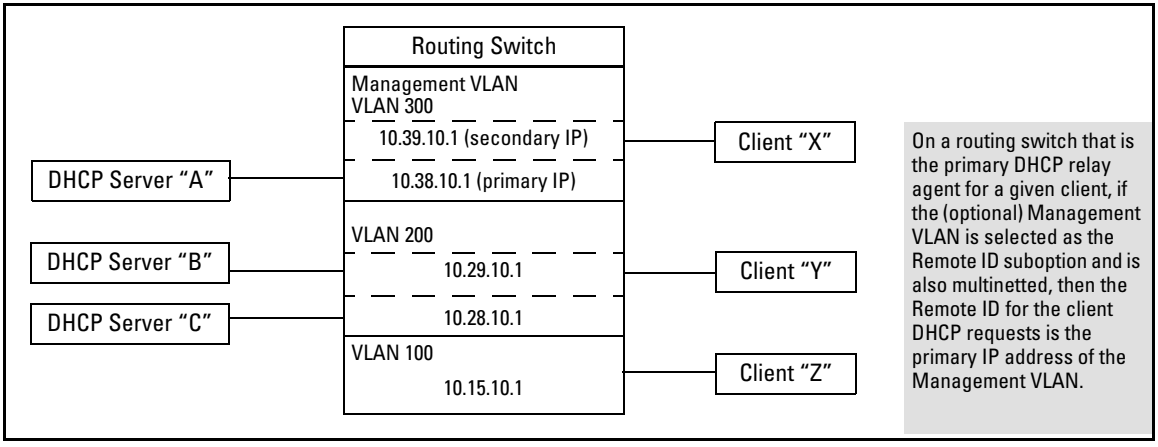

Figure 12. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption

Table 3. DHCP Operation for the Topology in Figure 12

Client	Remote ID	giaddr*	DHCP Server	
X	10.38.10.1	10.39.10.1	A only	If a DHCP client is in the Management VLAN, then its DHCP requests can go only to a DHCP server that is also in the Management VLAN. Routing to other VLANs is not allowed.
Y	10.38.10.1	10.29.10.1	B or C	Clients outside of the Management VLAN can send DHCP requests only to DHCP servers outside of the Management VLAN. Routing to the Management VLAN is not allowed.
Z	10.38.10.1	10.15.10.1	B or C	

*The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (*gateway interface address*). This is the IP address of the VLAN on which the request packet was received from the client. For more information, refer to RFC 2131 and RFC 3046.

Operating Notes

- Routing is not allowed between the Management VLAN and other VLANs. Thus, a DHCP server must be available in the Management VLAN if there are clients in the Management VLAN that require a DHCP server.
- If the Management VLAN IP address configuration changes after **mgmt-vlan** has been configured as the remote ID suboption, the routing switch dynamically adjusts to the new IP addressing for all future DHCP requests.
- The Management VLAN and all other VLANs on the routing switch use the same MAC address.

UDP Broadcast Forwarding

Beginning with software release M.08.94, UDP Broadcast Forwarding is available on the ProCurve 3400cl and 6400cl switches. For further information, refer to the section titled "UDP Broadcast Forwarding on 5300xl Switches" in the "IP Routing Features" chapter of the *Advanced Traffic Management Guide* for your switch. (Note that this manual covers multiple switches and the description of UDP Broadcast Forwarding is no longer restricted to just the 5300xl switches.)

Some applications rely on client requests sent as limited IP broadcasts addressed to a UDP application port. If a server for the application receives such a broadcast, the server can reply to the client. Since typical router behavior, by default, does not allow broadcast forwarding, a client's UDP broadcast requests cannot reach a target server on a different subnet unless the router is configured to forward client UDP broadcasts to that server.

A switch with routing enabled includes optional per-VLAN UDP broadcast forwarding that allows up to 256 server and/or subnet entries on the switch (16 entries per-VLAN). If an entry for a particular UDP port number is configured on a VLAN and an inbound UDP broadcast packet with that port number is received on the VLAN, then the switch routes the packet to the appropriate subnet. (Each entry can designate either a single device or a single subnet. The switch ignores any entry that designates multiple subnets.)

Releases M.08.95 through M.08.101

Software fixes only; no new enhancements in version M.08.95.

Software versions M.08.96 through M.08.98 for the 6400cl series switches were never built.

