Release Notes:
Version E.10.67 Software
for the ProCurve Series 5300xl Switches

Release E.10.61 supports these switches:

- ProCurve Switch 5304xl (J4850A)
- ProCurve Switch 5308xl (J4819A)
- ProCurve Switch 5348xl (J4849A) – 48-port (10/100) bundle in Switch 5304xl chassis
- ProCurve Switch 5372xl (J4848A) – 72-port (10/100) bundle in Switch 5308xl chassis
- ProCurve Switch 5304xl-32G (J8166A) – 32-port (10/100/1000) bundle in 5304xl chassis
- ProCurve Switch 5308xl-48G (J8167A) – 48-port (10/100/1000) bundle in 5308xl chassis

These release notes include information on the following:

FEC, CDP Removal

Starting with Software version E.10.09, FEC trunks (Cisco Systems' FastEtherChannel for aggregated links) are no longer supported, and generation of CDP (Cisco Discovery Protocol) packets are no longer supported. In their place are IEEE standards based LACP aggregated links (as well as statically configured trunks) and generation of LLDP packets for device discovery. For more information, please see: **ftp://ftp.hp.com/pub/networking/software/LLDP-and-LACP-statement.pdf**.

Boot ROM Update Required

If your 5300xl is currently running software version E.07.37 or earlier, you must update the Boot ROM by loading and booting software version E.07.40 before installing switch software revisions later than E.07.40.

Caution

The startup-config file saved under version E.10.*xx* or greater is backward-compatible with version E.08.*xx*, but is NOT backward-compatible with E.07.*xx* or earlier software versions. Users are advised to save a copy of any pre-E.08.*xx* startup-config file BEFORE UPGRADING to E.08.*xx* or greater, in case there is ever a need to revert to pre-E.08.*xx* software. For instructions on copying the startup-config file, see Appendix A in the *Management and Configuration Guide*, available on the ProCurve Networking Web site: http:\\www.procurve.com. Click on Technical Support, then Product Manuals.

Publication Number

Part Number 5991-2127
August 2007

Applicable Product

ProCurve Switch 5304xl	(J4850A)
ProCurve Switch 5308xl	(J4819A)
ProCurve Switch 5348xl	(J4849A)
ProCurve Switch 5372xl	(J4848A)
ProCurve Switch 5304xl-32G	(J8166A)
ProCurve Switch 5308xl-48G	(J8167A)

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

Clarifications

Enhancements

Software Fixes in Release E.06.01 through E.10.67

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 HP's ProCurve web site as described below.

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

   http://www.procurve.com.

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

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

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

Downloading Software to the Switch

Caution

The startup-config file generated by the latest software release may not be backward-compatible with the same file generated by earlier software releases. Refer to "Boot ROM Update Required" on the front page.

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

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

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 E_10_2x.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 E_10_2x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

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

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

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

3. Reboot the switch.

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation 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 Microsoft Windows NT® terminal emulator, you would use the **Send File** option in the **Transfer** drop-down menu.)

Syntax: **copy xmodem flash < unix | pc >**

For example, to download a software file from a PC:

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 57600 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 57600, execute this command:

   ```
   ProCurve(config)# console baud-rate 57600
   ```

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

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

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

5. Use the following command to confirm that the software downloaded correctly:

   ```
   ProCurve> show system
   ```

   Check the **Firmware revision** line to verify that the switch cownloaded the new software.

6. 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.) Remeber to return your terminal emulator to the same baud rate as the switch.

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 "Do you want to save current configuration [y/n] ?" prompt.

Software Index for ProCurve Networking Products

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)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
T	Switch 2900 Series (2900-24G, and 2900-48G)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Minimum Software Versions for Series 5300xl Switch Features

For Switch 5300xl Hardware Accessories.

ProCurve Device	Minimum Supported Software Version
J4820A 24-Port 10/100-TX Module	E.05.04
J4821A 4-Port 100/1000-T Module	E.05.04
J4839A Redundant Power Supply (RPS)	E.05.04
J4852A 12-Port 100-FX MTRJ Module	E.06.10
J4878A 4-Port Mini-GBIC Module	E.05.04
J4858A Gigabit-SX-LC Mini-GBIC	E.05.04
J4859A Gigabit-LX-LC Mini-GBIC	E.05.04
J4860A Gigabit-LH-LC Mini-GBIC	E.06.01
J8161A 24-Port 10/100-TX PoE Module	E.08.22
J4907A 16-Port 10/100/1000-T Module	E.08.42
J8162A Access Controller xl Module	E.09.21
J8177B 1000Base-T Mini-GBIC	E.09.22
J9001A Wireless Edge Services xl Module	E.10.30
J9003A Redundant Wireless Services xl Module	E.10.30

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

LLDP and LACP

Starting with Software version E.10.10, FEC trunks (Cisco Systems' FastEtherChannel for aggregated links) are no longer supported, and generation of CDP (Cisco Discovery Protocol) packets are no longer supported. In their place are IEEE standards-based LACP aggregated links (as well as statically configured trunks) and generation of LLDP packets for device discovery.

For more information, please see: **ftp://ftp.hp.com/pub/networking/software/LLDP-and-LACP-statement.pdf**.

Non-Genuine Mini-GBIC Detection and Protection Initiative

Non-genuine ProCurve Transceivers and Mini-GBICs have been offered for sale in the marketplace. To protect customer networks from these unsupported products, starting with release E.09.22, ProCurve switch software includes the capability to detect and disable non-genuine transceivers and mini-GBICs discovered in Series 5300xl Switch ports. When a non-genuine device is discovered, the switch disables the port and generates an error message in the Event Log.

Mesh Design Optimization

Mesh performance can be enhanced by using mesh designs that are as small and compact as possible while still meeting the network design requirements. The following are limits on the design of meshes and have not changed:

1. Any switch in the mesh can have up to 24 meshed ports.
2. A mesh domain can contain up to 12 switches.
3. Up to 5 inter-switch meshed hops are allowed in the path connecting two nodes.
4. A fully interconnected mesh domain can contain up to 5 switches.

Mesh performance can be optimized by keeping the number of switches and the number of possible paths between any two nodes as small as possible. As mesh complexity grows, the overhead associated with dynamically calculating and updating the cost of all of the possible paths between nodes grows exponentially. Cost discovery packets are sent out by each switch in the mesh every 30 seconds and are flooded to all mesh ports. Return packets include a cost metric based on inbound and outbound queue depth, port speed, number of dropped packets, etc. Also, as mesh complexity grows, the number of hops over which a downed link has to be reported may increase, thereby increasing the reconvergence time.

The simplest design is the two-tier design because the number of possible paths between any two nodes is kept low and any bad link would have to be communicated only to it's neighbor switch.

As shown here, meshing allows multiple redundant links between switches in the domain, and more than one link is allowed between any two switches in the domain.

