

# Release Notes:

## Version L.10.24 Software

*for the ProCurve Series 4200vl Switches*

---

Release L.10.24 supports these switches:

- ProCurve Switch 4204vl (J8770A), 4208vl (J8773A), 4202vl-72 (J8772A), and 4202vl-48G (J8771A)

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 8](#))
- A listing of software enhancements in this release ([page 18](#))
- A listing of software fixes included in releases L.10.01 through L.10.24 ([page 66](#))

---

### **Security Note:**

Downloading and booting software release L.10.20 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 “Switch Management Access Security” on page 8 and “Using SNMP To View and Configure Switch Authentication Features” on page 51.

### **Related Publications**

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at [www.procurve.com](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 Series 6400cl, Series 5300xl, Series 4200vl, and Series 3400cl switches.

© Copyright 2006-2007 Hewlett-Packard Company, LP.  
The information contained herein is subject to change  
without notice.

### Publication Number

5991-4696  
March 2007

### Applicable Products

ProCurve Switch 4204vl	(J8770A)
ProCurve Switch 4208vl	(J8773A)
ProCurve Switch 4202vl-72	(J8772A)
ProCurve Switch 4202vl-48G	(J8771A)

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

# Contents

<b>Software Management</b> . . . . .	<b>1</b>
Software Updates . . . . .	1
Downloading Switch Documentation and Software from the Web . . . . .	1
Downloading Software to the Switch . . . . .	2
TFTP Download from a Server . . . . .	3
Xmodem Download From a PC or Unix Workstation . . . . .	4
Saving Configurations While Using the CLI . . . . .	5
ProCurve Switch, Routing Switch, and Router Software Keys . . . . .	6
Minimum Software Versions for Series 4200vl Switch . . . . .	7
OS/Web/Java Compatibility Table . . . . .	7
<b>Enforcing Switch Security</b> . . . . .	<b>8</b>
Switch Management Access Security . . . . .	8
Default Settings Affecting Security . . . . .	8
Local Manager Password . . . . .	9
Inbound Telnet Access and Web Browser Access . . . . .	9
Secure File Transfers . . . . .	9
SNMP Access (Simple Network Management Protocol) . . . . .	10
Physical Access to the Switch . . . . .	11
Other Provisions for Management Access Security . . . . .	12
Network Access Security . . . . .	13
Access Control Lists (ACLs) . . . . .	13
Web and MAC Authentication . . . . .	13
Secure Shell (SSH) . . . . .	14
Secure Socket Layer (SSLv3/TLSv1) . . . . .	14
Traffic/Security Filters . . . . .	14
802.1X Access Control . . . . .	15
Port Security, MAC Lockdown, MAC Lockout, and IP Lockdown . . . . .	16
Key Management System (KMS) . . . . .	16
Connection-Rate Filtering Based On Virus-Throttling Technology . . . . .	17

<b>Enhancements</b> .....	<b>18</b>
Release L.10.02 Enhancements .....	18
MSTP Default Path Cost Controls .....	18
Release L.10.03 Enhancements .....	18
Release L.10.04 Enhancements .....	19
DHCP Option 82: Using the Management VLAN IP Address for the Remote ID .....	19
Release L.10.05 Enhancements .....	21
Release L.10.06 Enhancements .....	21
Show sFlow Commands .....	21
Release L.10.07 Enhancements .....	24
Uni-Directional Link Detection (UDLD) .....	24
Release L.10.08 Enhancements .....	31
Configuring 802.1X Controlled Directions .....	31
Release L.10.09 Enhancements .....	33
DHCP Snooping Overview .....	33
Enabling DHCP Snooping .....	33
Enabling DHCP Snooping on VLANs .....	36
Configuring DHCP Snooping Trusted Ports .....	36
Configuring Authorized Server Addresses .....	37
Using DHCP Snooping with Option 82 .....	38
The DHCP Binding Database .....	41
Release L.10.10 Enhancements .....	44
Release L.10.11 Enhancements .....	44
Release L.10.20 Enhancements .....	45
Spanning Tree Per-Port BPDU Filtering .....	46
Spanning Tree BPDU Protection .....	49
Using SNMP To View and Configure Switch Authentication Features .....	51
TCP/UDP Port Closure .....	54
Instrumentation Monitor .....	56
Adding SNMPv3 Users With AES .....	60
Configuring Loop Protection .....	61
Release L.10.23 Enhancements .....	63
Release L.10.24 Enhancements .....	64

Configuring the Source IP Address for SNMP Requests and Traps .....	64
<b>Software Fixes in Release L.10.01 - L.10.24 .....</b>	<b>66</b>
Release L.10.02 .....	66
Release L.10.03 .....	67
Release L.10.04 .....	68
Release L.10.05 .....	69
Release L.10.06 .....	69
Release L.10.07 .....	69
Release L.10.08 .....	70
Release L.10.09 .....	71
Release L.10.10 .....	71
Release L.10.11 .....	71
Release L.10.20 .....	72
Release L.10.23 .....	73
Release L.10.24 .....	73

# 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:  
[www.procurve.com](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 [www.procurve.com](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 ([www.procurve.com](http://www.procurve.com)). After you acquire the new software file, you can use one of the following methods for downloading it to the switch:

- For a TFTP transfer from a server, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.
  - Use the **copy tftp** command in the switch's CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and select the **Xmodem** option.
  - Use the **copy xmodem** command in the switch's CLI (page 4).
- Use the download utility in ProCurve Manager Plus.

---

### Note

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

---

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

## TFTP Download from a Server

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

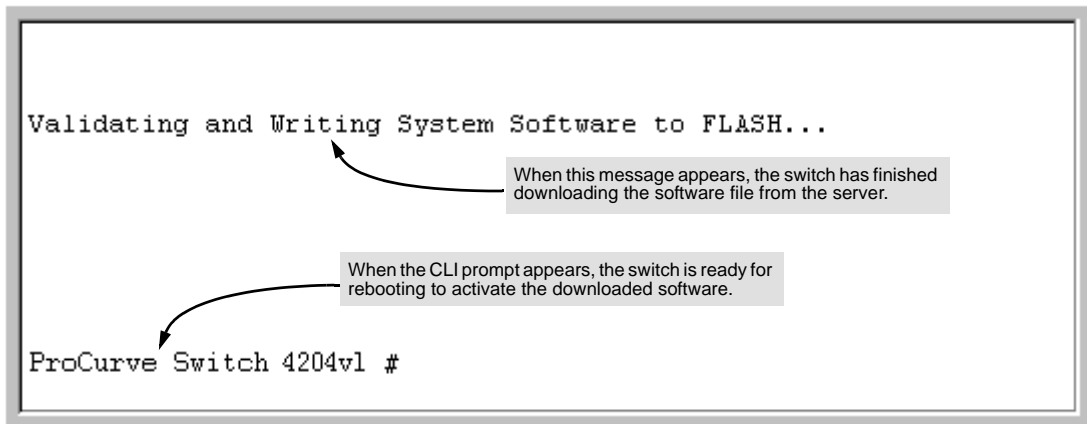
Note that if you do not specify the flash destination, the TFTP download defaults to the primary flash.

For example, to download a software file named L\_10\_0x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve # copy tftp flash 10.28.227.103 L_10_0x.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. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
4. Reboot the switch from the flash area that holds the new software (primary or secondary).

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



## Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

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

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

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

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

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

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

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

2. Execute the following command in the CLI:

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

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

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

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

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

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

---

## 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] ?
```

## Software Management

ProCurve Switch, Routing Switch, and Router Software Keys

# ProCurve Switch, Routing Switch, and Router Software Keys

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

Version L.10.01 is the first software release for the ProCurve Series 4200vl switches.

## Minimum Software Versions for Series 4200vl Switch

The following table lists minimum software versions required to support ProCurve Series 4200vl switch hardware.

<b>ProCurve Device</b>	<b>Minimum Supported Software Version</b>
J8768A ProCurve Switch vl 24-port Gig-T Module	L.10.23
J9030A ProCurve Switch 4208vl-72GS 68 10/100/1000 + 4 SFP	L.10.23
J9033A ProCurve Switch vl 20-port Gig-T + 4-port SFP Module	L.10.23
J9064A ProCurve Switch 4204vl-48GS 44 10/100/1000 + 4 SFP	L.10.23

## OS/Web/Java Compatibility Table

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

<b>Operating System</b>	<b>Internet Explorer</b>	<b>Java</b>
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, 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 L.10.20, 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 L.10.20 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 51) is not desirable for your network, then immediately after downloading and booting from the L.10.20 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 L.10.20 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 recommended 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.

# Enhancements

---

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

Enhancements are listed in chronological order, oldest to newest software release. To review the list of enhancements included since the last general release that was published, begin with [“Release L.10.10 Enhancements” on page 44.](#)

## Release L.10.02 Enhancements

Release L.10.02 includes the following enhancements:

### 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

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.

## Release L.10.03 Enhancements

*No enhancements, software fixes only.*

## Release L.10.04 Enhancements

Release L.10.04 includes the following enhancements:

- TheDHCP Option 82 enhancement (see details below)
- Enhancement to display Port Name along with Port number on the Web User Interface, Status and Configuration screens.

### 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* for your switch.

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 L.10.04, 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.

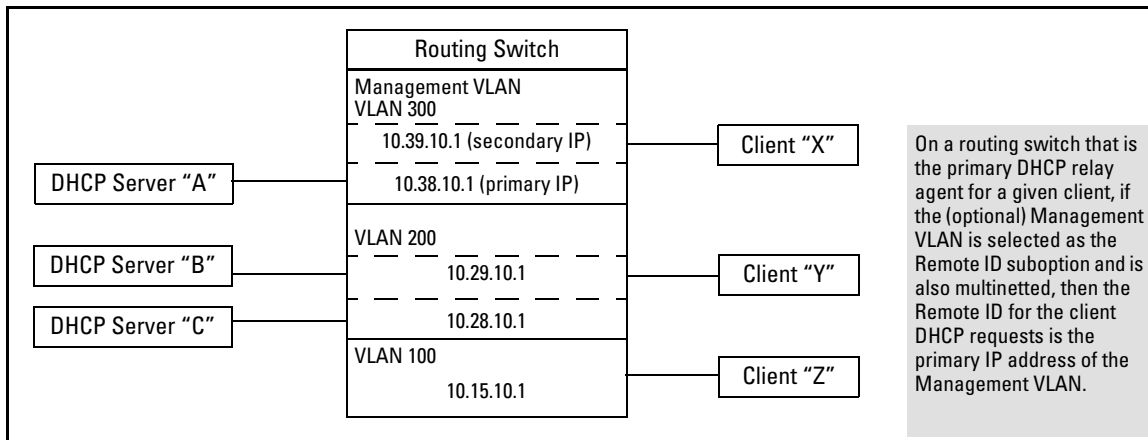
**ip:** Specifies the IP address of the VLAN on which the client DHCP packet enters the routing switch. In the case of a multinetted VLAN, the remote ID suboption uses the IP address of the subnet on which the client request packet is received.

**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
```



**Figure 2. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption**

The resulting effect on DHCP operation for clients X, Y, and Z is shown in [Table 1](#).

**Table 1. DHCP Operation for the Topology in Figure 2**

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.

## Release L.10.05 Enhancements

*No enhancements, software fixes only.*

## Release L.10.06 Enhancements

Release L.10.06 includes the following enhancements:

### Show sFlow Commands

In earlier software releases, the only method for checking whether sFlow is enabled on the switch was via an snmp request. Beginning with software release L.10.06, the 4200vl switches have added the following show sFlow commands that allow you to see sFlow status via the CLI.