Software fixes only; no new enhancements in version M.08.99, after which the code for the 6400cl series switches branched to M.08.101.

Software fixes only, no new enhancements for version M.08.101

Release M.08.102

Release M.08.102 includes the following enhancements:

- Added support for the J8440B 10-GbE X2-CX4 Transceiver.

Release M.08.103

Release M.08.103 includes the following enhancements:

- Added support for PIM Dense Mode. For details, refer to Chapter 5, "PIM-DM (Dense Mode) on the 5300xl Switches" in the *Advanced Traffic Management Guide for the ProCurve Series 6400cl/5300xl/4200vl/3400cl Switches.*

Releases M.08.104 through M.08.106

Software fixes only, no new enhancements.

Release M.08.107

Release M.08.107 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_1000335860) - This enhancement provides a configuration option for the source IP address field of SNMP response and generated trap PDUs.
- Enhancement (PR_1000376626) - Enhanced CLI "qos dscp-map he" help and "show dscp-map" text to warn user that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.

Software Fixes in Release M.08.51 - M.08.10*x*

Software fixes are listed in chronological order, oldest to newest. To review the list of fixes included since the last general release that was published, go to "Release M.08.103" on page 55.

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

Release M.08.62 was the first software release for the ProCurve 6400cl Series.

Release M.08.63

Problems Resolved in Release M.08.63 (Not a general release)

- **Crash (PR_1000205768)** — A **null** System Name in the Web user interface may crash the switch with a message similar to:

  ```
  "Software exception at lldpSysNameTlv.c:251 -- in 'mlldpCtrl', task ID
  = 0x12dc88 -> ASSERT: failed".
  ```

- **Web UI (PR_93721)** — The web user interface Status screen does not display all ports, and the scroll bar does not work.
- **Web UI (PR_1000191635)** — The Port column may not be sorted correctly in all Web user interface screens.
- **XRRP (PR_1000217651)** — Running different XRRP versions causes excessive event log messages like:

  ```
  Rcvd a pkt with version number 2, expected 1
  ```

  ```
  Remote rtr 2 domain 2 is miss-configured.
  ```

- **Crash (PR_1000217354)** — Bus error in **mSnmpCtrl** task when adding a less-specific route and adding it again through the CLI.

Release M.08.64

Problems Resolved in Release M.08.64 (Not a general release)

- **IP Routing (PR_1000220668)**— Fatal exception when routing with more than 8 trunks configured and IP routing enabled.

Release M.08.65

Problems Resolved in Release M.08.65 (Never released)

- **Crash (PR_1000194486)** — The switch may crash with a message similar to:

  ```
  Software exception at bcm 1 CpuLearn.c:1308.
  ```

- **Counters (PR_1000221089)** — The 64 bit counters may not always be correct.
- **Counters (PR_1000219548)** — Collision counters do not increment accurately.

Release M.08.66

Problems Resolved in Release M.08.66 (Not a general release)

- **PPMGR (PR_1000225645)**— The ProCurve 10GbE X2-SC SR Optic (J8436A) transceiver fails self test on boot up when installed in slot B/8.

Release M.08.67

Problems Resolved in Release M.08.67 (Not a general release)

- **Authentication (PR_1000217338)** — Inconsistent authentication results with EAP-TLS and EAP-PEAP authorization types.
- **Config (PR_1000207697)** — Loading a startup-configuration file fails when attempting to declare a VLAN in the configuration file as a management VLAN, and the VLAN does not currently exist on the switch. The switch indicates the downloaded file as being corrupted, listing the `vid` of the specified management VLAN as not being found.
- **RSTP (PR_99049)** — Switch does not detect and block network topology loops on a single port. For example, the port connects to a hub that has a loop or the port connects to an inactive node via IBM 'Type 1' cable.
- **Web UI (PR_1000214188)** — The scroll bar does not display or respond correctly after resizing a window.

Release M.08.68

Problems Resolved in Release M.08.68 (Not a general release)

- **Switching (PR_1000232312)** — In cases where traffic is being L2 switched or L3 routed from one port at Gigabit speeds to a group of ports (i.e. to a VLAN) where one of the outbound ports is running at a slower speed, traffic may have been dropped even to egress ports running at Gigabit speeds. This PR addresses the dropped packets for the Gig-to-Gig port traffic. Gig-to-100Mbps transfers may still experience packet drops due to congestion (as is normal in any oversubscribed scenario).