Note also that a switch can have up to 24 ports configured for meshing.

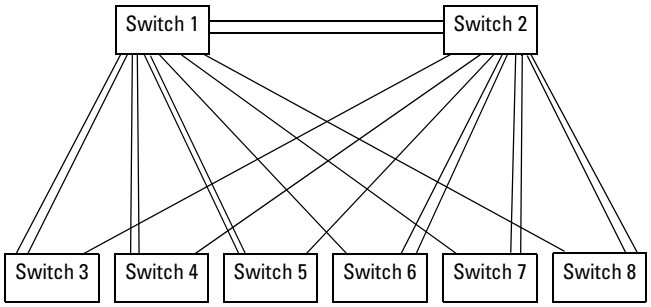

Figure 1. Example of a Two-Tier Mesh Design

Other factors affecting the performance of mesh networks include the number of destination addresses that have to be maintained, and the overall traffic levels and patterns. However a conservative approach when designing new mesh implementations is to use the two-tier design and limit the mesh domain to eight switches where possible.

For more information, refer to the chapter titled “Switch Meshing” in the Advanced Traffic Management Guide for your switch.

General Switch Traffic Security Guideline

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

1. Disabled/Enabled physical port
2. MAC lockout (Applies to all ports on the switch.)
3. MAC lockdown
4. Port security
5. Authorized IP Managers
6. Application features at higher levels in the OSI model, such as SSH.

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

The Management VLAN IP Address

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

Heavy Memory Usage with PIM-DM

Heavy use of PIM (Many S/G--source-group--flows over many VLANs) combined with other memory-intensive features, can oversubscribe memory resources and impact overall performance. If available memory is exceeded, the switch drops any new multicast flows, and generates appropriate log messages. Corrective actions can include reducing the number of VLANs on the 5300xl device by moving some VLANs to another device, free up system resources by disabling another, non-PIM feature, and/or moving some hosts to another device. For more information, refer to "Operating Notes" and "Messages Related to PIM Operation" in the chapter titled "PIM DM (Dense Mode)" in the *Advanced Traffic Management Guide* (February, 2004 or later) for the ProCurve Series 5300xl switches. For more information on PIM-DM operation, refer to the chapter titled "PIM-DM (Dense Mode)" in the *Advanced Traffic Management Guide* for the ProCurve Series 5300xl switches. (To download switch documentation for software release E.09.*xx*, refer to "Software Updates" on page 1.)

Change in QoS Priority and Policy Limit

Beginning with software release E.09.22, the switch allows configuration of up to 250 priority and/or DSCP policy configurations. Attempting to add more than 250 entries generates an error message in the CLI.

Heavy use of QoS, combined with other memory-intensive features, can oversubscribe memory resources and impact overall performance. Updating the switch software from an earlier release in which more than 250 entries were configured causes the switch to drop any entries in excess of the first 250 and to generate an event log message indicating this action. For more information, refer to "QoS Operating Notes" in the chapter titled "Quality of Service (QoS): Managing Bandwidth More Effectively" in the *Advanced Traffic Management Guide* for the ProCurve Series 5300xl switches (part number 5990-6051, January 2005 or later). Note that the above limit supercedes the limit indicated in the January 2005 edition of the *Advanced Traffic Management Guide*. To download switch documentation for software release E.09.22, refer to "Software Updates" on page 1.

Interoperating with 802.1s Multiple Spanning-Tree

The ProCurve implementation of Multiple Spanning-Tree (MSTP) in software release E.08.*xx* and greater complies with the IEEE 802.1s standard and interoperates with other devices running compliant versions of 802.1s. Note that the ProCurve Series 9300 routing switches do not offer 802.1s-compliant MSTP. Thus, to support a connection between a 9300 routing switch and a 5300xl switch running MSTP, configure the 9300 with either 802.1D (STP) or 802.1w (RSTP). For more information

on this topic, refer to the chapter titled "Spanning-Tree Operation" in the *Advanced Traffic Management Guide* (part number 5990-6051, January 2005 or later). (To download switch documentation for software release E.09.22, refer to "Software Updates" on page 1.)

Rate-Limiting

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

As a performance consideration, implementing rate-limiting in heavy traffic situations involving QoS, can affect overall performance. For more information on rate-limiting operation, refer to "Operating Notes for Rate-Limiting" in the chapter titled "Optimizing Traffic Flow with Port Controls, Port Trunking, and Filters" of the Management and Configuration Guide (part number 5990-6050, January 2005 or later) for the ProCurve Series 5300xl switches. (To download switch documentation for software release E.09.22, refer to "Software Updates" on page 1.)

Time Zone Offset

Starting with release E.05.*xx*, the method of configuring the Time Zone for TimeP or SNTP configuration has been updated. Previous switch software for all ProCurve switches used positive time offset values for time zones that are West of GMT and negative values for time zones that are East of GMT. The standards indicate that time zones West of GMT should be designated by negative offset values, and time zones East of GMT by positive values. Software version E.05.*xx* updates this configuration method, but if you use the same values for indicating time zones as you did for previous ProCurve switches, the time will be set incorrectly on your Series 5300GL switch. For example, for previous ProCurve switches, the US Pacific time zone was configured by entering **+480**. With software version E.05.*xx*, the US Pacific time zone must now be configured by entering **-480**.

Enhancements

Unless otherwise noted, each new release includes the features added in all previous releases. Enhancments are listed in chronological order, oldest to newest software release. To review the list of enhancements included since the last general release that was published, begin with "Release E.10.56 Enhancements" on page 53.

Descriptions and instructions for enhancements included in Release E.10.02 or earlier are included in the latest release of manuals for the ProCurve 5300xl switches (Oct. 2005), available on the web at **http://www.hp.com/rnd/support/manuals/5300xl.htm**

Release E.10.03 through E.10.23 Enhancements

Software fixes only; no new enhancements. Versions E.10.11 to E.10.19 were never built.

Release E.10.24 Enhancements

CLI Port Rate Display

Beginning with release E.10.24 the CLI "show interface [port list]" command includes the port rate in the display. The rate displayed is the average for a period of 5 minutes, given in bps for 1G ports, or in Kbps for 10G ports. You can also use the CLI command: show interface port-utilization to display port-rate over a period of 5 minutes.

Release E.10.25 and E.10.26 Enhancements

Software fixes only; no new enhancements.

Release E.10.27 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 the 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 E.10.28 through E.10.29 Enhancements

Software fixes only; no new enhancements.

Release E.10.30 Enhancements

Release E.10.31 includes the following enhancement:

- Added support for J9001A and J9003A wireless xl modules.