**Syntax:** show sflow agent

*Displays sFlow agent information. The agent address is normally the ip address of the first vlan configured.*

**Syntax:** show sflow destination

*Displays information about the management station to which the sFlow sampling-polling data is sent.*

**Syntax:** show sflow sampling-polling <port-list/range>

*Displays status information about sFlow sampling and polling.*

**Syntax:** show sflow all

*Displays sFlow agent, destination, and sampling-polling status information for all the ports on the switch.*

## Terminology

**sFlow** — An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

**sFlow agent** — A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

**sFlow destination** — The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

## Viewing SFlow Configuration

The **show sflow agent** command displays read-only switch agent information. The version information shows the sFlow MIB support and software versions; the agent address is typically the ip address of the first vlan configured on the switch.

```
ProCurve# show sflow agent
  Version           1.3;HP;L.10.06
  Agent Address     10.0.10.228
```

**Figure 3. Viewing sFlow Agent Information**

The **show sflow destination** command includes information about the management-station's destination address, receiver port, and owner.

```
ProCurve# show sflow destination
sflow                               Enabled
Datagrams Sent                       221
Destination Address                   10.0.10.41
Receiver Port                         6343
Owner                                 admin
Timeout (seconds)                    333
Max Datagram Size                     1400
Datagram Version Support              5
```

**Figure 4. Example of Viewing sFlow Destination Information**

Note the following details:

- **Destination Address** remains blank unless it has been configured on the switch via SNMP.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.
- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

The **show sflow sampling-polling** command displays information about sFlow sampling and polling on the switch. You can specify a list or range of ports for which to view sampling information.

```
ProCurve# show sflow sampling-polling 1-5

sflow destination Enabled

Port | Sampling                Dropped | Polling
     | Enabled Rate           Header Samples | Enabled Interval
-----+-----
1   | Yes      6500000  128  5671234 | Yes      60
2   | No       50           128   0      | Yes     300
3   | Yes     2000          100  24978  | No       30
4   | Yes     200           100  4294967200 | Yes     40
5   | Yes    20000         128   34     | Yes     500
```

**Figure 5. Example of Viewing sFlow Sampling and Polling Information**

The **show sflow all** command combines the outputs of the preceding three show commands including sFlow status information for all the ports on the switch.

## Release L.10.07 Enhancements

Release L.10.07 includes the following enhancements:

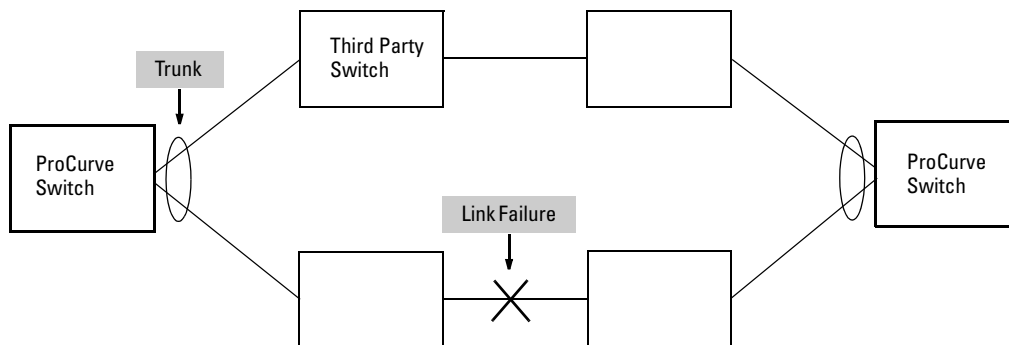
- Added support for Unidirectional Fiber Break Detection.

### Uni-Directional Link Detection (UDLD)

Uni-directional Link Detection (UDLD) monitors a link between two ProCurve switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks. Figure 6 shows an example.

**Scenario 1 (No UDLD):** Without UDLD, the switch ports remain enabled despite the link failure. Traffic continues to be load-balanced to the ports connected to the failed link.

**Scenario 2 (UDLD-enabled):** When UDLD is enabled, the feature blocks the ports connected to the failed link.



**Figure 6. UDLD Example**

In this example, each ProCurve switch load balances traffic across two ports in a trunk group. Without the UDLD feature, a link failure on a link that is not directly attached to one of the ProCurve switches remains undetected. As a result, each switch continues to send traffic on the ports connected to the failed link. When UDLD is enabled on the trunk ports on each ProCurve switch, the switches detect the failed link, block the ports connected to the failed link, and use the remaining ports in the trunk group to forward the traffic.

Similarly, UDLD is effective for monitoring fiber optic links that use two uni-direction fibers to transmit and receive packets. Without UDLD, if a fiber breaks in one direction, a fiber port may assume the link is still good (because the other direction is operating normally) and continue to send

traffic on the connected ports. UDLD-enabled ports, however, will prevent traffic from being sent across a bad link by blocking the ports in the event that either the individual transmitter or receiver for that connection fails.

Ports enabled for UDLD exchange health-check packets once every five seconds (the link-keepalive interval). If a port does not receive a health-check packet from the port at the other end of the link within the keepalive interval, the port waits for four more intervals. If the port still does not receive a health-check packet after waiting for five intervals, the port concludes that the link has failed and blocks the UDLD-enabled port.

When a port is blocked by UDLD, the event is recorded in the switch log or via an SNMP trap (if configured); and other port blocking protocols, like spanning tree or meshing, will not use the bad link to load balance packets. The port will remain blocked until the link is unplugged, disabled, or fixed. The port can also be unblocked by disabling UDLD on the port.

## Configuration Considerations

- UDLD is configured on a per-port basis and must be enabled at both ends of the link. See the note below for a list of ProCurve switches that support UDLD.
- To configure UDLD on a trunk group, you must configure the feature on each port of the group individually. Configuring UDLD on a trunk group's primary port enables the feature on that port only.
- Dynamic trunking is not supported. If you want to configure a trunk group that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the trunk group, you can re-add the UDLD configuration.

---

### Note

UDLD interoperates with the following ProCurve switch series: 3400, 3500, 5300, 5400, 6200, 6400, and 9300. Consult the release notes and current manuals for required software versions.

---

## Configuring UDLD

The following commands allow you to configure UDLD via the CLI.

**Syntax:** [no] interface <port-list> link-keepalive

*Enables UDLD on a port or range of ports.*

*To disable the feature, enter the **no** form of the command.*

*Default: UDLD disabled*

**Syntax:** link-keepalive interval <interval>

*Determines the time interval to send UDLD control packets. The <interval> parameter specifies how often the ports send a UDLD packet. You can specify from 10 – 100, in 100 ms increments, where 10 is 1 second, 11 is 1.1 seconds, and so on.  
Default: 50 (5 seconds)*

**Syntax:** link-keepalive retries <num>

*Determines the maximum number of retries to send UDLD control packets. The <num> parameter specifies the maximum number of times the port will try the health check. You can specify a value from 3 – 10.  
Default: 5*

**Syntax:** [no] interface <port-list> link-keepalive vlan <vid>

*Assigns a VLAN ID to a UDLD-enabled port for sending of tagged UDLD control packets. Under default settings, untagged UDLD packets can still be transmitted and received on tagged only ports—however, a warning message will be logged.  
The **no** form of the command disables UDLD on the specified port(s).  
Default: UDLD packets are untagged; tagged only ports will transmit and receive untagged UDLD control packets*

**Enabling UDLD.** UDLD is enabled on a per port basis. For example, to enable UDLD on port a1, enter:

```
ProCurve(config)#interface a1 link-keepalive
```

To enable the feature on a trunk group, enter the appropriate port range. For example:

```
ProCurve(config)#interface a1-a4 link-keepalive
```

---

## Note

When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLD-configured ports in the same vlan. That is, UDLD control packets will “pass through” a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

---

**Changing the Keepalive Interval.** By default, ports enabled for UDLD send a link health-check packet once every 5 seconds. You can change the interval to a value from 10 – 100 deciseconds, where 10 is 1 second, 11 is 1.1 seconds, and so on. For example, to change the packet interval to seven seconds, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive interval 70
```

**Changing the Keepalive Retries.** By default, a port waits five seconds to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries four more times by sending up to four more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

You can change the maximum number of keepalive attempts to a value from 3 – 10. For example, to change the maximum number of attempts to 4, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive retries 4
```

**Configuring UDLD for Tagged Ports.** The default implementation of UDLD sends the UDLD control packets untagged, even across tagged ports. If an untagged UDLD packet is received by a non-ProCurve switch, that switch may reject the packet. To avoid such an occurrence, you can configure ports to send out UDLD control packets that are tagged with a specified VLAN.

To enable ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter a command such as the following at the interface configuration level:

```
ProCurve(config)#interface 1 link-keepalive vlan 22
```

---

## Notes

- You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.
  - If a VLAN ID is not specified, then UDLD control packets are sent out of the port as untagged packets.
  - To re-assign a VLAN ID, re-enter the command with the new VLAN ID number. The new command will overwrite the previous command setting.
  - When configuring UDLD for tagged ports, you may receive a warning message if there are any inconsistencies with the port's VLAN configuration (see page 30 for potential problems).
-



## Viewing UDLD Information

The following show commands allow you to display UDLD configuration and status via the CLI.

**Syntax:** show link-keepalive

*Displays all the ports that are enabled for link-keepalive.*

**Syntax:** show link-keepalive statistics

*Displays detailed statistics for the UDLD-enabled ports on the switch.*

**Syntax:** clear link-keepalive statistics

*Clears UDLD statistics. This command clears the packets sent, packets received, and transitions counters in the show link-keepalive statistics display.*

**Displaying Summary UDLD Information.** To display summary information on all UDLD-enabled ports, enter the **show link-keepalive** command. For example:

```
ProCurve(config)# show link-keepalive

Total link-keepalive enabled ports: 4
Keepalive Retries: 3           Keepalive Interval: 1 sec

Port  Enabled  Physical  Keepalive  Adjacent  UDLD
      Status   Status   Status    Switch    VLAN
-----
1  Yes   up       up         00d9d-f9b700  200
2  Yes   up       up         01560-7b1600
3  Yes   down    off-line
4  Yes   up       failure
5  No    down    off-line
```

Figure 7. Example of UDLD Information displayed using Show Link-Keepalive Command

**Displaying Detailed UDLD Status Information.** To display detailed UDLD information for specific ports, enter the **show link-keepalive statistics** command. For example:

```
ProCurve(config)# show link-keepalive statistics
```

Port:	1	Neighbor MAC Addr:	0000a1-b1c1d1
Current State:	up	Neighbor Port:	5
Udld Packets Sent:	1000	State Transitions:	2
Udld Packets Received:	1000	Link-vlan:	1
Port Blocking:	no		
Port:	2	Neighbor MAC Addr:	000102-030405
Current State:	up	Neighbor Port:	6
Udld Packets Sent:	500	State Transitions:	3
Udld Packets Received:	450	Link-vlan:	200
Port Blocking:	no		
Port:	3	Neighbor MAC Addr:	n/a
Current State:	off line	Neighbor Port:	n/a
Udld Packets Sent:	0	State Transitions:	0
Udld Packets Received:	0	Link-vlan:	1
Port Blocking:	no		
Port:	4	Neighbor MAC Addr:	n/a
Current State:	failure	Neighbor Port:	n/a
Udld Packets Sent:	128	State Transitions:	8
Udld Packets Received:	50	Link-vlan:	1
Port Blocking:	yes		

Ports 1 and 2 are UDLD-enabled and show the number of health check packets sent and received on each port.