Release M.08.69

Problems Resolved in Release M.08.69

- **802.1s STP (PR_1000229407) -** Edge port configuration is lost after the configuration file is transferred using TFTP.
- **802.1X (PR_1000208530)** - Switch may crash with 802.1X configured, with a message similar to:

  ```
  Crash: aaa8021x_init dereferencing a null pointer, writing to low
  memory
  ```

- **CLI (PR1000202435)** — "show config" does not show IGMP fast-leave configuration.
- **Config (PR_94943)** — Setup Screen allows Proxy-ARP configuration when IP routing is disabled
- **Config (PR1000216051)** — Copying a previously saved startup-configuration with "stack join (mac address)" to a member switch of the IP stack will break the membership of that stack.
- **Crash (PR_1000229656)** - switch crashes when RADIUS is unavailable.
- **Crash (PR_1000233993)** - Switch may crash with a message similar to:

  ```
  Software exception at exception.c:373 -- in 'mSnmpCtrl', task ID =
  0x5b85fd0 -> Memory system error.
  ```

- **Crash (PR_1000239085) -** The switch may crash with a message similar to:

  ```
  Software exception at esi_stacking.c:2578 -- in 'tHttpd'.
  ```

- **DHCP (PR1000207419)** — DHCP Relay agent is disabled by default.
- **IP Helper/DHCP Relay (PR_1000197046)** - IP helper may not handle "DHCP Inform" relay properly.
- **Menu (PR_1000221018)** - Setup Menu allows Proxy-ARP configuration when IP routing is disabled.
- **Port Security (PR_1000203984)** — CLI port-security "mac-address" command will save address above the limit.
- **SNMP (PR_1000212170) —** The Switch transmits Warm and Cold Start traps with an agent address of 0.0.0.0.
- **Spanning Tree (PR_1000214598)** - The switch will not accept the spanning-tree 1 mode fast command within the CLI.
- **System Hang (PR_1000200341)** - Added an exception handler to prevent a case where the system may hang.

- **XRRP (PR_1000217922)** — XRRP router may fail back to the XRRP peer router even with Infinite Failback enabled.

Release M.08.70

Problems Resolved in Release M.08.70 (Not a general release)

- **ACL (PR_1000213663)** — When configuring ACLs, the Switch incorrectly reports:

  ```
  Duplicate access control entry.
  ```

- **Broadcast throttling (PR_1000240494)** — Broadcast throttling does not work correctly on Gigabit/second and 10-Gigabit/second ports.
- **Mesh (PR_1000218463)** — If a mesh link goes down and a redundant (xSTP) link external to the mesh goes into a forwarding state, connectivity across the mesh may be lost for a previously learned MAC address.
- **MIB (PR_1000236875)** — The switch is reporting etherType/size errors as part of "ifInDiscards," but the packets are not really dropped.
- **Packet buffers (PR_1000237366)** — Improved packet buffer allocation for better data handling.
- **Self-test (PR_1000239302)** — The Switch reports a false self-test failure when a J8436A SR transceiver is installed in Port B of a J8435A 10-GbE Media Flex module.
- **Web/Stack Mgmt (PR_1000239924)** — As an IP Stack Management Commander, the Switch does not display the device view (back of box) for a 2626 switch that is a member.

Release M.08.71

Problems Resolved in Release M.08.71 (Never released)

- **Crash (PR_1000232283)** — The switch may crash with a message similar to:

  ```
  Software exception at fileTransferTFTP.c:182 -- in 'mftTask', task ID = 0x107ee0.
  ```

- **LLDP (PR_1000241315)** — CLI command "show LLDP" does not display information correctly.
- **Web Auth (PR_1000230444)** — Using port-based web authentication on the Switch will cause some users to never receive the web authentication screen. This occurs if a client receives the same unauthenticated DHCP address that a previous authorized client has used.
- **802.1s (PR_1000233920)** — 802.1s (MSTP) blocks a port that is connected to an RSTP device.