Release E.10.31 Enhancements

Release E.10.31 includes the following enhancement:

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

Release E.10.32 Enhancements

Release E.10.32 includes the following enhancements:

- Added DHCP Option 82 functionality for 5300xl series.
- Support for Fast Boot CLI & SNMP implementation

Using Fastboot To Reduce Boot Time

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

Syntax: [no] fastboot

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

Syntax: show fastboot

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

For example:

```
ProCurve(config)# show fastboot

    Fast Boot:  Disabled
```

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

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

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

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

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

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

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

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

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

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

(Default: **mac***)*

Example

In the routing switch in figure 1, option 82 has been configured with **mgmt-vlan** for the Remote ID.

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

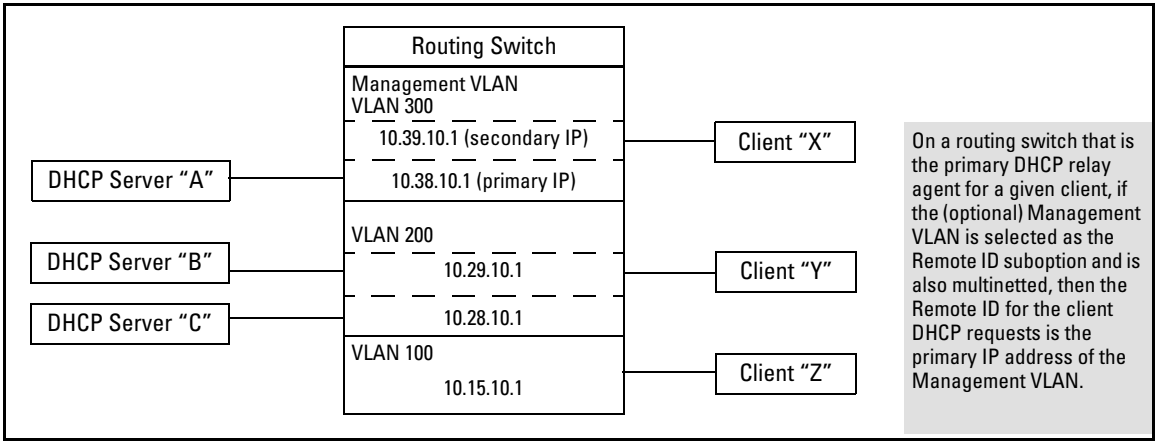

Figure 2. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption

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 E.10.33 Enhancements

Release E.10.33 includes the following enhancements:

- **Enhancement (PR_1000330704)** — Added RADIUS Command Authorization and Accounting for the Command Line Interface (CLI).

Release E.10.34 through E.10.35 Enhancements

Software fixes only, no new enhancements.

Release E.10.36 Enhancements

Release E.10.36 includes the following enhancements:

SFlow Show 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 E.10.36, the 5300xl 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;E.10.36
  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 E.10.37 Enhancements

Release E.10.37 includes the following enhancement:

Spanning Tree Show Commands

The **show spanning-tree detail** command previously displayed 802.1D (STP) and 802.1w (RSTP) status and counters for all ports on the switch. Beginning with software release E.10.37, this command provides 802.1s (MSTP) multi-instance spanning tree details and displays additional parameters to enhance spanning-tree reporting via the CLI.

The following shows RSTP sample output from the enhanced command.

```
ProCurve# show spanning-tree detail

 Status and Counters - RSTP Port(s) Detailed Information

  Port                      : 1
  Status                    : Up
  Role                      : Root
  State                     : Forwarding
  Priority                  : 128
  Path Cost                 : 200000
  Root Path Cost            : 10
  Root Bridge ID            : 1:0001e7-215e00
  Designated Bridge ID      : 32768:0001e7-3d0080
  Designated Port ID        : 128:75
  AdminEdgePort             : Yes
  OperEdgePort              : No
  AdminPointToPointMAC      : Force-True
  OperPointToPointMAC       : Yes
  Aged BPDUs Count          : 0
  Loop-back BPDUs Count     : 0
  TC Detected               : 1
  TC Flag Transmitted        : 0          TC ACK Flag Transmitted  : 0
  TC Flag Received           : 0         TC ACK Flag Received     : 47

  RSTP        RSTP        CFG         CFG         TCN         TCN
  BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx    BPDUs Tx    BPDUs Rx
  ----------- ----------- ----------- ----------- ----------- -----------
  3           0           0           256654      47          0
```

Figure 6. Example of Show Spanning-Tree Detail

Operating Notes

- TC refers to a Topology Change detected on the given port. Note the following details:
  - **TC Detected** counter shows when a port identifies a topology change (increments when the particular non-Edge port goes into forwarding). For RSTP and MSTP, this would be due to the switch's link going to forwarding.
  - **TC Flag Transmitted** counter shows the number of TC notifications sent out of the port. This refers to propagating a topology change that occurred on another port (that is, a TC Detected increment) or to propagating a topology change received on another port (that is, TC Flag Received).
  - **TC Flag Received** counter shows the number of TC notifications (RSTP or MSTP style BPDU with the TC flag set) received on the port.
  - **TC ACK Flag Transmitted** is an 802.1D mode counter. It will only increment when the port is operating in 802.1D mode and an 802.1D style PDU is sent out of the port.
  - **TC ACK Flag Received** is an 802.1D mode counter. It will only increment when the port is operating in 802.1D mode and an 802.1D style PDU is received on the port.
- With STP and RSTP activated:
  - The **show spanning tree detail** command shows all active RSTP port by port.
  - The **show spanning-tree** <port-list> **detail** command shows the specified port-list RSTP port by port detail.
- With MSTP activated:
  - The **show spanning tree detail** command shows all active MSTP port by port. This command only gives information concerning the common spanning tree (CST) ports. To view counters pertaining to a specific spanning-tree instance, you must use the **show spanning-tree instance** <inst> **detail** command. The **show spanning-tree** <port-list> **detail** command shows the specified port-list MSTP port by port detail.
  - The **show spanning-tree instance** <inst> **detail** command shows all ports active for a specific instance of MSTP.
  - The **show spanning-tree** <port-list> **instance** <inst> detail shows the specified port-list for the specified instance of MSTP.
  - **TC ACK Flag Transmitted** and **TC ACK Flag Received** are part of the CST counters displayed by the **show spanning tree detail** command. **TC Detected**, **TC Flag Transmitted**, and **TC Flag Received** are included only with the **instance** parameter due to the nature of MSTP.

Release E.10.38 Enhancements

Release E.10.38 includes the following enhancement:

- Support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3.

Release E.10.39 Enhancements

Release E.10.39 contains software fixes only, no new enhancments.

Release E.10.40 Enhancements

Release E.10.40 includes the following enhancement:

- If SCP or SFTP is enabled, TFTP is automatically disabled. TFTP cannot be enabled if either SCP or SFTP are enabled.

Release E.10.41 Enhancements

Release E.10.41 contains software fixes only, no new enhancments.

