Release Notes:
Version L.10.09 Software
for the ProCurve Series 4200vl Switches

Release L.10.09 supports these switches:

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

These release notes include information on the following:

Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at **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.

Publication Number

5991-4696
September 2006 -B

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

Contents

Software Management

Software Updates

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

Downloading Switch Documentation and Software from the Web

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

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

   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**.
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**). 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:

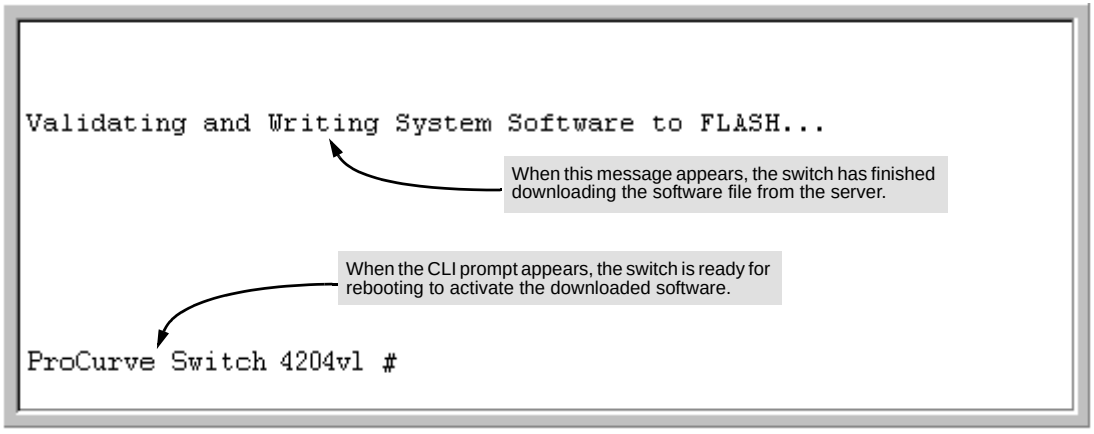

Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

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] ?
```

ProCurve Switch, Routing Switch, and Router Software Keys

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

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

OS/Web/Java Compatibility Table

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

Operating System	Internet Explorer	Java
Windows NT 4.0 SP6a	5.00, 5.01 5.01, SP1 6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.3.1.12 – Version 1.4.2.05
Windows 2000 Pro SP4	5.05, SP2 6.0, SP1	
Windows XP Pro SP2	6.0, SP1	Sun Java 2 Runtime Environment: – Version 1.5.0.02
Windows Server SE 2003 SP1	6.0, SP1	

Clarifications and Updates

There are currently no clarification or updates to existing documentation related to the Series 4200vl Switches, or L10.0x code.

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.10.03 Enhancements" on page 9.

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
```

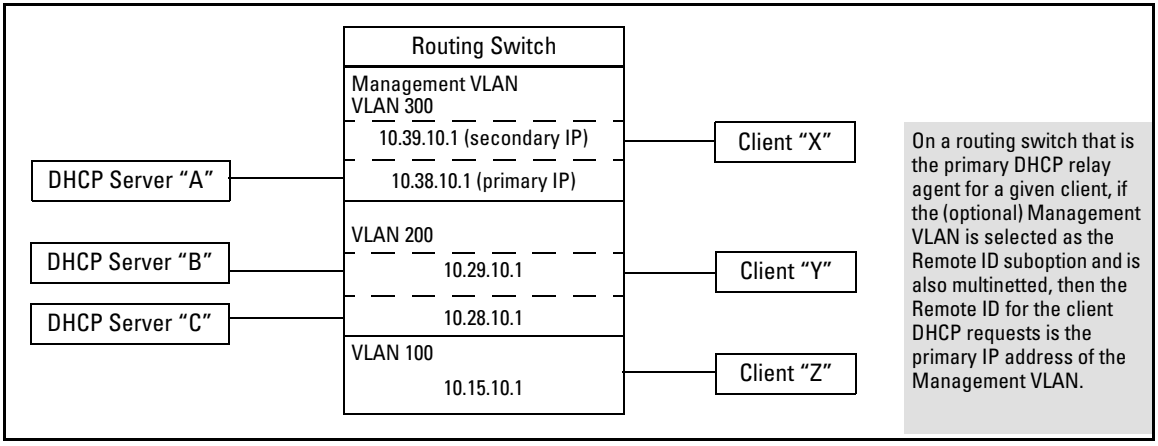

Figure 2. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption

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;M.10.03
  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 mangement 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 enhancement:

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.