Release M.08.72

Problems Resolved in Release M.08.72 (Not a general release)

- **Crash (PR_1000234773)** — The switch may crash with a message similar to:

  ```
  "ifInfo" task:  SubSystem 0 went down:  01/01/90 00:03:16 NMI event
  SW:IP=0x004c1bdc MSR:0x0000b032 LR:0x004c3850 Task='ifInfo' Task
  ID=0x137c980 cr: 0x22242040 sp:0x0137bef8 xer:0x00000000.
  ```

- **Flow Control (PR_1000241296)** — Switch was unable to support flow control between any ingress and any egress ports.
- **SNMP (PR_1000003378)** — SNMP switch time may drift with event log updates occurring every 1.5 hours.
- **Web UI (PR_1000211978)** — On a Stack Management Commander, when using "stack access" to view members, the screen does not display correct information.

Release M.08.73

Problems Resolved in Release M.08.73 (Not a general release)

- **Crash (PR_1000282197)** — The 3400cl-48G may experience crash or reboot symptoms on initial install of the switch. The crashes have a PPC crash heading. The switch may reboot with no crash history, simply the following message:

  ```
  System reboot due to power failure.
  ```

- **Boot ROM** — Updated to I.08.07 version to support fix for PR 1000282197.

Release M.08.74

Problems Resolved in Release M.08.74 (Not a general release)

Meshing (PR_1000282427) — Multicast traffic not forwarded out 10 Gigabit mesh ports.

Release M.08.75

Problems Resolved in Release M.08.75

- **LR optic (PR_1000282195)** — After a switch reboot, certain 10GbE X2-SC LR Optic (J8437A) transceivers will lose its configuration. Administrator will be unable to turn off LACP, and CLI commands will not be displayed.
- **XRRP (PR_1000280213)** — When configuring a XRRP instance, although the subnet is configured properly, the following error message is logged:

  ```
  No subnet configured for the IP address
  ```

Release M.08.76

Problems Resolved in Release M.08.76 (Never released)

- **IP Routing (PR_1000254254)** — L3 address table is not learned correctly from unsolicited ARPs.
- **RADIUS (PR_1000285456)** — If more than one RADIUS assigned vendor specific attribute (including Port-cos, rate-limiting-ingress, or ACLs) is configured with a non-vendor specific attribute, only the first vendor specific attribute may be recognized by the switch.
- **TCP (PR_1000246186)** — Switch is susceptible to VU#498440.
- **VLAN (PR_1000214406)** — When trying to delete a VLAN created as a management VLAN, the switch fails to remove the management VLAN statement from the running configuration file.

Web UI (PR_1000284653) — When using the web user interface "IP Stack Management", and there are more than 100 potential Members present on a VLAN, the Switch will learn new potential Members, but deletes previously learned Members.

Release M.08.77

Problems Resolved in Release M.08.77 (Not a general release)

- **ACL (PR_1000283338)** — The commands "`show port-access mac`" and "`show port-access web`" incorrectly display the number of clients authenticated.
- **Meshing (PR_1000219337)** — Unstable RSTP topology when root switch is power-cycled and connected to a mesh.

Release M.08.78

Problems Resolved in Release M.08.78 (Not a general release)

- **Enhancement (PR_1000291806)** — Fast boot enhancement.
- **MSTP (PR_1000286883)** — Slow MSTP fail-over and fall-back time.

Release M.08.79

Problems Resolved in Release M.08.79 (Not a general release)

- **Fault (PR_1000089786)** — Chassis fault LED stops blinking after a new OS image was downloaded to the switch.

- **Ports (PR_1000090867)** — The dual personality ports (RJ-45 and mini-GBIC) lose state (running speed) after being hot swapped in or out.
- **Enhancement (PR_100292455)** — Rate display for ports on CLI. New command: "`show interface port-utilization`", not available on Menu nor Web Interface.

Release M.08.80

Problems Resolved in Release M.08.80 (Never released)

- **RSTP (PR_1000297195)** — The switch repeatedly flushes its MAC address table, resulting in intermittent flooding of all traffic.

Release M.08.81

Problems Resolved in Release M.08.81 (Not a general release)

- **XRRP (PR_1000291250)** — When a XRRP router is rebooted and activates its virtual MAC address, it incorrectly transmits ARP requests, which fails to update forwarding tables and ARP caches.