Release E.10.42 Enhancements

Release E.10.42 includes the following enhancements:

- Support for Unidirectional Fiber Break Detection. See "Uni-Directional Link Detection (UDLD)" on page 23 for details.
- 802.1X Controlled Directions enhancement for the 5300xl switches. With this enhancement, administrators can use "Wake-on-LAN" with computers that are connected to ports configured for 802.1X authentication. See "Configuring 802.1X Controlled Directions" on page 30.

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 7 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.

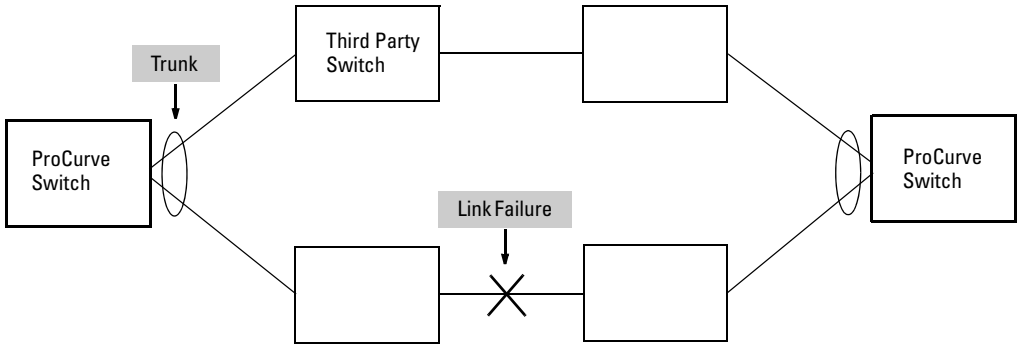

Figure 7. UDLD Example

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 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 29 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:

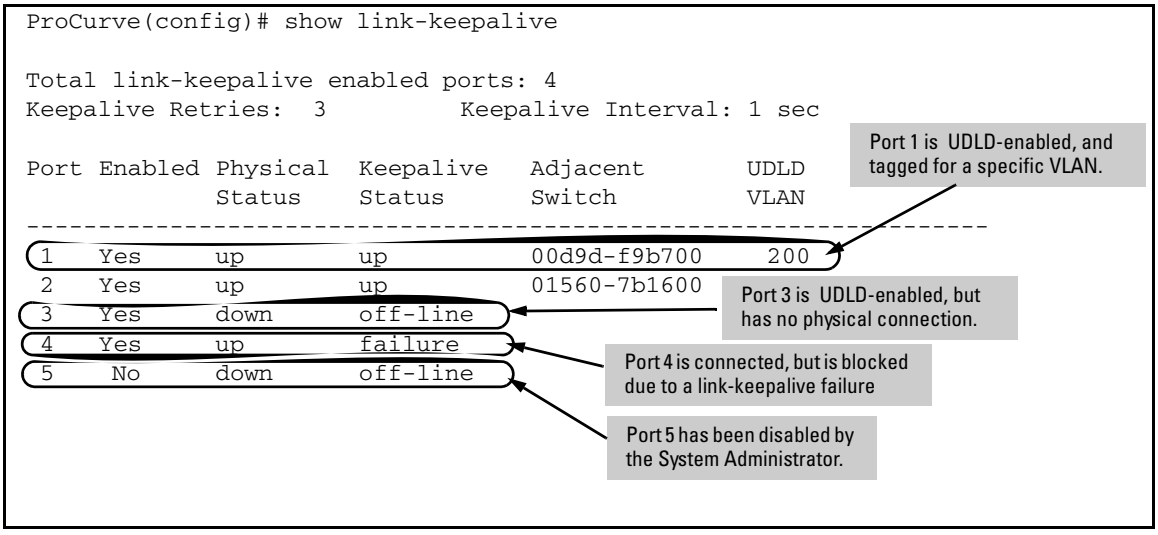

Figure 8. Example of UDLD Information displayed using Show Link-Keepalive Command

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

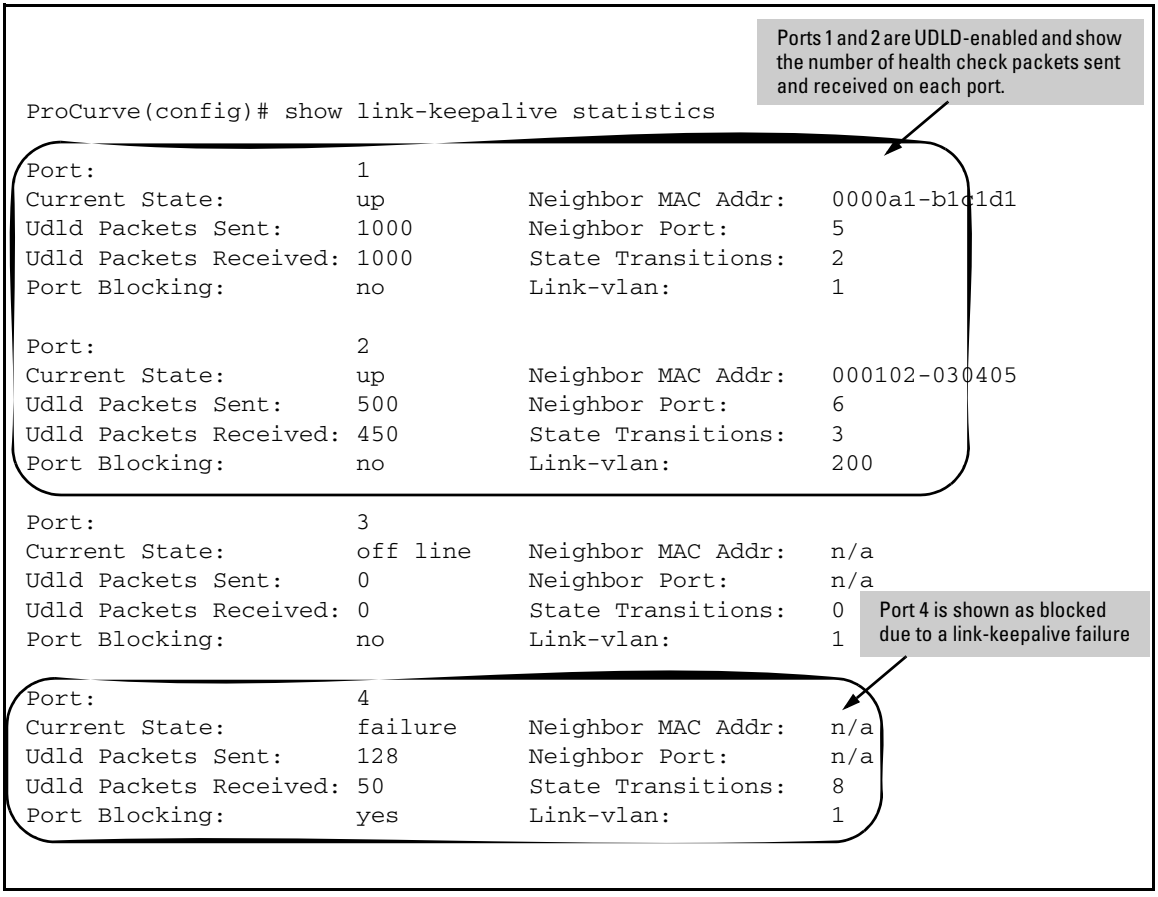

Figure 9. Example of Detailed UDLD Information displayed using Show Link-Keepalive Statistics Command

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 9 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.