Port 4 is shown as blocked due to a link-keepalive failure

**Figure 8. Example of Detailed UDLD Information displayed using Show Link-Keepalive Statistics Command**

**Clearing UDLD Statistics.** To clear UDLD statistics, enter the following command:

```
ProCurve# clear link-keepalive statistics
```

This command clears the Packets sent, Packets received, and Transitions counters in the **show link keepalive statistics** display (see Figure 8 for an example).

## Configuration Warnings and Event Log Messages

**Warning Messages.** The following table shows the warning messages that may be issued and their possible causes, when UDLD is configured for tagged ports.

**Table 2. Warning Messages caused by configuring UDLD for Tagged Ports**

CLI Command Example	Warning Message	Possible Problem
link-keepalive 6	Possible configuration problem detected on port 6. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to enable UDLD on a port that is a tagged only port, but did not specify a configuration for tagged UDLD control packets. In this example, the switch will send and receive the UDLD control packets untagged despite issuing this warning.
link-keepalive 7 vlan 4	Possible configuration problem detected on port 7. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to configure tagged UDLD packets on a port that does not belong to the specified VLAN. In this example, if port 7 belongs to VLAN 1 and 22, but the user tries to configure UDLD on port 7 to send tagged packets in VLAN 4, the configuration will be accepted. The UDLD control packets will be sent tagged in VLAN 4, which may result in the port being blocked by UDLD if the user does not configure VLAN 4 on this port.
no vlan 22 tagged 20	Possible configuration problem detected on port 18. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to remove a VLAN on port that is configured for tagged UDLD packets on that VLAN. In this example, if port 18, 19, and 20 are transmitting and receiving tagged UDLD packets for Vlan 22, but the user tries to remove Vlan 22 on port 20, the configuration will be accepted. In this case, the UDLD packets will still be sent on Vlan 20, which may result in the port being blocked by UDLD if the users do not change the UDLD configuration on this port.

**Note:** If you are configuring the switch via SNMP with the same problematic VLAN configuration choices, the above warning messages will also be logged in the switch's event log.

**Event Log Messages.** The following table shows the event log messages that may be generated once UDLD has been enabled on a port.

**Table 3. UDLD Event Log Messages**

Message	Event
I 01/01/06 04:25:05 ports: port 4 is deactivated due to link failure.	A UDLD-enabled port has been blocked due to part of the link having failed.
I 01/01/06 06:00:43 ports: port 4 is up, link status is good.	A failed link has been repaired and the UDLD-enabled port is no longer blocked.

## Release L.10.08 Enhancements

Release L.10.08 includes the following enhancements:

- Increased the maximum number of 802.1X users per port to 8.
- 802.1X Controlled Directions enhancement. With this change, Administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.

### Configuring 802.1X Controlled Directions

After you enable 802.1X authentication on specified ports, you can use the **aaa port-access controlled-directions** command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state.

As documented in the IEEE 802.1X standard, an 802.1X-aware port that is unauthenticated can control traffic in either of the following ways:

- In both ingress and egress directions by disabling both the reception of incoming frames and transmission of outgoing frames
- Only in the ingress direction by disabling only the reception of incoming frames.

**Prerequisite.** As documented in the IEEE 802.1X standard, the disabling of incoming traffic and transmission of outgoing traffic on an 802.1X-aware egress port in an unauthenticated state (using the **aaa port-access controlled-directions in** command) is supported only if:

- The port is configured as an edge port in the network using the **spanning-tree edge-port** command.
- The 802.1s Multiple Spanning Tree Protocol (MSTP) or 802.1w Rapid Spanning Tree Protocol (RSTP) is enabled on the switch. MSTP and RSTP improve resource utilization while maintaining a loop-free network.

For information on how to configure the prerequisites for using the **aaa port-access controlled-directions in** command, see Chapter 4, “Multiple Instance Spanning-Tree Operation” in the *Advanced Traffic Management Guide*.

**Syntax:** `aaa port-access <port-list> controlled-directions <both | in>`

**both (default):** *Incoming and outgoing traffic is blocked on an 802.1X-aware port before authentication occurs.*

**in:** *Incoming traffic is blocked on an 802.1X-aware port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated 802.1X-aware ports.*

## Wake-on-LAN Traffic

The Wake-on-LAN feature is used by network administrators to remotely power on a sleeping workstation (for example, during early morning hours to perform routine maintenance operations, such as patch management and software updates).

The **aaa port-access controlled-direction in** command allows Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port that has not yet transitioned to the 802.1X authenticated state; the **controlled-direction both** setting prevents Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port until authentication occurs.

---

### Note

Although the **controlled-direction in** setting allows Wake-on-LAN traffic to traverse the switch through unauthenticated 802.1X-aware egress ports, it does not guarantee that the Wake-on-LAN packets will arrive at their destination. For example, firewall rules on other network devices and VLAN rules may prevent these packets from traversing the network.

---

## Operating Notes

- Using the **aaa port-access controlled-directions in** command, you can enable the transmission of Wake-on-LAN traffic on unauthenticated egress ports that are configured for 802.1X .

Because a port can be configured for more than one type of authentication to protect the switch from unauthorized access, the last setting you configure with the **aaa port-access controlled-directions** command is applied to all authentication methods configured on the switch.

For information about how to configure and use MAC and Web authentication, refer to the *Access and Security Guide* for your switch.

- To display the currently configured 802.1X Controlled Directions value, enter the **show port-access authenticator config** command.
- When an 802.1X-authenticated port is configured with the **controlled-directions in** setting, eavesdrop prevention is not supported on the port.

## Example: Configuring 802.1X Controlled Directions

The following example shows how to enable the transmission of Wake-on-LAN traffic in the egress direction on an 802.1X-aware port before it transitions to the 802.1X authenticated state and successfully authenticates a client device.

```
ProCurve(config)# aaa port-access authenticator a10
ProCurve(config)# aaa authentication port-access eap-radius
ProCurve(config)# aaa port-access authenticator active
ProCurve(config)# aaa port-access a10 controlled-directions in
```

**Figure 1-9. Example of Configuring 802.1X Controlled Directions**

## Release L.10.09 Enhancements

- Added DHCP Protection enhancement (DHCP Snooping) for switch 4200vl.

### DHCP Snooping Overview

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped. Conditions for dropping packets are shown below.

Condition for Dropping a Packet	Packet Types
A packet from a DHCP server received on an untrusted port	DHCPOFFER, DHCPACK, DHCPNACK
If the switch is configured with a list of authorized DHCP server addresses and a packet is received from a DHCP server on a trusted port with a source IP address that is not in the list of authorized DHCP server addresses.	DHCPOFFER, DHCPACK, DHCPNACK
Unless configured to not perform this check, a DHCP packet received on an untrusted port where the DHCP client hardware address field does not match the source MAC address in the packet	N/A
Unless configured to not perform this check, a DHCP packet containing DHCP relay information (option 82) received from an untrusted port	N/A
A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database is different from the port on which the packet is received	DHCPRELEASE, DHCPDECLINE

### Enabling DHCP Snooping

DHCP snooping is enabled globally by entering this command:

```
ProCurve(config)# dhcp-snooping
```

Use the **no** form of the command to disable DHCP snooping.

**Syntax:** [no] dhcp-snooping [authorized-server | database | option | trust | verify | vlan]

**authorized server:** *Enter the IP address of a trusted DHCP server. If no authorized servers are configured, all DHCP server addresses are considered valid. Maximum: 20 authorized servers*

**database:** *To configure a location for the lease database, enter a URL in the format **tftp://ip-addr/ascii-string**. The maximum number of characters for the URL is 63.*

**option:** *Add relay information option (Option 82) to DHCP client packets that are being forwarded out trusted ports. The default is **yes**, add relay information.*

**trust:** *Configure trusted ports. Only server packets received on trusted ports are forwarded. Default: **untrusted**.*

**verify:** *Enables DHCP packet validation. The DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or the packet is dropped. Default: **Yes***

**vlan:** *Enable DHCP snooping on a vlan. DHCP snooping must be enabled already. Default: **No***

To display the DHCP snooping configuration, enter this command:

```
ProCurve(config)# show dhcp-snooping
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping
DHCP Snooping Information
  DHCP Snooping           : Yes
  Enabled Vlans           :
  Verify MAC              : Yes
  Option 82 untrusted policy : drop
  Option 82 Insertion     : Yes
  Option 82 remote-id     : mac
  Store lease database    : Not configured
  Port Trust
  -----
  B1      No
  B2      No
  B3      No
```

**Figure 10. An Example of the DHCP Snooping Command Output**

To display statistics about the DHCP snooping process, enter this command:

```
ProCurve(config)# show dhcp-snooping stats
```

An example of the output is shown below.

```
ProCurve(config)# show dhcp-snooping stats
```

Packet type	Action	Reason	Count
server	forward	from trusted port	8
client	forward	to trusted port	8
server	drop	received on untrusted port	2
server	drop	unauthorized server	0
client	drop	destination on untrusted port	0
client	drop	untrusted option 82 field	0
client	drop	bad DHCP release request	0
client	drop	failed verify MAC check	0

**Figure 11. Example of Show DHCP Snooping Statistics**



## Enabling DHCP Snooping on VLANs

DHCP snooping on VLANs is disabled by default. To enable DHCP snooping on a VLAN or range of VLANs enter this command:

```
ProCurve(config)# dhcp-snooping vlan <vlan-id-range>
```

You can also use this command in the vlan context, in which case you cannot enter a range of VLANs for snooping.

Below is an example of DHCP snooping enabled on VLAN 4.

```
ProCurve(config)# dhcp-snooping vlan 4
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac
```

**Figure 12. Example of DHCP Snooping on a VLAN**

## Configuring DHCP Snooping Trusted Ports

By default, all ports are untrusted. To configure a port or range of ports as trusted, enter this command:

```
ProCurve(config)# dhcp-snooping trust <port-list>
```

You can also use this command in the interface context, in which case you are not able to enter a list of ports.

```
ProCurve(config)# dhcp-snooping trust B1-B2
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : Yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : mac

Store lease database : Not configured

Port  Trust
-----
B1    Yes
B2    Yes
B3    No
```

**Figure 13. Example of Setting Trusted Ports**

DHCP server packets are forwarded only if received on a trusted port; DHCP server packets received on an untrusted port are dropped.

Use the **no** form of the command to remove the trusted configuration from a port.

## Configuring Authorized Server Addresses

If authorized server addresses are configured, a packet from a DHCP server must be received on a trusted port AND have a source address in the authorized server list in order to be considered valid. If no authorized servers are configured, all servers are considered valid. You can configure a maximum of 20 authorized servers.

To configure a DHCP authorized server address, enter this command in the global configuration context:

```
ProCurve(config)# dhcp-snooping authorized-server
                  <ip-address>
```

```
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : No
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : subnet-ip

Authorized Servers
-----
111.222.3.4
10.0.0.11
```

**Figure 14. Example of Authorized Servers for DHCP Snooping**

## Using DHCP Snooping with Option 82

DHCP adds Option 82 (relay information option) to DHCP request packets received on untrusted ports by default. (See the preceding section *Configuring DHCP Relay* for more information on Option 82.)

When DHCP is enabled globally and also enabled on a VLAN, and the switch is acting as a DHCP relay, the settings for the DHCP relay Option 82 command are ignored when snooping is controlling Option 82 insertion. Option 82 inserted in this manner allows the association of the client's lease with the correct port, even when another device is acting as a DHCP relay or when the server is on the same subnet as the client.