Release M.08.82

Problems Resolved in Release M.08.82 (Not a general release)

- **Meshing (PR_1000300165)** — Packets larger than 1482 bytes within a mesh will be reported as FCS receive errors and may generate excessive CRC error messages in the event log.
- **RSTP (PR_1000300623)** — Under some circumstances, the switch may allow packets to loop for an extended period of time.

Release M.08.83

Problems Resolved in Release M.08.83 (Not a general release)

- **Crash (PR_1000297510)** — When using the Web User Interface and the switch is set as commander for stacking, the switch may crash.
- **Event Log/ARP (PR_1000293466)** — Generic Link Up message not showing up and unnecessary flushing of ARP cache.
- **KMS (PR_1000287934)** — Some Key Management System (KMS) configuration commands have no effect.

- **Setup (PR_1000301498)** — Manual IP address can not be set using "setup" menu. (pre-release)

Release M.08.84

Problems Resolved in Release M.08.84 (Never released)

- **CLI Enhancement (PR_1000306695)** — Added "show tech transceivers" to display Serial Number information for installed mGBIC and 10Gig X2 transceivers. Allows removable transceiver serial numbers to be read without removal of the transceivers from the switch.

Release M.08.85

Problems Resolved in Release M.08.85 (Never released)

- **RSTP** (No PR) — Resolved broadcast storm caused by an unstable RSTP topology.

Release M.08.86

Problems Resolved in Release M.08.86

- **CLI/DHCP (PR_1000286898)** — Under some conditions, the CLI may freeze or lock up.
- **IGMP (PR_1000301557)** — Data-driven IGMP does not prevent flooding when no IP address exists on a VLAN.
- **RSTP (PR_1000306227)** — RSTP TCNs cause high CPU utilization and slow software based routing.
- **SNMP (PR_1000295753)** — Removing 'public' SNMP community generates an empty Event Log message.

Release M.08.87

Problems Resolved in Release M.08.87 (Not a general release)

- **Crash/STP (PR_1000307280)** — Inconsistent or incorrect STP data may cause the switch to crash with a message similar to:

```
Software exception at stp_mib.c:248 -- in 'mSnmpCtrl', task ID =
0x12d14b8\n-> ASSERT:  failed.
```

- **Menu (PR_1000306213)** — When using the Menu to create a trunk, the new trunk ports will become disabled after a switch reboot.

- **OSPF (PR_1000280427)** — OSPF MD5 Authentication failure.
- **RSTP (PR_1000309683)** — Temporary routing or switching problems after RSTP is disabled.

Release M.08.88

Problems Resolved in Release M.08.88 (Not a general release)

- **CLI (PR_1000310849)** — Under a heavy load where packets received on a 10-Gigabit port are dropped, the RX drop counter values decrease when they should increase.
- **LLDP (PR_1000310666)** — The command "show LLDP" does not display information learned from CDPv2 packets.
- **SNMP Traps (PR_1000285195)** — Switch does not save the option to disable a Link up/down SNMP trap after a switch reboot.
- **Web /Stacking (PR_1000308933)** — Added Web User Interface stacking support for the new Series 3500yl switches, providing a 3500yl "back-of-box" display when the 3400cl or 6400cl is stack commander and a 3500yl is a stack member.

Release M.08.89

Problems Resolved in Release M.08.89 (Never released)

- **Enhancements (PR_1000313819)** — Added two enhancements:
  - DNS Names for Ping and Traceroute
  - RADIUS Configuration via SNMP. For details refer to "Using SNMP To View and Configure Switch Authentication Features" on page 32.
- **Port Security (PR_1000304202)** — The port-security MAC address learn mode does not function correctly between 'port-security' ports.
- **SNMP (PR_1000310841)**— User can assign illegal values for CosDSCPPolicy through SNMP. All other user-interfaces for configuring QoS function correctly.

Release M.08.90

Problems Resolved in Release M.08.90 (Not a general release)

- **Crash/log (PR_1000282359)** - When searching the log for an extremely long string, the switch may crash with a bus error similar to:

```
PPC Bus Error exception vector 0x300: Stack Frame=0x0c8c1a70 HW
Addr=0x6a73616c IP=0x007d3bc0 Task='mSess1' Task ID=0xc8c2920 fp:
0x6b61736a sp:0x0c8c1b30 lr:0x007d3b28.
```

- **MSTP Enhancement (PR_1000310463)** - Implemented new CLI command "spanning-tree legacy-path-cost". See "MSTP Default Path Cost Controls" on page 35 for details.