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 10. Example of Configuring 802.1X Controlled Directions

Release E.10.43 Enhancements

Release E.10.43 includes the following enhancement:

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

Release E.10.44 Enhancements

Release E.10.44 includes the following enhancement:

- DHCP Protection enhancement for switch 5300xl. See DHCP Snooping below.

Release E.10.45 included software fixes only, no new enhancements.

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 in the folloiwng figure.

```
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 11. 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 12. 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 13. Example of DCHP 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 14. 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 15. 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 16. 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 17. 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>]

file	*Must be in Uniform Resource Locator (URL) format — "tftp://ip-address/ascii-string". The maximum filename length is 63 characters.*
delay	*Number of seconds to wait before writing to the database. Default = 300 seconds.*
timeout	*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.*

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 18. 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 that 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>.

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 E.10.46 Enhancements

Release E.10.46 includes the following enhancements:

- **Enhancement (PR_1000346164)** — RSTP/MSTP BPDU Protection enhancement. When this feature is enabled on a port and that port receives a spanning tree BPDU, the switch will disable (drop link) the port, log a message, and optionally, send an SNMP TRAP.
- **Enhancement (PR_1000365862)** — Addition to the RSTP/MSTP BPDU Protection enhancement. This portion of the enhancement added the option of configuring ports that had been previously disabled by BPDU Protection to be automatically re-enabled.

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 19.

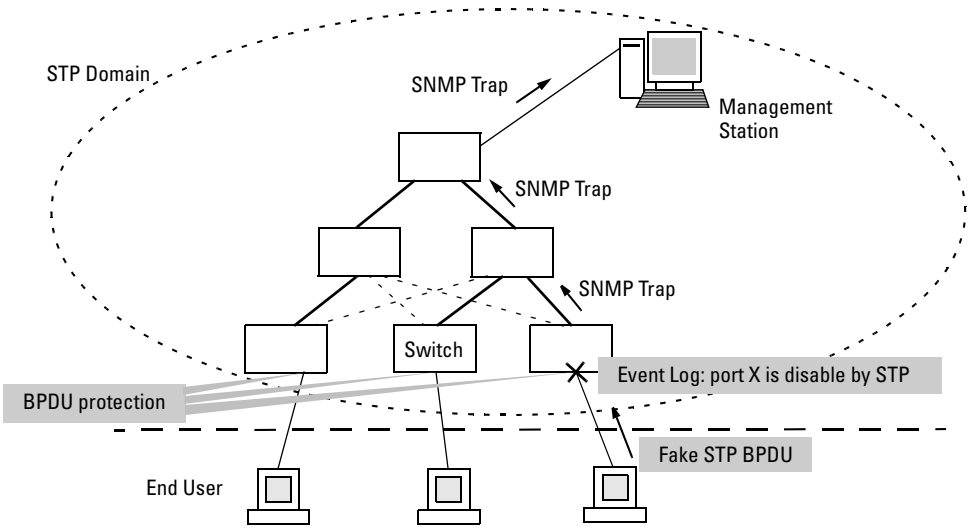

Figure 19. Example of BPDU Protection Enabled at the Network Edge

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 STP 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 trap 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

                  |            Prio                  | Designated    Hello
  Port Type       | Cost       rity  State           | Bridge        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
```

Ports with BPDU protection enabled

Errant BPDU detected on this port

Example of BPDU Protection Additions to Show Spanning Tree Command

Release E.10.47 Enhancements

Release E.10.47 included software fixes only, no new enhancements.

Release E.10.48 Enhancements

Release E.10.48 includes the following enhancements:

Enhancement (PR_1000376406) — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration. See “Configuring Loop Protection” on page 47.

Enhancement (PR_1000379804) — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

Configuring Loop Protection

You can use BPDU protection for systems that have spanning tree enabled (See "Spanning Tree BPDU Protection" on page 43), 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


      Loop         Loop      Loop       Time              Rx            Port
  Port Protection  Detected  Count      Since Last Loop   Action        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 20. Example of Show Loop Protect Display

Release E.10.49 Enhancements

Release E.10.49 includes the following enhancement:

- **Enhancement (PR_1000336169)** — Added support for STP Per Port BPDU Filtering and related SNMP Traps. See Spanning Tree Per-Port BPDU Filtering on the following page.

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 43 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.