---

### Note

DHCP snooping only overrides the Option 82 settings on a VLAN that has snooping enabled, not on VLANS without snooping enabled.

---

If DHCP snooping is enabled on a switch where an edge switch is also using DHCP snooping, it is desirable to have the packets forwarded so the DHCP bindings are learned. To configure the policy for DHCP packets from untrusted ports that already have Option 82 present, enter this command in the global configuration context.

**Syntax:** [no] dhcp-snooping option 82 [remote-id <mac | subnet-ip | mgmt-ip>]  
[untrusted-policy <drop | keep | replace>]

*Enables DHCP Option 82 insertion in the packet.*

**remote-id**     *Set the value used for the **remote-id** field of the relay information option.*

**mac:** *The switch mac address is used for the remote-id. This is the default.*

**subnet-ip:** *The IP address of the VLAN the packet was received on is used for the remote-id. If **subnet-ip** is specified but the value is not set, the MAC address is used.*

**mgmt-ip:** *The management VLAN IP address is used as the remote-id. If **mgmt-ip** is specified but the value is not set, the MAC address is used.*

**untrusted-policy**     *Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). The default is **drop**.*

**drop:** *The packet is dropped.*

**keep:** *The packet is forwarded without replacing the option information.*

**replace:** *The existing option is replaced with a new Option 82 generated by the switch.*

---

## Note

The default **drop** policy should remain in effect if there are any untrusted nodes, such as clients, directly connected to this switch.

---

## Changing the Remote-id from a MAC to an IP Address

By default, DHCP snooping uses the MAC address of the switch as the remote-id in Option 82 additions. The IP address of the VLAN the packet was received on or the IP address of the management VLAN can be used instead by entering this command with the associated parameter:

```
ProCurve(config)# dhcp-snooping option 82 remote-id  
                  <mac | subnet-ip | mgmt-ip>
```

```
ProCurve(config)# dhcp-snooping option 82 remote-id subnet-  
ip  
ProCurve(config)# show dhcp-snooping  
  
DHCP Snooping Information  
  
DHCP Snooping           : Yes  
Enabled Vlans           : 4  
Verify MAC               : Yes  
Option 82 untrusted policy : drop  
Option 82 Insertion      : Yes  
Option 82 remote-id      : subnet-ip
```

**Figure 15. Example of DHCP Snooping Option 82 using the VLAN IP Address**

## Disabling the MAC Address Check

DHCP snooping drops DHCP packets received on untrusted ports when the check address (chaddr) field in the DHCP header does not match the source MAC address of the packet (default behavior). To disable this checking, use the **no** form of this command.

```
ProCurve(config)# dhcp-snooping verify mac
```

```
ProCurve(config)# dhcp-snooping verify mac
ProCurve(config)# show dhcp-snooping

DHCP Snooping Information

DHCP Snooping           : Yes
Enabled Vlans           : 4
Verify MAC              : yes
Option 82 untrusted policy : drop
Option 82 Insertion     : Yes
Option 82 remote-id     : subnet-ip
```

**Figure 16. Example Showing the DHCP Snooping Verify MAC Setting**

## The DHCP Binding Database

DHCP snooping maintains a database of up to 8192 DHCP bindings on untrusted ports. Each binding consists of:

- Client MAC address
- Port number
- VLAN identifier
- Leased IP address
- Lease time

The switch can be configured to store the bindings at a specific URL so they will not be lost if the switch is rebooted. If the switch is rebooted, it will read its binding database from the specified location. To configure this location use this command.

**Syntax:** [no] dhcp-snooping database [file<tftp://<ip-address>/<ascii-string>>]  
[delay<15-86400>][timeout<0-86400>]

<b>file</b>	<i>Must be in Uniform Resource Locator (URL) format — “tftp://ip-address/ascii-string”. The maximum filename length is 63 characters.</i>
<b>delay</b>	<i>Number of seconds to wait before writing to the database. Default = 300 seconds.</i>
<b>timeout</b>	<i>Number of seconds to wait for the database file transfer to finish before returning an error. A value of zero (0) means retry indefinitely. Default = 300 seconds.</i>

A message is logged in the system event log if the DHCP binding database fails to update.

To display the contents of the DHCP snooping binding database, enter this command.

**Syntax:** show dhcp-snooping binding

```
ProCurve(config)# show dhcp-snooping binding
```

MacAddress	IP	VLAN	Interface	Time left
22.22.22.22.22.22	10.0.0.1	4	B2	1600

**Figure 17. Example Showing DHCP Snooping Binding Database Contents**

---

## Note

If a lease database is configured, the switch drops all DHCP packets until the lease database is read. This only occurs when the switch reboots and is completed quickly. If the switch is unable to read the lease database from the tftp server, it waits until that operation times out and then begins forwarding DHCP packets.

---

## Enabling Debug Logging

To enable debug logging for DHCP snooping, use this command.

**Syntax:** [no] debug dhcp-snooping [agent | event | packet]

- agent**      *Displays DHCP snooping agent messages.*
- event**      *Displays DHCP snooping event messages.*
- packet**     *Displays DHCP snooping packet messages.*

## Operational Notes

- DHCP is not configurable from the web management interface or menu interface.
- If packets are received at too high a rate, some may be dropped and need to be re-transmitted.
- ProCurve recommends running a time synchronization protocol such as SNTP in order to track lease times accurately.
- A remote server must be used to save lease information or there may be a loss of connectivity after a switch reboot.

## Log Messages

**Server <ip-address> packet received on untrusted port <port-number> dropped.** Indicates a DHCP server on an untrusted port is attempting to transmit a packet. This event is recognized by the reception of a DHCP server packet on a port that is configured as untrusted.

**Ceasing untrusted server logs for %s.** More than one packet was received from a DHCP server on an untrusted port. To avoid filling the log file with repeated attempts, untrusted server drop packet events will not be logged for the specified <duration>.

**Client packet destined to untrusted port <port-number> dropped.** Indicates that the destination of a DHCP client unicast packet is on an untrusted port. This event is recognized when a client unicast packet is dropped because the destination address is out a port configured as untrusted.

**Ceasing untrusted port destination logs for %s.** More than one client unicast packet with an untrusted port destination was dropped. To avoid filling the log file with repeated attempts, untrusted port destination attempts will not be logged for the specified <duration>.

**Unauthorized server <ip-address> detected on port <port-number>.** Indicates that an unauthorized DHCP server is attempting to send packets. This event is recognized when a server packet is dropped because there are configured authorized servers and a server packet is received from a server that is not configured as an authorized server.

**Ceasing unauthorized server logs for <duration>.** More than one unauthorized server packet was dropped. To avoid filling the log file with repeated attempts, unauthorized server transmit attempts will not be logged for the specified <duration>.

**Received untrusted relay information from client <mac-address> on port <port-number>.** Indicates the reception on an untrusted port of a client packet containing a relay information option field. This event is recognized when a client packet containing a relay information option field is dropped because it was received on a port configured as untrusted.

**Ceasing untrusted relay information logs for <duration>.** More than one DHCP client packet received on an untrusted port with a relay information field was dropped. To avoid filling the log file with repeated attempts, untrusted relay information packets will not be logged for the specified <duration>.

**Client address <mac-address> not equal to source MAC <mac-address> detected on port <port-number>.** Indicates that a client packet source MAC address does not match the “chaddr” field. This event is recognized when the dhcp-snooping agent is enabled to filter DHCP client packets that do not have a matching “chaddr” field and source MAC address.

**Ceasing MAC mismatch logs for <duration>.** More than one DHCP client packet with a mismatched source MAC and chaddr field was dropped. To avoid filling the log file with repeated attempts, client address mismatch events will not be logged for the specified <duration>.



## Enhancements

### Release L.10.10 Enhancements

**Attempt to release address <ip-address> leased to port <port-number> detected on port <port-number> dropped.** Indicates an attempt by a client to release an address when a DHCPRELEASE or DHCPDECLINE packet is received on a port different from the port the address was leased to.

**Ceasing bad release logs for %s.** More than one bad DHCP client release packet was dropped. To avoid filling the log file with repeated bad release dropped packets, bad releases will not be logged for <duration>.

**Lease table is full, DHCP lease was not added.** The lease table is full and this lease will not be added to it.

**Write database to remote file failed errno (error-num).** An error occurred while writing the temporary file and sending it using tftp to the remote server.

**DHCP packets being rate-limited.** Too many DHCP packets are flowing through the switch and some are being dropped.

**Snooping table is full.** The DHCP binding table is full and subsequent bindings are being dropped.

## Release L.10.10 Enhancements

Release L.10.10 includes the following enhancements:

- **Enhancement (PR\_1000351445)**— The "show tech transceiver" CLI command output now contains the HP part number and revision information for all transceivers on the switch..

## Release L.10.11 Enhancements

*No enhancements, software fixes only.*

**NOTE:** Versions L.10.12 through L.10.19 were never built. The code branched to L.10.20 with no intervening releases.

## Release L.10.20 Enhancements

The enhancements included in Release L.10.20 are listed below along with a link to the page where you can find a description related to its implementation if applicable.

- **Enhancement (PR\_1000336169)** — Added support for STP Per Port BPDU Filtering and SNMP Traps. See “Spanning Tree Per-Port BPDU Filtering” on page 46.
- **Enhancement (PR\_1000346164)** — When this feature is enabled on a port, the switch will disable (drop link) a port that receives a spanning tree BPDU, log a message, and optionally send an SNMP TRAP. See “Spanning Tree BPDU Protection” on page 49.
- **Enhancement (PR\_1000313819)** — RADIUS Configuration via SNMP. For details refer to “Using SNMP To View and Configure Switch Authentication Features” on page 51.
- **Enhancement (PR\_100292455)** — Rate display for ports on CLI. New command: "show interface port-utilization", not available on Menu nor Web Interface.
- **Enhancement (PR\_1000311510)** — Ping conformance as defined in RFC 2925.
- **Enhancement (PR\_1000331027)** — TCP/UDP port closure enhancement. See “TCP/UDP Port Closure” on page 54.
- **Enhancement (PR\_1000330743)** — Denial of Service logging enhancement with implementation of Instrumentation Monitor. See “Instrumentation Monitor” on page 56.
- **Enhancement (PR\_1000338847)** - Added support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3. See “Adding SNMPv3 Users With AES” on page 60.
- **Enhancement (PR\_1000339546)** - Addition of the "clear log" CLI command.
- **Enhancement (PR\_1000374085)** - This enhancement expands the use of the Controlled Directions parameter to also support mac/web authentication. Refer to “Configuring 802.1X Controlled Directions” on page 31 for details on using the Controlled Directions parameter. This enhancement includes support for MAC authentication and Web authentication configured with the **aaa port-access controlled-directions** command. For additional information about how to configure and use MAC and Web authentication, refer to the *Access and Security Guide* for your switch.
- **Enhancement (PR\_1000376406)** - Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration. See “Configuring Loop Protection” on page 61.
- **Enhancement (PR\_1000358900)** — A RADIUS accounting enhancement was made.

## Spanning Tree Per-Port BPDU Filtering

The STP BPDU filter feature allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets and stay locked in the spanning-tree forwarding state. All other ports will maintain their role.

Here are some sample scenarios in which this feature may be used:

- To have STP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.
- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of standard spanning-tree operations.
- To protect the network from denial of service attacks with spoofing spanning-tree BPDUs by dropping incoming BPDU frames.

---

### Note

BPDU protection imposes a more secure mechanism that implements port shut down and a detection alert when an errant BPDU frame is received (see page 49 for details). BPDU protection will take precedence over BPDU filtering if both features have been enabled on the same port.