Release M.08.91

Problems Resolved in Release M.08.91 (Never released)

- **MSTP Enhancement (PR_1000313986)** - Implemented new CLI command, "spanning-tree legacy-mode".
- **RADIUS (PR_1000316158)** - After a switch reboot, the switch does not recognize a response from a RADIUS or TACACS server.
- **Performance Enhancement (PR_1000291806)** - Allow user configuration of the packet buffer queuing mode. For details, see "QoS Pass-Through Mode" on page 36.

Release M.08.92

Problems Resolved in Release M.08.92 (Not a general release)

- **Config (PR_1000298146)** — Enabling QoS-passthrough Mode causes incorrect information to be displayed in the "show configuration" command.

Release M.08.93

Problems Resolved in Release M.08.93 (Not a general release)

- **Help (PR_1000317711)** — In the VLAN menu Help text, the word 'default' is spelled incorrectly.
- **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.
- **SNMP (PR_1000315054)**— SNMP security violations appear in syslog after a valid SNMPv3 "get" operation.

Release M.08.94

Problems Resolved in Release M.08.94 (Not a general release)

- **Enhancements (PR_1000319920)** — Added support for following features:
  - DHCP Option 82 functionality, and
  - UDP broadcast forwarding
- **Menu (PR_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.

Release M.08.95

Problems Resolved in Release M.08.95 (Not a general release)

- **STP/RSTP/MSTP (PR_1000300623)** — In some cases STP/RSTP/MSTP may allow a loop, resulting in a broadcast storm.

Releases M.08.96 through M.08.98 were never built.

Release M.08.99

Problems Resolved in Release M.08.99 (Not a general release)

- **Counters (PR_1000321097)** — Drop counters may display incorrect information.
- **Crash (PR_1000323675)** — The Switch may crash with a message similar to:

  ```
  ASSERT: Software exception at aaa8021x_proto.c:501 -- in 'm8021xCtrl'.
  ```

- **ICMP (PR_1000235905)** — Switch does not send a “destination unreachable” response message when trying to access an invalid UDP port.
- **OSPF (PR_1000319678)** — Switch does not accept IP fragmented OSPF packets.
- **SNMPv3 (PR_1000325021)** — Under some conditions, SNMPv3 lines are not written to the running-configuration file.

Release M.08.101

Problems Resolved in Release M.08.101 (Not a general release)

- **CLI (PR_1000317554)** — The command "show version" does not display the full version number.
- **Crash/sFlow (PR_1000327132)** — The Switch may crash with a message similar to:

  ```
  Software exception in ISR at btmDmaApi.c:304.
  ```

- **Crash/SSHv2 (PR_1000320822)** — The Switch does not generate SSHv2 keys and may crash with a message similar to:

  ```
  TLB Miss: Virtual Addr=0x00000000 IP=0x80593a30 Task='swInitTask' Task
  ID=0x821ae330 fp:0x00000000 sp:0x821adfb8 ra:0x800803f0 sr:0x1000fc01.
  ```

- **Crash (PR_1000322009)** — The Switch may crash with a message similar to:

  ```
  Software exception in ISR at queues.c:123.
  ```

- **sFlow (PR_1000321195)** — A network management application may incorrectly report traffic spikes when sFlow is first re-enabled.

Release M.08.102

Problems Resolved in Release M.08.102

- **Crash/STP (PR_1000335117)** — Improvement of the PR_1000300623 fix, first included in M.08.95.
- **Enhancement (PR_1000309540)** — Added support for the J8440B 10-GbE X2-CX4 Transceiver.
- **OSPF (PR_1000323201)** — OSPF with MD5 authentication enabled does not always redistribute connected networks.
- **Transceiver (PR_1000310852)** — The 10-GbE X2-SC LR transceiver (J8437A) may have excessive link toggles during Switch bootup.