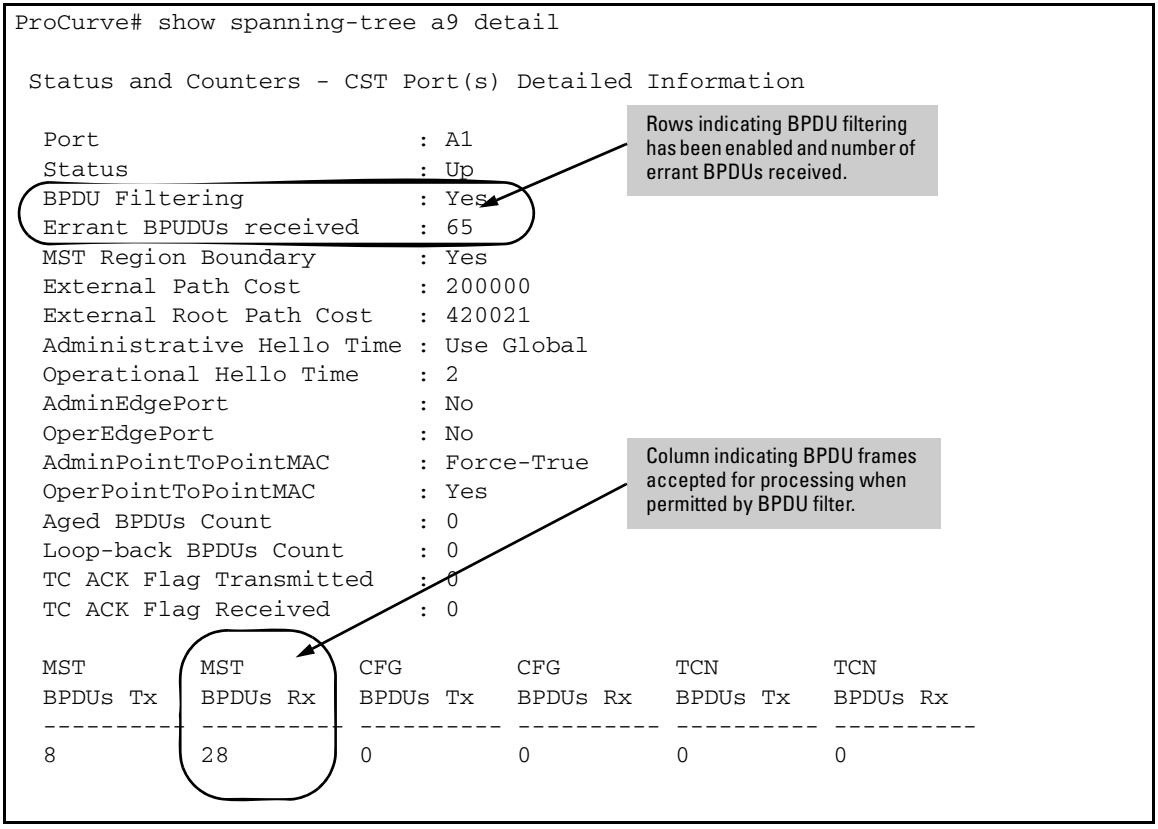

Figure 21. Example of BPDU Filter Fields in Show Spanning Tree Detail Command

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

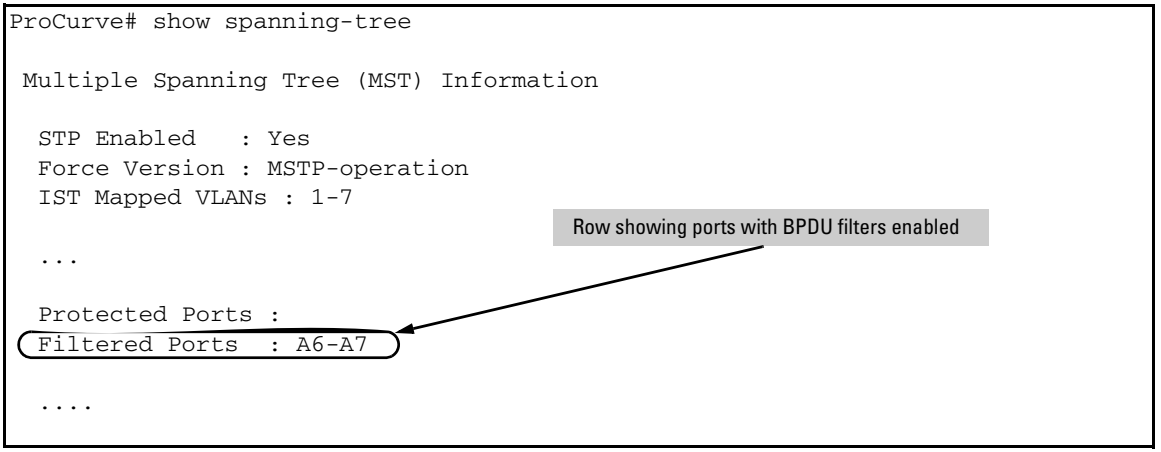

Figure 22. Example of BPDU Filtered Ports Field in Show Spanning Tree Command

Viewing Configuration of BPDU Filtering

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

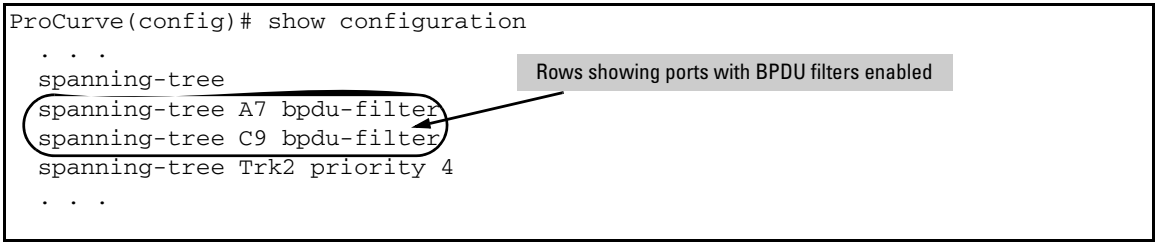

Figure 23. Example of BPDU Filters in the Show Configuration Command

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

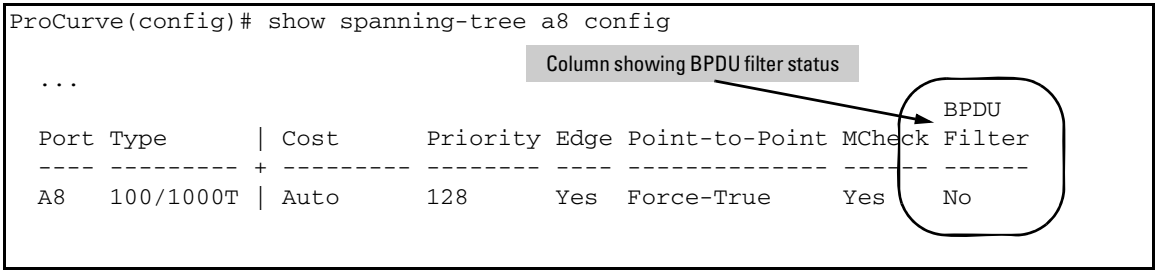

Figure 24. Example of BPDU Filter Status in Show Spanning Tree Configuration Command

Release E.10.50 Enhancements

Release E.10.50 includes the following enhancement:

- **Enhancement (PR_1000335860)** — This enhancement provides a configuration option for the source IP address field of SNMP response and SNMP trap PDUs.

Release E.10.51 Enhancements

Release E.10.51 includes the following enhancement:

- **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 5300 switch is 1664.

Release E.10.52 Enhancements

Release E.10.52 includes the following enhancement:

- **Enhancement (PR_1000374085)** — This enhancement expands the use of the Controlled Directions parameter to also support MAC and Web authentication. See “Configuring 802.1X Controlled Directions” on page 30 for additional information on using Controlled Directions.

Release E.10.53 Enhancements

Release E.10.53 includes the following enhancement:

- **Enhancement (PR_1000376626)** — Enhanced CLI "qos dscp-map he" help and "show dscp-map" text to warn user that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.

Release E.10.54 and E.10.55 Enhancements

Release E.10.54 was never released, and had no new enhancements.

Release E.10.55 had no new enhancements, software fixes only.

Release E.10.56 Enhancements

Release E.10.56 contains software fixes only, no new enhancments.

Release E.10.57 Enhancements

Release E.10.57 contains software fixes only, no new enhancments.

Releases E.10.58 and E.10.59 (Never built)

Releases E.10.58 and E.10.59 were never built.

Release E.10.60 Enhancements

Release E.10.60 contains software fixes only, no new enhancments.

Release E.10.61 Enhancements

Release E.10.61 contains software fixes only, no new enhancments.

Release E.10.62 Enhancements

Release E.10.62 contains software fixes only, no new enhancments.