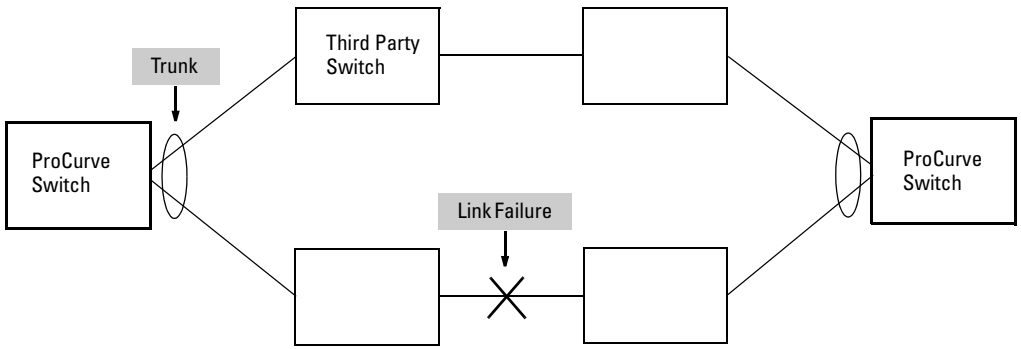

Figure 6. UDLD Example

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 continue 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: 2600, 2800, 3400, 3500, 4200, 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 al link-keepalive
```

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

```
ProCurve(config)#interface al-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 l 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 20 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:

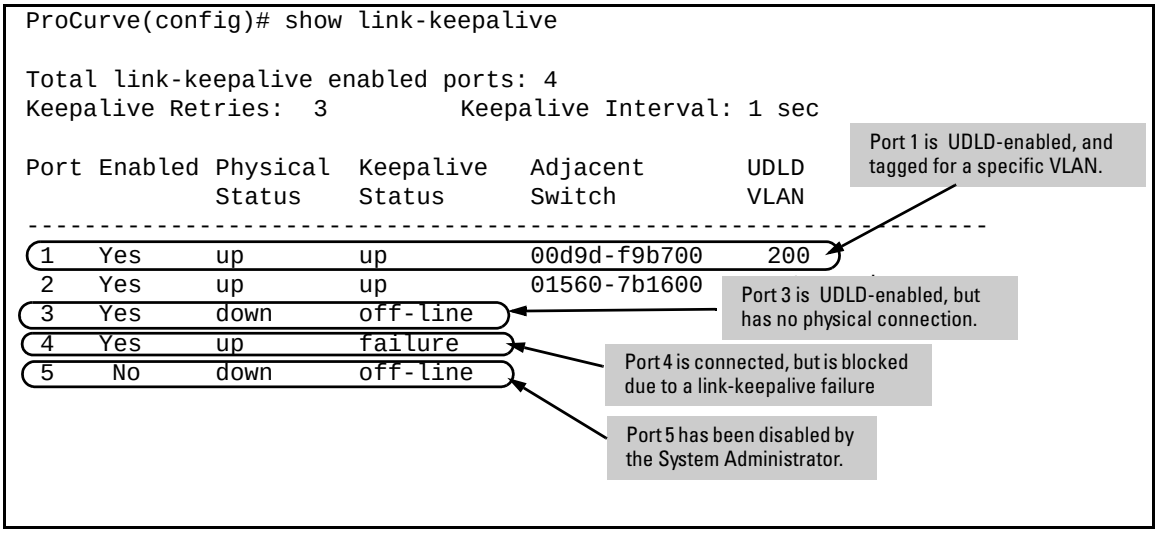

Figure 7. Example of UDLD Information displayed using Show Link-Keepalive Command