Release M.08.103

Problems Resolved in Release M.08.103 (Not a general release)

- **CLI (PR_1000334412)** — Operator level can save Manager privilege level changes to the configuration.
- **Counters (PR_1000327308)** — 10-Gig port with STP blocked will increment RX drops on broadcast packets.
- **Enhancement (PR_1000340595)** — Added support for PIM Dense Mode. For details, refer to Chapter 5, "PIM-DM (Dense Mode) on the 5300xl Switches" in the *Advanced Traffic Management Guide for the ProCurve Series 6400cl/5300xl/4200vl/3400cl Switches.*

Release M.08.104

Problems Resolved in Release M.08.104 (Not a general release)

- **CLI (PR_1000322029)** — The command "show vlans" does not display data correctly in the status field.
- **Crash (PR_1000339551)** — When using the Menu to disable IP routing, the Switch may crash with a message similar to:

  ```
  PPC Bus Error exception vector 0x300: Stack-frame=0x0162e030
  HW Addr=0x2e2e2e2d.
  ```

- **DHCP (PR_1000343149)** — Client cannot obtain an IP address when two DHCP servers are connected on different local networks.
- **Menu (PR_1000319651)** — In the "Internet (IP) Service" menu screen, the user is unable to use the "Save" function to exit the screen. User must use "Cancel" to exit from the screen.
- **Transceiver (PR_1000349320)** — Some 10-GbE X2-CX4 transceivers fail to initialize correctly and lose their configuration.
- **VLAN (PR_1000284852)** — The Switch may transmit packets with a VLAN ID that is out of range.
- **Web UI (PR_1000340311)** — When using the web user interface and accessing the "Security" tab, the switch will request the manager username and password. Then select the "Port Access" button, a second log-in box appears and requests the same manager username and password multiple times, causing the IE browser to hang and requiring the browser to be reset.

Release M.08.105

Problems Resolved in Release M.08.105 (Not a general release)

- **802.1X (PR_1000353479)** — Changing the supplicant start period (e.g., "aaa port-access supplicant A1 start-period 15") corrupts the supplicant password on a switch that is configured as a supplicant.
- **LACP (PR_1000352012)** — An LACP state change does not properly reset a 10-Gig port, communication through affected ports fails until port is toggled.

Release M.08.106

Problems Resolved in Release M.08.106 (Not a general release)

- **Link Failure (PR_1000361488)** — The B version of the 10-GbE X2-CX4 transceiver (J8440B) may not initialize correctly, causing link failure.

Release M.08.107

Problems Resolved in Release M.08.107

- **CLI (PR_1000292887)** — The CLI command "aaa port-access web-based <port-list> redirect-url" accepts only the first 103 characters of the maximum allowed value of 127 characters.
- **CLI (PR_1000364628)** — The command output from "show ip rip peer" yields an improperly formatted peer IP address.
- **CLI/Config (PR_1000377413)** — The CLI does not prevent an invalid configuration from being loaded. With this fix, configurations with excess IP Addresses in QoS entries will result in an error message and the config file will not load.
- **CLI/LLDP (PR_1000377191)** — Output from the CLI command, "show lldp info remote-device <port>" shows a blank field for the chassis ID.
- **CLI (PR_1000240838)** — If an invalid time is entered using "clock set" command, the switch responds with an "invalid date" error.
- **CLI (PR_1000199785)** — The tab help function (command-completion) for "IP RIP authentication" is inaccurate. The help selection lists "OCTET-STR Set authentication key" when it should be "ASCII-STR Set RIP auhentication key (maximum 16 characters)".
- **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.
```

- **Crash (PR_1000382962)** — Executing the CLI command, "sho int" on a miniGBIC that is not linked, may cause the switch to crash with a message similar to:

```
Divide by Zero Error: IP=0x8017becc Task='mSess1' Task ID=0x834b19d0
fp:0x00000018 sp:0x834b0d20 ra:0x8017be18 sr:0x1000fc01 Division by
0 Crash at cli_opershow_action.c:1298.
```

- **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.

- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Enhancement (PR_1000335860)** — This enhancement provides a configuration option for the source IP address field of SNMP response and generated trap PDUs.
- **Enhancement (PR_1000376626)** — Enhanced CLI "qos dscp-map he" help and "show dscp-map" text to warn users that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.
- **RX drop counters (PR_1000390921)** — If all VLANs are tagged on a port, the RX drop counters increment at a rate of 1 every 3 seconds on the 10-Gig ports.
- **Web/RADIUS (PR_1000368520)** — Web Authentication does not authenticate clients due to a failure to send RADIUS requests to the configured server.

March 2007
Manual Part Number
5991-4765