Release E.10.63 Enhancements

Release E.10.63 contains software fixes only, no new enhancments.

Release E.10.64 Enhancements

Release E.10.64 includes the following enhancement:

- **Enhancement (PR_1000340292)** — Flash file system compaction improvements were completed.
- **Enhancement (PR_1000433763)** — The Dynamic ARP Protection feature was added.

Dynamic ARP Protection

Introduction

On the VLAN interfaces of a routing switch, dynamic ARP protection ensures that only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded. For more information about the ARP cache, refer to “ARP Cache Table” in the *Multicast and Routing Guide*.

ARP requests are ordinarily broadcast and received by all devices in a broadcast domain. Most ARP devices update their IP-to-MAC address entries each time they receive an ARP packet even if they did not request the information. This behavior makes an ARP cache vulnerable to attacks.

Because ARP allows a node to update its cache entries on other systems by broadcasting or unicasting a gratuitous ARP reply, an attacker can send his own IP-to-MAC address binding in the reply that causes all traffic destined for a VLAN node to be sent to the attacker's MAC address. As a result, the attacker can intercept traffic for other hosts in a classic "man-in-the-middle" attack. The attacker gains access to any traffic sent to the poisoned address and can capture passwords, e-mail, and VoIP calls or even modify traffic before resending it.

Another way in which the ARP cache of known IP addresses and associated MAC addresses can be poisoned is through unsolicited ARP responses. For example, an attacker can associate the IP address of the network gateway with the MAC address of a network node. In this way, all outgoing traffic is prevented from leaving the network because the node does not have access to outside networks. As a result, the node is overwhelmed by outgoing traffic destined to another network.

Dynamic ARP protection is designed to protect your network against ARP poisoning attacks in the following ways:

- Allows you to differentiate between trusted and untrusted ports.
- Intercepts all ARP requests and responses on untrusted ports before forwarding them.
- Verifies IP-to-MAC address bindings on untrusted ports with the information stored in the lease database maintained by DHCP snooping and user-configured static bindings (in non-DHCP environments):
    - If a binding is valid, the switch updates its local ARP cache and forwards the packet.
    - If a binding is invalid, the switch drops the packet, preventing other network devices from receiving the invalid IP-to-MAC information.

DHCP snooping intercepts and examines DHCP packets received on switch ports before forwarding the packets. DHCP packets are checked against a database of DHCP binding information. Each binding consists of a client MAC address, port number, VLAN identifier, leased IP address, and lease time. The DHCP binding database is used to validate packets by other security features on the switch.

If you have already enabled DHCP snooping on a switch, you may also want to add static IP-to-MAC address bindings to the DHCP snooping database so that ARP packets from devices that have been assigned static IP addresses are also verified.

- Supports additional checks to verify source MAC address, destination MAC address, and IP address.

  ARP packets that contain invalid IP addresses or MAC addresses in their body that do not match the addresses in the Ethernet header are dropped.

When dynamic ARP protection is enabled, only ARP request and reply packets with valid IP-to-MAC address bindings in their packet header are relayed and used to update the ARP cache.

Dynamic ARP protection is implemented in the following ways on a switch:

- You can configure dynamic ARP protection only from the CLI; you cannot configure this feature from the web or menu interfaces.
- Line rate—Dynamic ARP protection copies ARP packets to the switch CPU, evaluates the packets, and then re-forwards them through the switch software. During this process, if ARP packets are received at too high a line rate, some ARP packets may be dropped and will need to be retransmitted.
- The SNMP MIB, HP-ICF-ARP-PROTECT-MIB, is created to configure dynamic ARP protection and to report ARP packet-forwarding status and counters.

Enabling Dynamic ARP Protection

To enable dynamic ARP protection for VLAN traffic on a routing switch, enter the **arp protect vlan** command at the global configuration level.

Syntax: [no] arp protect vlan [*vlan-range*]

vlan-range *Specifies a VLAN ID or a range of VLAN IDs from one to 4094; for example, 1–200.*

An example of the **arp protect vlan** command is shown here:

```
ProCurve(config)# arp protect vlan 1-101
```

Configuring Trusted Ports

In a similar way to DHCP snooping, dynamic ARP protection allows you to configure VLAN interfaces in two categories: trusted and untrusted ports. ARP packets received on trusted ports are forwarded without validation.

By default, all ports on a switch are untrusted. If a VLAN interface is untrusted:

- The switch intercepts all ARP requests and responses on the port.
- Each intercepted packet is checked to see if its IP-to-MAC binding is valid. If a binding is invalid, the switch drops the packet.

You must configure trusted ports carefully. For example, in the topology in Figure 4, Switch B may not see the leased IP address that Host 1 receives from the DHCP server. If the port on Switch B that is connected to Switch A is untrusted and if Switch B has dynamic ARP protection enabled, it will see ARP packets from Host 1 as invalid, resulting in a loss of connectivity.

On the other hand, if Switch A does not support dynamic ARP protection and you configure the port on Switch B connected to Switch A as trusted, Switch B opens itself to possible ARP poisoning from hosts attached to Switch A.

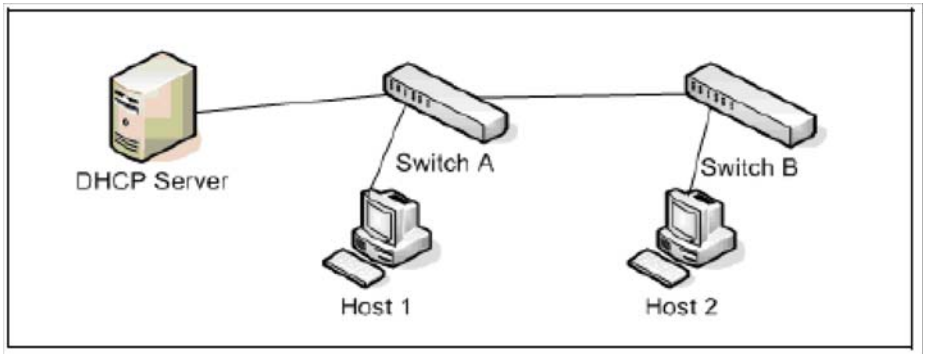

Figure 4. Configuring Trusted Ports for Dynamic ARP Protection

Take into account the following configuration guidelines when you use dynamic ARP protection in your network:

- You should configure ports connected to other switches in the network as trusted ports. In this way, all network switches can exchange ARP packets and update their ARP caches with valid information.
- Switches that do not support dynamic ARP protection should be separated by a router in their own Layer 2 domain. Because ARP packets do not cross Layer 2 domains, the unprotected switches cannot unknowingly accept ARP packets from an attacker and forward them to protected switches through trusted ports.

To configure one or more Ethernet interfaces that handle VLAN traffic as trusted ports, enter the **arp protect trust** command at the global configuration level. The switch does not check ARP requests and responses received on a trusted port.