---

## Configuring STP BPDU Filters

The following commands allow you to configure BPDU filters via the CLI.

**Syntax:** [no] spanning-tree <port-list | all> bpdu-filter

*Enables/disables the BPDU filter feature on the specified port(s).*

For example, to configure BPDU filtering on port a9, enter:

```
ProCurve(config)# spanning-tree a9 bpdu-filter
```

---

### Caution

Ports configured with the BPDU filter mode remain active (learning and forward frames); however, spanning-tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and remove ("no") the bpdu-filter.

## Viewing Status of BPDU Filtering

The **show spanning-tree <port-list> detail** command has been extended to show per-port BPDU filter mode as shown below.

```

ProCurve# show spanning-tree a9 detail

Status and Counters - CST Port(s) Detailed Information

Port                : A1
Status              : Up
BPDU Filtering      : Yes
Errant BPUDUs received : 65
MST Region Boundary : Yes
External Path Cost  : 200000
External Root Path Cost : 420021
Administrative Hello Time : Use Global
Operational Hello Time  : 2
AdminEdgePort       : No
OperEdgePort        : No
AdminPointToPointMAC : Force-True
OperPointToPointMAC  : Yes
Aged BPDUs Count    : 0
Loop-back BPDUs Count : 0
TC ACK Flag Transmitted : 0
TC ACK Flag Received  : 0

MST          MST          CFG          CFG          TCN          TCN
BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx
-----
8           28          0           0           0           0
  
```

The diagram includes two callout boxes with arrows pointing to specific fields in the command output:

- A grey callout box with the text "Rows indicating BPDU filtering has been enabled and number of errant BPUDUs received." has an arrow pointing to the "BPDU Filtering : Yes" and "Errant BPUDUs received : 65" lines.
- A grey callout box with the text "Column indicating BPDU frames accepted for processing when permitted by BPDU filter." has an arrow pointing to the "MST BPDUs Rx" column in the summary table, which shows a value of 28.

**Figure 18. Example of BPDU Filter Fields in Show Spanning Tree Detail Command**

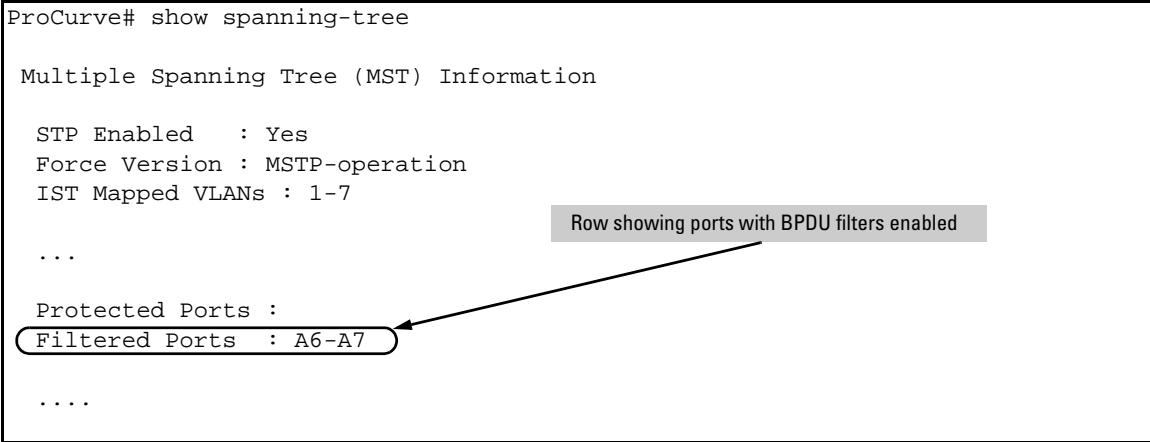
The **show spanning-tree** command has also been extended to display BPDU filtered ports.

```
ProCurve# show spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-7
...

Protected Ports :
Filtered Ports   : A6-A7
....
```

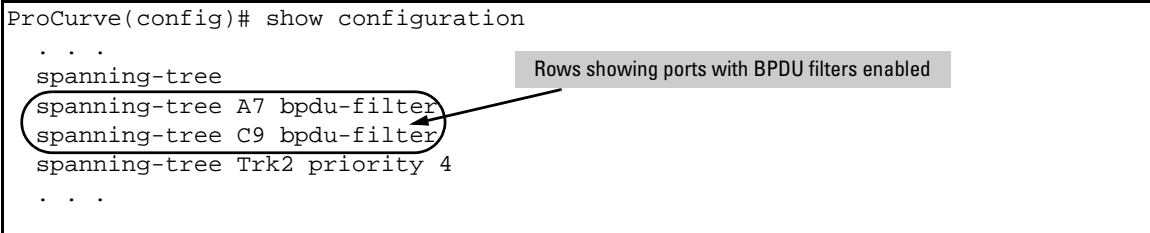


**Figure 19. Example of BPDU Filtered Ports Field in Show Spanning Tree Command**

### Viewing Configuration of BPDU Filtering

The BPDU filter mode adds an entry to the spanning tree category within the configuration file.

```
ProCurve(config)# show configuration
. . .
spanning-tree
spanning-tree A7 bpdu-filter
spanning-tree C9 bpdu-filter
spanning-tree Trk2 priority 4
. . .
```



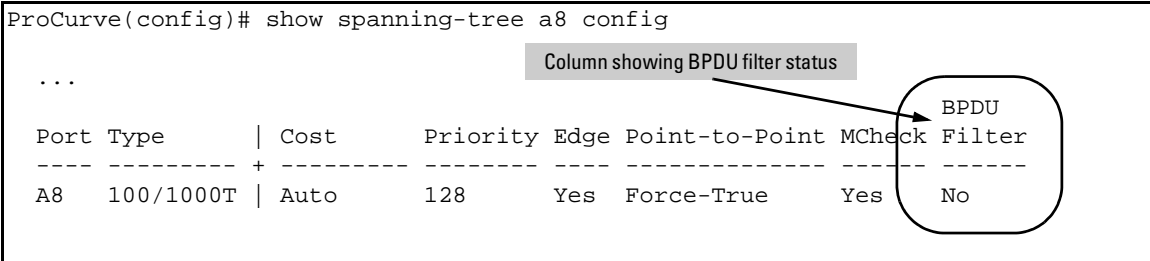
**Figure 20. Example of BPDU Filters in the Show Configuration Command**

The **spanning-tree show < port> configuration** command displays the BPDU's filter state.

```
ProCurve(config)# show spanning-tree a8 config

...

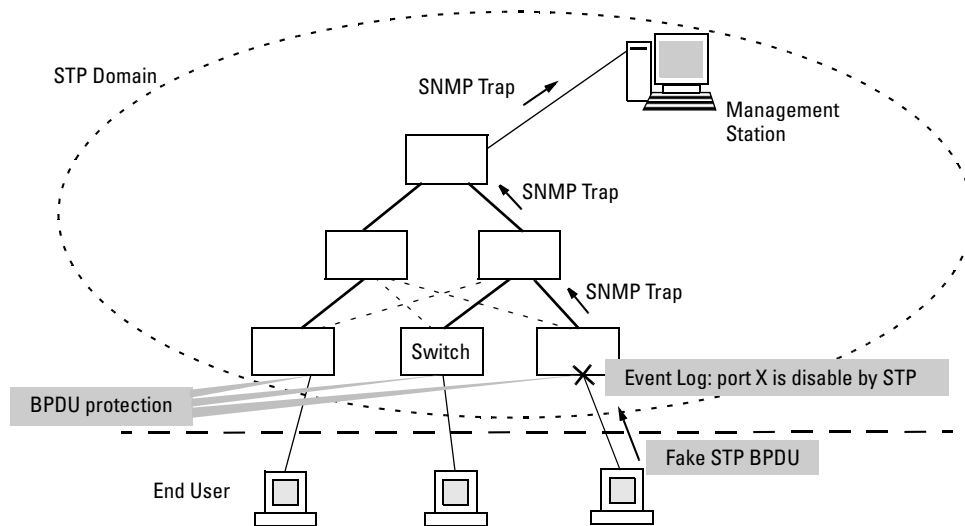
Port Type          | Cost      Priority Edge Point-to-Point MCheck Filter
-----+-----
A8 100/1000T | Auto     128    Yes  Force-True    Yes    No
```



**Figure 21. Example of BPDU Filter Status in Show Spanning Tree Configuration Command**

## Spanning Tree BPDU Protection

The BPDU protection feature is a security enhancement to Spanning Tree Protocol (STP) operation. It can be used to protect the active STP topology by delimiting its legal boundaries, thereby preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection would be applied to edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, the feature will disable that port and alert the network manager via an SNMP trap as shown in Figure 22.



**Figure 22. Example of BPDU Protection Enabled at the Network Edge**

## Terminology

**BPDU** — Acronym for bridge protocol data unit. BPDUs are data messages that are exchanged between the switches within an extended LAN that use a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by placing redundant switch ports in a backup, or blocked, state.

**BPDU Filtering** — Spanning-tree configuration mode that prevents the switch from receiving and transmitting BPDU frames on a specific port.

**BPDU Protection** — Spanning-tree configuration mode which disables a port where BPDU frames are received.

**MSTP** — Multiple Spanning Tree Protocol, defined in IEEE 802.1s. Each MSTI (multiple spanning tree instance) on a physical port provides loop free connectivity for the group of VLANs associated with that instance. This means that traffic transported on different VLANs can be distributed for load-balancing among links between switches.

**RSTP** — Rapid Spanning Tree Protocol, defined in IEEE 802.1w and ratified in IEEE 802.1D-2004.

**Spanning-tree** — Generic term to refer to the many spanning-tree flavors: now deprecated STP, RSTP and VLAN-aware MSTP.

**STP** — Spanning Tree Protocol, part of the original IEEE 802.1D specification. The 2004 edition completely deprecates STP. Both RSTP and MSTP have fallback modes to handle STP.

**SNMP** — Simple Network Management Protocol, used to remotely manage network devices.

---

## Note

The switches covered in these Release Notes, use the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Under standard settings, your MSTP-configured switch interoperates effectively with both STP (IEEE 802.1D) and RSTP (IEEE 802.1w) spanning-tree devices. For more information, refer to the chapter entitled *Multiple Instance Spanning-Tree Operation* in the *Advanced Traffic Management Guide* for your switch.

---

## Configuring BPDU Protection

The following commands allow you to configure BPDU protection via the CLI.

**Syntax:** [no] spanning-tree <port-list> bpdu protection

*Enables/disables the BPDU protection feature on a port*

**Syntax:** [no] spanning-tree traps errant bpdu

*Enables/disables the sending of errant BPDU traps.*

For example, to configure BPDU protection on ports 1 to 10, enter:

```
ProCurve(config)# spanning-tree 1-10 bpdu protection
```

When BPDU protection is enabled, the following steps are set in process:

1. When an STP BPDU packet is received, STP treats it as an unauthorized transmission attempt and shuts down the port that the BPDU came in on.
2. An event message is logged and an SNMP notification trap is generated.
3. The port remains disabled until re-enabled manually by a network administrator.

---

## Caution

This command should only be used to guard edge ports that are not expected to participate in STP operations. Once BPDU protection is enabled, it will disable the port as soon as any BPDU packet is received on that interface.