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

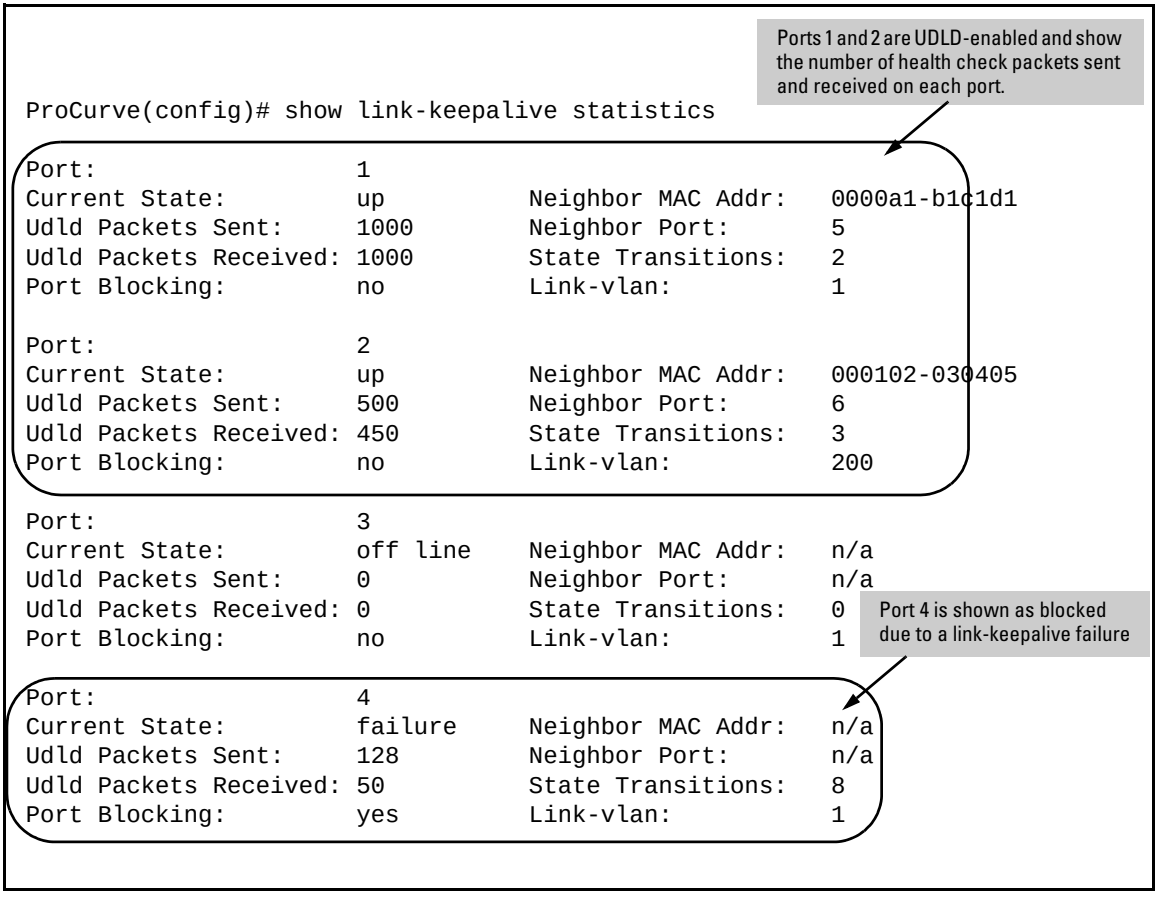

Figure 8. Example of Detailed UDLD Information displayed using Show Link-Keepalive Statistics Command

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.

Release L.10.09 Enhancements

- Added DHCP Protection enhancement for switch 4200vl.

Software Fixes in Release L.10.01 - L.10.0*x*

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.10.03" on page 23.

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='tHttpd' 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 8 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 9 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 11 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.
- **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. See "Uni-Directional Link Detection (UDLD)" on page 14 for details.

- **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 (lldpXMedRemDeviceClass) 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.

September 2006 -B
Manual Part Number
5991-4696