---

## Viewing BPDU Protection Status

The **show spanning-tree** command has additional information on BPDU protection as shown below.

```
ProCurve# show spanning-tree 1-10

Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-7

...

Protected Ports : 3-7,9
Filtered Ports  : 10
```

Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP	Edge
1	100/1000T	200000	128	Forwarding	000883-024500	2	Yes	No
2	100/1000T	200000	128	Forwarding	000883-122740	2	Yes	No
3	100/1000T	200000	128	BpduError		2	Yes	Yes
4	100/1000T	Auto	128	Disabled				
5	100/1000T	200000	128	Forwarding		2	Yes	Yes
6	100/1000T	200000	128	Forwarding		2	Yes	Yes
7	100/1000T	200000	128	Forwarding		2	Yes	Yes
8	100/1000T	Auto	128	Disabled				
9	100/1000T	Auto	128	Disabled				
10	100/1000T	200000	128	Forwarding		2	Yes	Yes

**Figure 23. Example of BPDU Protection Additions to Show Spanning Tree Command**

## 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 L.10.20, the 4200 switches allow, by default, manager-only SNMP read/write access to a subset of the authentication MIB objects for the following features:



## Enhancements

### Release L.10.20 Enhancements

- 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 [“Switch Management Access 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 [“SNMP Access \(Simple Network Management Protocol\)” on page 10](#).)

---

## 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.

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

SNMP Communities

Community Name	MIB View	Write Access
public	Manager	Unrestricted

Trap Receivers

Link-Change Traps Enabled on Ports [All] : All

Send Authentication Traps [No] : No

Address	Community	Events Sent in Trap
---------	-----------	---------------------

[Excluded MIBs]

[hpSwitchAuthenticationMIB]

This command disables SNMP security MIB access.

Indicates that SNMP security MIB access is disabled, which is the nondefault setting.

**Figure 24. 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 #L.10.20

hostname "ProCurve"
[snmp-server mib hpSwitchAuthMIB excluded ] ← Indicates that SNMP access
ip default-gateway 10.10.24.55           to the authentication
snmp-server community "public" Operator configuration MIB
vlan 1                                   (hpSwitchAuth) is disabled.
  name "DEFAULT_VLAN"
  untagged 1-26
  ip address 10.10.24.100 255.255.255.0
  exit
password manager
```

**Figure 25. Using the show run Command to View the Current Authentication MIB Access State**

## TCP/UDP Port Closure

In earlier software releases, certain UDP ports were always open. Beginning with software release L.10.20, all TCP/UDP ports on the 3400cl switches will remain closed until the associated services are enabled on the switch.

The following ports and services are affected by this change:

Port	Service
69	TFTP
161	SNMP
520	RIP
1507	Stacking (SNMP)

To open any of these ports, the respective services must first be enabled on the switch. For information on how to enable/disable these services, refer to the following command listings . For details on each service, refer to the latest version of the switch's software documentation available on the ProCurve Networking Web site.

## Enabling/Disabling TFTP

The TFTP server and client can be enabled and/or disabled independently.

**Syntax:** [no] tftp < client | server >

*Enables or disables the TFTP client.*

**client:** *Enables or disables the TFTP client.*

*(Default: disabled)*

**server:** *Enables or disables the TFTP server.*

*(Default: disabled)*

**Note:** Both the **tftp** command (with no arguments) and the **tftp client** command can be used to enable or disable the tftp client.

## Enabling/Disabling SNMP

To enable/disable SNMP, use the following commands.

**Syntax:** [no] snmp-server enable

*Enables or disables SNMP v1/v2.*

*(Default: disabled)*

**Syntax:** [no] snmpv3 enable

*Enables or disables SNMP v3.*

*(Default: disabled)*

---

## Notes

- The SNMP port (161) will be opened if either SNMP v1/2 or SNMP v3 are enabled, or remain closed if both are disabled.
- The **snmp-server enable** command takes precedence over the **snmp-server enable traps** command that is used to enable or disable authentication traps to be sent when a management station attempts an unauthorized access.
- If SNMP is disabled, both the SNMP port (161) and the stacking port (1507) will remain closed.

---

## Enabling/Disabling RIP

To enable/disable RIP, use the following command.

**Syntax:** [no] router rip

*Enables, disables, or configures Routing Internet Protocol (RIP) on the switch.*

*(Default: disabled)*

---

## Note

The **router rip** command exists in previous software versions. In this implementation, however, RIP must be enabled in order to open the port on the switch.

---

## Enabling/Disabling Stacking

To enable/disable stacking, use the following command.

**Syntax:** [no] stack

*Enables stacking (SNMP) on the switch. (Default: disabled)*

---

### Note

The **stack** command exists in previous software versions. In this implementation, however, both stacking and SNMP must be enabled to open the port on the switch. If either feature is disabled, the port will remain closed.

---

## Instrumentation Monitor

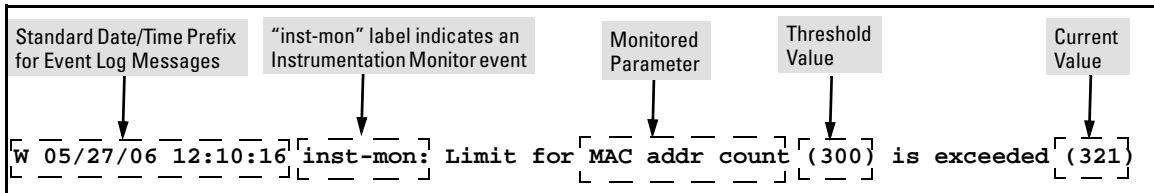
The 3400cl switches have instrumentation to monitor many operating parameters at pre-determined intervals. Beginning with software release L.10.20, this capability can be used to detect anomalies caused by security attacks or other irregular operations on the switch. The following table shows the parameters that can be monitored, and the possible security attacks that may trigger an alert:

Parameter Name	Description
pkts-to-closed-ports	The count of packets per minute sent to closed TCP/UDP ports. An excessive amount of packets could indicate a port scan, in which an attacker is attempting to expose a vulnerability in the switch.
arp-requests	The count of ARP requests processed per minute. A large amount of ARP request packets could indicate a host infected with a virus that is trying to spread itself.
ip-address-count	The number of destination IP addresses learned in the IP forwarding table. Some attacks fill the IP forwarding table causing legitimate traffic to be dropped.
system-resource-usage (Denial of Service logging)	The percentage of system resources in use. Some Denial-of-Service (DoS) attacks will cause excessive system resource usage, resulting in insufficient resources for legitimate traffic.
login-failures/min	The count of failed CLI login attempts or SNMP management authentication failures. This indicates an attempt has been made to manage the switch with an invalid login or password. Also, it might indicate a network management station has not been configured with the correct SNMP authentication parameters for the switch.
port-auth-failures/min	The count of times a client has been unsuccessful logging into the network
system-delay	The response time, in seconds, of the CPU to new network events such as BPDU packets or packets for other network protocols. Some DoS attacks can cause the CPU to take too long to respond to new network events, which can lead to a breakdown of Spanning Tree or other features. A delay of several seconds indicates a problem.
mac-address-count	The number of MAC addresses learned in the forwarding table. Some attacks fill the forwarding table so that new conversations are flooded to all parts of the network.

Parameter Name	Description
mac-moves/min	The average number of MAC address moves from one port to another per minute. This usually indicates a network loop, but can also be caused by DoS attacks.
learn-discards/min	Number of MAC address learn events per minute discarded to help free CPU resources when busy.

## Operating Notes

- To generate alerts for monitored events, you must enable the instrumentation monitoring log and/or SNMP trap. The threshold for each monitored parameter is configurable and can be adjusted to minimize false alarms (see “[Configuring Instrumentation Monitor](#)” on page 58).
- When a parameter exceeds its threshold, an alert (event log message and/or SNMP trap) is generated to inform network administrators of this condition. The following example shows an event log message that occurs when the number of MAC addresses learned in the forwarding table exceeds the configured threshold:



**Figure 26. Example of Event Log Message generated by Instrumentation Monitor**

- Alerts are automatically rate limited to prevent filling the log file with redundant information. The following is an example of alerts that occur when the device is continually subject to the same attack (too many MAC addresses in this instance):

```

W 01/01/90 00:05:00 inst-mon: Limit for MAC addr count (300) is exceeded (321)
W 01/01/90 00:10:00 inst-mon: Limit for MAC addr count (300) is exceeded (323)
W 01/01/90 00:15:00 inst-mon: Limit for MAC addr count (300) is exceeded (322)
W 01/01/90 00:20:00 inst-mon: Limit for MAC addr count (300) is exceeded (324)
W 01/01/90 00:20:00 inst-mon: Ceasing logs for MAC addr count for 15 minutes

```

**Figure 27. Example of the rate limiting that occurs when multiple messages are generated**

In the preceding example, if a condition is reported 4 times (persists for more than 15 minutes) then alerts cease for 15 minutes. If after 15 minutes the condition still exists, the alerts cease for 30 minutes, then for 1 hour, 2 hours, 4 hours, 8 hours, and after that the persisting condition is reported once a day. Note that ProCurve switches also have the ability to send event log entries to a syslog server.

## Known Limitations

As of release L.10.20, the instrumentation monitor runs once every five minutes. The current implementation does not track information such as the port, MAC, and IP address from which an attack is received.

## Configuring Instrumentation Monitor

The following commands and parameters are used to configure the operational thresholds that are monitored on the switch. By default, the instrumentation monitor is disabled.

**Syntax:** [no] instrumentation monitor [parameterName{all}] [<low|med|high|limitValue>]

**[log]** : Enables/disables instrumentation monitoring log so that event log messages are generated every time there is an event which exceeds a configured threshold.  
(Default threshold setting when instrumentation monitoring is enabled: **enabled**)

**[all]** : Enables/disables all counter types on the switch but does not enable/disable instrumentation monitor logging.  
(Default threshold setting when enabled: **see parameter listings below**)

**[arp-requests]** : The number of arp requests that are processed each minute.  
(Default threshold setting when enabled: **1000 (med)**)

**[ip-address-count]**: The number of destination IP addresses learned in the IP forwarding table.  
(Default threshold setting when enabled: **1000 (med)**)

**[learn-discards]** : The number of MAC address learn events per minute discarded to help free CPU resources when busy.  
(Default threshold setting when enabled: **100 (med)**)

**[login-failures]** : The count of failed CLI login attempts or SNMP management authentication failures per hour.  
(Default threshold setting when enabled: **10 (med)**)

**[mac-address-count]** : The number of MAC addresses learned in the forwarding table. You must enter a specific value in order to enable this feature.  
(Default threshold setting when enabled: **1000 (med)**)

**[mac-moves]** : The average number of MAC address moves per minute from one port to another.  
(Default threshold setting when enabled: **100 (med)**)

**[pkts-to-closed-ports]** : The count of packets per minute sent to closed TCP/UDP ports.  
(Default threshold setting when enabled: **10 (med)**)

**[port-auth-failures]** : The count of times per minute that a client has been unsuccessful logging into the network.  
(Default threshold setting when enabled: **10 (med)**)

**[system-resource-usage]**: The percentage of system resources in use.  
(Default threshold setting when enabled: **50 (med)**)

**[system-delay]** : The response time, in seconds, of the CPU to new network events such as BPDU packets or packets for other network protocols.  
(Default threshold setting when enabled: **3 seconds (med)**)

**[trap]** : Enables or disables SNMP trap generation.  
(Default setting when instrumentation monitoring is enabled: **disabled**)

To enable instrumentation monitor using the default parameters and thresholds, enter the general **instrumentation monitor** command. To adjust specific settings, enter the name of the parameter that you wish to modify, and revise the threshold limits as needed.

## Examples

To turn on monitoring and event log messaging with the default medium values:

```
ProCurve(config)# instrumentation monitor
```

To turn off monitoring of the system delay parameter:

```
ProCurve(config)# no instrumentation monitor system-delay
```

To adjust the alert threshold for the MAC address count to the low value:

```
ProCurve(config)# instrumentation monitor mac-address-count low
```

To adjust the alert threshold for the MAC address count to a specific value:

```
ProCurve(config)# instrumentation monitor mac-address-count 767
```

To enable monitoring of learn discards with the default medium threshold value:

```
ProCurve(config)# instrumentation monitor learn-discards
```

To disable monitoring of learn discards:

```
ProCurve(config)# no instrumentation monitor learn-discards
```

To enable or disable SNMP trap generation:

```
ProCurve(config)# [no] instrumentation monitor trap
```

## Viewing the Current Instrumentation Monitor Configuration

The **show instrumentation monitor configuration** command displays the configured thresholds for monitored parameters, as shown in figure 28 on the next page.

An alternate method of determining the current Instrumentation Monitor configuration is to use the **show run** command. However, the show run command output does not display the threshold values for each limit setting.



```
ProCurve# show instrumentation monitor configuration

PARAMETER                                LIMIT
-----
mac-address-count                        1000 (med)
ip-address-count                         1000 (med)
system-resource-usage                    50 (med)
system-delay                             5 (high)
mac-moves/min                            100 (med)
learn-discards/min                       100 (med)
ip-port-scans/min                        10 (med)
arp-requests/min                         100 (low)
login-failures/min                       10 (med)
port-auth-failures/min                   10 (med)

SNMP trap generation for alerts: enabled
Instrumentation monitoring log : enabled
```

**Figure 28. Viewing the Instrumentation Monitor Configuration**

## Adding SNMPv3 Users With AES

To use SNMPv3 on the switch, you must configure the users that will be assigned to different groups. To configure SNMP users on the switch:

1. Configure users in the User Table with the **snmpv3 user** command. To view the list of configured users, enter the **show snmpv3 user** command.
2. Assign users to Security Groups based on their security model with the **snmpv3 group** command .

Refer to the chapter titled “Configuring for Network Management Applications” in the *Management and Configuration Guide* for your switch for details on adding SNMPv3 users.

---

### Caution

If you add an SNMPv3 user without authentication and/or privacy to a group that requires either feature, the user will not be able to access the switch. Ensure that you add a user with the appropriate security level to an existing security group.

To configure an SNMPv3 user, you must first add the user name to the list of known users with the **snmpv3 user** command.

## SNMPv3 User Commands

**Syntax:** [no] snmpv3 user <user\_name>

*Adds or deletes a user entry for SNMPv3. Authorization and privacy are optional, but to use privacy, you must use authorization. When you delete a user, only the <user\_name> is required.*

[auth <md5 | sha> <auth\_pass>]

*With authorization, you can set either MD5 or SHA authentication. The authentication password <auth\_pass> must be 6-32 characters in length and is mandatory when you configure authentication. Default: None*

[priv <des | aes> <priv\_pass>]

*With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption. The privacy password <priv\_pass> must be 6-32 characters in length and is mandatory when you configure privacy.  
Default: DES*

**Note:** *Only AES 128-bit and DES 56-bit encryption are supported as privacy protocols. Other non-standard encryption algorithms, such as AES-172, AES-256, and 3-DES are not supported.*

**Listing Users.** To display the management stations configured to access the switch with SNMPv3 and view the authentication and privacy protocols that each station uses, enter the **show snmpv3 user** command.

**Syntax:** show snmpv3 user

## Configuring Loop Protection

You can use BPDU protection for systems that have spanning tree enabled (See [“Spanning Tree BPDU Protection” on page 49](#)), however, the BPDU protection feature cannot detect the formation of loops when an unmanaged device on the network drops spanning tree packets. To protect against the formation of loops in these cases, you can enable the Loop Protection feature, which provides protection by transmitting loop protocol packets out ports on which loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet on a port that has **send-disable** configured, it shuts down the port from which the packet was sent.

You can configure the **disable-timer** parameter for the amount of time you want the port to remain disabled (0 to 604800 seconds). If you configure a value of zero, the port will not be re-enabled.

To enable loop protection, enter this command:

```
ProCurve(config)# loop-protect <port-list>
```

**Syntax:** [no] loop-protect <port-list> [receiver-action <send-disable | no-disable> ]  
[transmit-interval <1-10> ] | [disable-timer <0-604800>] |  
[trap <loop-detected>]

*Allows you to configure per-port loop protection on the switch.*

[receiver-action <send-disable | no-disable>]

*Sets the action to be taken when a loop is detected on the port. The port that received the loop protection packet determines what action is taken. If send-disable is configured, the port that transmitted the packet is disabled. If no-disable is configured, the port is not disabled.*

*Default: send-disable*

[trap <loop-detected>]

*Allows you to configure loop protection traps The “loop-detected” trap indicates that a loop was detected on a port.*

[disable-timer <0-604800>]

*How long (in seconds) a port is disabled when a loop has been detected. A value of zero disables the auto re-enable functionality.*

*Default: Timer is disabled*

[transmit-interval <1-10>]

*Allows you to configure the time in seconds between the transmission of loop protection packets.*

*Default: 5 seconds*

To display information about ports with loop protection, enter this command.

**Syntax:** show loop-protect <port-list>

*Displays the loop protection status. If no ports are specified, the information is displayed only for the ports that have loop protection enabled.*

```
ProCurve(config)# show loop-protect 1-4

Status and Counters - Loop Protection Information

Transmit Interval (sec) : 5
Port Disable Timer (sec) : 5
Loop Detected Trap      : Enabled
```

Port	Loop Protection	Loop Detected	Loop Count	Time Since Last Loop	Rx Action	Port Status
1	Yes	No	0		send-disable	Up
2	Yes	No	0		send-disable	Up
3	Yes	No	0		send-disable	Up
4	Yes	No	0		send-disable	Up

**Figure 29. Example of Show Loop Protect Display**

## Release L.10.23 Enhancements

***Versions L.10.21 and L.10.22 were never released.***

Release L.10.23 includes the following enhancements:

- **Enhancement** — Support for the following products was added:
  - J8768A - ProCurve Switch vl 24-port Gig-T Module
  - J9030A - ProCurve Switch 4208vl-72GS 68 10/100/1000 + 4 SFP
  - J9033A - ProCurve Switch vl 20-port Gig-T + 4-port SFP Module
  - J9064A - ProCurve Switch 4204vl-48GS 44 10/100/1000 + 4 SFP

## Release L.10.24 Enhancements

Release L.10.24 includes the following enhancements:

- **Enhancement (PR\_1000373226)** - Support was added for a future SFP transceiver.
- **Enhancement (PR\_1000379804)** - Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Enhancement (PR\_1000385565)** - (CLI) The port security MAC address limit per port has been increased from 8 to 32 when learn mode is 'static' or 'configured'. However, the global limit of static/configured MAC addresses per ProCurve Series 4200vl switch is 208.
- **Enhancement (PR\_1000335860)** - This enhancement provides a configuration option for the source IP address field of SNMP response and generated trap PDUs.

### Configuring the Source IP Address for SNMP Requests and Traps

The switch uses the interface IP address as the source IP address in the IP header when sending a response to SNMP requests. For multi-netted interfaces, the source IP address is the outgoing interface IP address, which may be different from the IP address in the destination field of the IP header of the request. It is sometimes desirable for security reasons to send SNMP replies from the same IP address as the one on which the corresponding SNMP request was received. You can configure this capability with the **snmp-server response-source** and **snmp-server trap-source** commands.

**Syntax:** [no] snmp-server response-source [dst-ip-of-request | IP-ADDR | loopback<0-7>]

*Allows you to specify the source IP address of the SNMP response pdu. The default SNMP response pdu uses the IP address of the active interface from which the SNMP response was sent as the source IP address.*

*The **no** form of the command resets the switch to the default behavior (compliant with rfc-1517).*

*Default: Interface IP address*

**dst-ip-of-request:** *The destination IP address of the SNMP request pdu that will be used as the source IP address in the SNMP response pdu.*

**IP-ADDR:** *The user-specified IP address that will be used as the source IP address in the SNMP response pdu.*

**loopback <0-7>:** *The IP address configured for the specified loopback interface will be used as the source IP address in the SNMP response pdu. In the case of multiple addresses, the lowest alphanumeric address will be used.*

For example, to use the destination IP address as the source IP address, enter this command:

```
ProCurve(config)# snmp-server response-source dst-ip-of-request
```

To configure the source IP address for a generated trap pdu, enter this command.

**Syntax:** [no] snmp-server trap-source [ IP-ADDR | loopback<0-7>]

*Allows you to specify the source IP address for the trap pdu. The **no** form of the command resets the switch to the default behavior (compliant with rfc-1517).*

*Default: Interface IP address*

**IP-ADDR:** *The user-specified IP address that will be used as the source IP address in the generated trap.*

**loopback <0-7>:** *The IP address configured for the specified loopback interface will be used as the source IP address in the generated trap pdu. In the case of multiple addresses, the lowest alphanumeric address will be used.*

---

## Note

The **snmp-server response-source** and **snmp-server trap-source** commands configure the source IP address for IPv4 interfaces only.

---

The **show snmp-server** command displays the policy configuration.

## Software Fixes in Release L.10.01 - L.10.24

---

Software fixes are listed in chronological order, oldest to newest software release. To review the list of fixes included since the last general release that was published, begin with [“Release L.10.10” on page 71](#).

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

Release L.10.01 was the first software release for the ProCurve 4200vl Series.

---

### Release L.10.02

#### Problems Resolved in Release L.10.02

- **Crash/802.1X (PR\_1000302284)** — When 802.1X and MAC Authentication are both configured, the switch may crash with a message similar to:  

```
"SubSystem 4096 went down: 01/01/90 00:22:09 NMI event
SW:IP=0x003870a4 MSR:0x0024b032 LR:0x203081b0 Task='mWebAuth' Task
ID=0x12b4fa8 cr: 0x42000220 sp:0x012b6be8 xer:0x0100000f".
```
  - **Crash/Stacking (PR\_1000297510)** — When using Web User Interface and the switch is commander for stacking, the switch may crash with a message similar to:  

```
PPC Bus Error exception vector 0x300: Stack-frame=0x01731de8 HW
Addr=0x02800007 IP=0x0022dc30 Task='tHttptd' Task ID=0x1731fb0 fp:
0x0167d180 sp:0x01731ea8 lr:0x
```
  - **IGMP (PR\_1000301557)** — Data-driven IGMP requires an IP address on a VLAN to work properly.
  - **IP Forwarding (PR\_1000305739)** — When a user attempts to configure 'ip forward-protocol netbios-dgm', the switch incorrectly configures 'ip forward-protocol netbios-ns' instead.
  - **LACP (PR\_1000302457)** — Although default behavior is LACP disabled on all ports, upon bootup the switch event log reports, "lACP: Passive Dynamic LACP enabled on all ports".
  - **MSTP Enhancement (PR\_1000314692)** — Added new commands: “spanning-tree legacy-path-cost” and “spanning-tree legacy-mode”. See [“MSTP Default Path Cost Controls” on page 18](#) for details.
  - **QoS (PR\_1000304105)** — Maximum QoS rules limit is incorrect, internal to the switch.
  - **Setup (PR\_1000301498)** — Manual IP address cannot be set when using the "setup" menu.
-

- **SNMP (PR\_1000295753)** — Removing the 'public' SNMP community name generates an empty Event Log message.
- **SNMP (PR\_1000310841)** — User can assign illegal values for hpSwitchCosDSCPpolicyPriority through SNMP. All other user-interfaces for configuring QoS (CLI, Web UI, ProCurve Manager, and Radius) function correctly.
- **SNMP Link Up Traps and ARP Flush (PR\_1000293466)** — After issuing the CLI command: "snmp-server host <ip address> public all", generic Link Up traps are not generated. Also, the switch flushes its ARP cache whenever a port comes online, after issuing the command.
- **SNMP Traps (PR\_1000285195)** — When link-up/link-down traps are disabled for a port (using SNMP commands), after reboot the switch automatically re-enables those traps.
- **Web Authentication (PR\_1000302945)** — When a port is set to Web Authentication and the client fails authentication, it is assigned to the Unauthorized VLAN; however, it cannot communicate with other ports on the Unauthorized VLAN.
- **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 4200vl is stack commander and a 3500yl is a stack member.

## Release L.10.03

### Problems Resolved in Release L.10.03 (Not a general release)

- **Crash (PR\_1000282359)** — 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.
```
- **Help (PR\_1000317711)** — In the VLAN menu Help text, the word 'default' is mis-spelled.
- **Menu (PR\_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.
- **Routing (PR\_1000301005)** — Certain types of traffic cause the switch to route very slowly and drop packets.
- **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.



- **Web UI (PR\_1000308707)** — The QOS tab is missing from the Web User Interface when stacking is enabled.

## Release L.10.04

### **Problems Resolved in Release L.10.04** (Not a general release)

- **Counters (PR\_1000321097)** — Drop counters may display incorrect information.
- **Counters (PR\_1000321476)** — SNMP counter may display incorrect information.
- **Crash (PR\_1000322009)** — The Switch may crash with a message similar to:  

```
Software exception in ISR at queues.c:123.
```
- **Crash (PR\_1000323675)** — The Switch may crash with a message similar to:  

```
ASSERT: Software exception at aaa8021x_proto.c:501 -- in  
'm8021xCtrl'.
```
- **Crash (PR\_1000327132)** — The Switch may crash with a message similar to:  

```
Software exception in ISR at btmDmaApi.c:304.
```
- **DHCP Enhancement (PR\_1000311957)** — Added option to configure the switch to use the management VLAN IP address in the Option 82 field. See [“DHCP Option 82: Using the Management VLAN IP Address for the Remote ID”](#) on page 19 for details.
- **Enhancement (PR\_1000290489)** — Enhancement to display Port Name along with Port number on the Web User Interface Status and Configuration screens.
- **ICMP (PR\_1000235905)** — Switch does not send a 'destination unreachable' response message when trying to access an invalid UDP port.
- **sFlow (PR\_1000321195)** — A network management application may incorrectly report traffic spikes when sFlow is first re-enabled.
- **SNMPv3 (PR\_1000325021)** — Under some conditions, SNMPv3 lines are not written to the running-configuration file.

## Release L.10.05

### Problems Resolved in Release L.10.05 (Not a general release)

- **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.
```

- **Web UI (PR\_1000302713)** — When using the web user interface and a large amount of stacking interactions occur, portions of the information from the stack commander may no longer appear.

## Release L.10.06

### Problems Resolved in Release L.10.06 (Not a general release)

- **CLI (PR\_1000322029)** — The command "show vlans" does not display data correctly in the status field.
- **CLI (PR\_1000334412)** — Operator level can save Manager privilege level changes to the configuration.
- **sFlow Enhancement (PR\_1000337714)** — Added new "show sflow" commands to the CLI. See [“Show sFlow Commands” on page 21](#) for details.
- **Web UI (PR\_1000331431)** — The QoS Configuration Tab is not working correctly when using the Web User Interface.

## Release L.10.07

### Problems Resolved in Release L.10.07 (Not a general release)

- **Authentication (PR\_1000343377)** — When running the Windows XP 802.1X supplicant and the switch sends a re-authentication, Windows XP prompts the user to re-enter their username and password again.
- **Authentication (PR\_1000344961)** — A port with multiple 802.1X users on it will allow traffic to pass for a user after that user's supplicant has been stopped.
- **CLI (PR\_1000344362)** — The CLI help text was updated in the areas of ip igmp auto, forward, and blocked.

## Software Fixes in Release L.10.01 - L.10.24

### Release L.10.08

- **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.
- **Enhancement (PR\_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **Radius EAP (PR\_1000334731)** — PEAP/TLS EAP types fail to authenticate with Microsoft IAS Radius Server. The switch event log will report, "can't reach RADIUS server."

## Release L.10.08

### Problems Resolved in Release L.10.08 (Not a general release)

- **CLI (PR\_1000342461)** — When a trunk is configured on an uplink port, the command "show lldp info remote <port number>" reports incorrect information for the remote management address.
- **Enhancement (PR\_1000355089)** — This enhancement increases the maximum number of 802.1X users per port to 8.
- **Enhancement (PR\_1000355877)** — 802.1X Controlled Directions enhancement: with this change, administrators can use "Wake-on-LAN" with computers that are connected to ports configured for 802.1X authentication.
- **LLDP (PR\_1000310666)** — The command output from "show LLDP" does not display information learned from CDPv2 packets.
- **LLDP (PR\_1000301069)** — When the LLDP admin status of a port changes from TX to DIS/RX, the switch does not always send out shutdown frames.
- **LLDP (PR\_1000312285)** — The old value of the SNMP LLDP-MED trap (lldpXMedRem-DeviceClass) is supported.
- **LLDP (PR\_1000305141)** — The LLDP MED Location TLV format is not MED Draft 6 compatible.

## Release L.10.09

### Problems Resolved in Release L.10.09

- **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.
- **Enhancement (PR\_1000360934)** — Added DHCP Protection enhancement for switch 4200vl.

## Release L.10.10

### Problems Resolved in Release L.10.10 (not a general release)

- **802.1x (PR\_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports. This fix removes a limitation that requires these steps be done in a specific order.
- **CLI (PR\_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.
- **Enhancement (PR\_1000351445)** — The "show tech transceiver" CLI command output now contains the HP part number and revision information for all transceivers on the switch..
- **Source Port Filtering (PR\_1000352851)** — Source Port Filtering on trunks does not work when both the source and destination are trunk ports, even though the switch accepts the configuration.
- **Trunking (PR\_1000364354)** — When a switch with 30 or more trunks is rebooted, the switch may crash with a message similar to:

```
NMI event SW:IP=0x00456520 MSR:0x0000b032 LR:0x004564d0
Task='mLpMgrCtrl' Task ID=0x150d940 cr: 0x48000042 sp:0x0150d468
xer:0x00000000
```

## Release L.10.11

### Problems Resolved in Release L.10.11 (not a general release)

- **Crash (PR\_1000368540)** — Switch may crash with a message similar to:  
Software exception at parser.c:8012 -- in 'mSess2', task ID =  
0x90e10e0 -> ASSERT: failed.
- **Hang (PR\_1000346328)** — RMON alarms/events configuration files may become corrupt and prevent initialization, resulting in failure to boot.
- **RADIUS (PR\_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.

- **Web-UI (PR\_1000373711)** — Attempting to access the WebUI of a stack member without being logged on as Manager returns a "404 Page Not Found" error.

**NOTE:** Versions L.10.12 through L.10.19 were never built. The code branched to L.10.20 with no intervening releases.

## Release L.10.20

### **Problems Resolved in Release L.10.20** (not a general release)

Please refer to [“Release L.10.20 Enhancements”](#) section beginning on page 45 for additional details on the enhancements listed below.

- **Enhancement (PR\_1000336169)** — Added support for STP Per Port BPDU Filtering and SNMP Traps.
- **Enhancement (PR\_1000346164)** — When this feature is enabled on a port, the switch will disable (drop link) a port that receives a spanning tree BPDU, log a message, and optionally send an SNMP TRAP.
- **Enhancement (PR\_1000313819)** — This enhancement allows SNMP configuration of RADIUS configuration.
- **Enhancement (PR\_1000292455)** — Implemented rate display for ports on CLI. New command: "show interface port-utilization". Not available on Menu or Web Interface.
- **Enhancement (PR\_1000311510)** — Ping conformance as defined in RFC 2925
- **Enhancement (PR\_1000331027)** — TCP/UDP port closure enhancement.
- **Enhancement (PR\_1000330743)** — Denial of Service logging enhancement.
- **Enhancement (PR\_1000338847)** — Added support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3.
- **Enhancement (PR\_1000339546)** — Addition of the "clear log" CLI command
- **Enhancement (PR\_1000374085)** — This enhancement expands the use of the Controlled Directions parameter to also support mac/web authentication
- **Enhancement (PR\_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Enhancement (PR\_1000358900)** — A RADIUS accounting enhancement was made.
- **Module Hotswap (PR\_1000376980)** — When a module is hotswapped, the switch may crash with a message similar to:

```
Software exception at buffers.c:2237 -- in 'mPpmgrCtrl',  
task ID = 0x33eea88 -> ASSERT: failed
```

## Release L.10.23

*Versions L.10.21 and L.10.22 were never released.*

### Problems Resolved in Release L.10.23 (not a general release)

- **Enhancement** — Support for the following products was added: J8768A, J9030A, J9033A, and J9064A

## Release L.10.24

### Problems Resolved in Release L.10.24

- **CLI (PR\_1000332352)** - The output of a "show int brief" command should show the negotiated flow control status rather than the flow control configuration setting.
- **CLI (PR\_1000390970)** - The command "tftp-enable" is removed from the CLI since that functionality is served by "tftp server/client"
- **CLI/config (PR\_1000391119)** - Copying a configuration file to a switch with a BPDU protection timeout value set may produce an error similar to:  

```
CCCCline: 10007. 1200: Error setting configuration.
```
- **CLI/Show tech (PR\_1000378957)** - After a hotswap of chassis modules, the "show tech statistics" value for the field "linked port on box" may be inaccurate.
- **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 authentication key (maximum 16 characters)".
- **CLI (PR\_1000373443)** - The CLI "update" command help text and confirmation message is misleading and confusing.
- **Crash (PR\_1000392863)** - Switch may crash when "setmib tcpConnState" is used, with a message similar to:  

```
NMI event SW:IP=0x0079f4a0 MSR:0x00029210 LR:0x006dca60  
Task='eTelnetd' Task ID=0x8a7cbb0 cr: 0x20000042 sp:0x08a7c871
```
- **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\_1000373226)** - Support was added for a future SFP transceiver.
- **Enhancement (PR\_1000335860)** - This enhancement provides a configuration option for the source IP address field of SNMP response and generated trap PDUs.

**Software Fixes in Release L.10.01 - L.10.24**  
Release L.10.24

- **Enhancement (PR\_1000379804)** - Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Enhancement (PR\_1000385565)** - Port security static mac address limit increased to 32.
- **LED (PR\_1000378980)** - The full-duplex (FDx) mode LED incorrectly illuminates when ports on J8765B module negotiate to half-duplex.
- **MDIX (PR\_1000378954)** - Inaccurate detection of MDIX/MDI mode on J8768A and J9033A modules.
- **Syslog (PR\_1000379802)** - Forwarding of event log message to a configured syslog server is not disabled when a specific event log message has been disabled via MIB.
- **Trunking (PR\_1000238829)** - Trunks numbered trk10 and greater cause the output from the CLI command "show span" output to be misaligned.
- **Web UI (PR\_1000326265)** - Attempting to access the Web UI of a stack member hangs the browser.



© 2006 - 2007 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

March 2007  
Manual Part Number  
5991-4696