Syntax: [no] arp protect trust <*port-list*>

port-list	*Specifies a port number or a range of port numbers. Separate individual port numbers or ranges of port numbers with a comma; for example*: **c1-c3, c6**.

An example of the **arp protect trust** command is shown here:

```
ProCurve(config)# arp protect trust b1-b4, d1
```

Adding an IP-to-MAC Binding to the DHCP Database

A routing switch maintains a DHCP binding database, which is used for DHCP and ARP packet validation. Both the DHCP snooping and DHCP Option 82 insertion features maintain the lease database by learning the IP-to-MAC bindings on untrusted ports. Each binding consists of the client MAC address, port number, VLAN identifier, leased IP address, and lease time.

If your network does not use DHCP or if some network devices have fixed, user-configured IP addresses, you can enter static IP-to-MAC address bindings in the DHCP binding database. The switch uses manually configured static bindings for DHCP snooping and dynamic ARP protection.

To add the static configuration of an IP-to-MAC binding for a port to the database, enter the **ip source binding** command at the global configuration level.

Syntax: [no] ip source binding <*mac-address*> vlan <*vlan-id*> <*ip-address*> interface <*port-number*>

mac-address	*Specifies a MAC address to bind with a VLAN and IP address on the specified port in the DHCP binding database.*
vlan <*vlan-id*>	*Specifies a VLAN ID number to bind with the specified MAC and IP addresses on the specified port in the DHCP binding database.*
ip-address	*Specifies an IP address to bind with a VLAN and MAC address on the specified port in the DHCP binding database.*
interface <*port-number*>	*Specifies the port number on which the IP-to-MAC address and VLAN binding is configured in the DHCP binding database.*

An example of the **ip source binding** command is shown here:

```
ProCurve(config)# ip source binding 0030c1-7f49c0
interface vlan 100 10.10.20.1 interface A4
```

Note

Note that the **ip source binding** command is the same command used by the Dynamic IP Lockdown feature to configure static bindings. The Dynamic ARP Protection and Dynamic IP Lockdown features share a common list of source IP-to-MAC bindings.

Configuring Additional Validation Checks on ARP Packets

Dynamic ARP protection can be configured to perform additional validation checks on ARP packets. By default, no additional checks are performed. To configure additional validation checks, enter the **arp protect validate** command at the global configuration level.

Syntax: [no] arp protect validate <[src-mac] | [dst-mac] | [ip]>

src-mac	*(Optional) Drops any ARP request or response packet in which the source MAC address in the Ethernet header does not match the sender MAC address in the body of the ARP packet.*
dst-mac	*(Optional) Drops any unicast ARP response packet in which the destination MAC address in the Ethernet header does not mach the target MAC address in the body of the ARP packet.*
ip	*(Optional) Drops any ARP packet in which the sender IP address is invalid. Drops any ARP response packet in which the target IP address is invalid. Invalid IP addresses include: 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all Class E IP addresses.*

You can configure one or more of the validation checks. The following example of the **arp protect validate** command shows how to configure the validation checks for source MAC address and destination AMC address:

```
ProCurve(config)# arp protect validate src-mac dst-mac
```

Verifying the Configuration of Dynamic ARP Protection

To display the current configuration of dynamic ARP protection, including the additional validation checks and the trusted ports that are configured, enter the **show arp protect** command:

```
ProCurve(config)# show arp protect

ARP Protection Information

Enabled Vlans  : 1-4094
Validate  : dst-mac, src-mac

Port  Trust
----- -----
B1    Yes
B2    Yes
B3    No
B4    No
B5    No
```

Figure 5. The show arp protect Command

Displaying ARP Packet Statistics

To display statistics about forwarded ARP packets, dropped ARP packets, MAC validation failure, and IP validation failures, enter the **show arp protect statistics** command:

```
ProCurve(config)# show arp protect statistics

Status and Counters - ARP Protection Counters for VLAN 1

Forwarded pkts   : 10     Bad source mac     : 2
Bad bindings     : 1      Bad destination mac: 1
Malformed  pkts  : 0      Bad IP address     : 0

Status and Counters - ARP Protection Counters for VLAN 2

Forwarded pkts   : 1      Bad source mac     : 1
Bad bindings     : 1      Bad destination mac: 1
Malformed  pkts  : 1      Bad IP address     : 1
```

Figure 6. Show arp protect statistics Command

Monitoring Dynamic ARP Protection

When dynamic ARP protection is enabled, you can monitor and troubleshoot the validation of ARP packets with the **debug arp protect** command. Use this command when you want to debug the following conditions:

- The switch is dropping valid ARP packets that should be allowed.
- The switch is allowing invalid ARP packets that should be dropped.

```
ProCurve(config)# debug arp protect

1. ARP request is valid
"DARPP: Allow ARP request 000000-000001,10.0.0.1 for 10.0.0.2 port A1,
vlan "

2. ARP request detected with an invalid binding
"DARPP: Deny ARP request 000000-000003,10.0.0.1 port A1, vlan 1"

3. ARP response with a valid binding
"DARPP: Allow ARP reply 000000-000002,10.0.0.2 port A2, vlan 1"

4.ARP response detected with an invalid binding
"DARPP: Deny ARP reply 000000-000003,10.0.0.2 port A2, vlan 1"
```

Figure 7. Example of debug arp protect Command

Release E.10.65 Enhancements

Release E.10.65 contains software fixes only, no new enhancments.

Release E.10.66 Enhancements

Release E.10.66 contains software fixes only, no new enhancments.

Release E.10.67 Enhancements

Release E.10.67 contains software fixes only, no new enhancments.

Software Fixes in Release E.06.01 through E.10.61

Software fixes are listed in chronological order, oldest to newest.

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

Release E.05.04 was the first software release for the ProCurve Series 5300xl switches.

Release E.06.01

Problems Resolved in Release E.06.01

- **100/1000-T module (PR_4956) —** Bringing a port up and down while the port is running at or near maximum throughput may cause the module to reset.
- **802.1x (PR_4972) —** Support for 802.1x is not implemented in routing mode.
- **802.1x (PR_5043) —** When changing an 802.1x port configuration, the switch does not correctly restore default VLAN ID after disconnecting the port.
- **ARP (PR_4443) —** Switch incorrectly replied to an ARP packet with a header length ranging from 7 to 15 bytes. The switch now replies only if header length is equal to 6 bytes.
- **CDP (PR_4546) —** CDP multicast packets are not passed through the switch when CDP is disabled on the switch.
- **CLI/RIP (PR_5046) —** The CLI command 'show ip rip interface' results in the following:
  `"RIP interface information for 0.0.0.0, RIP is not configured on this..."`
- **CoS (PR_4738) —** Cannot configure CoS on a trunk port. Also, enhancements to CoS error handling when moving ports in and out of a trunk.
- **CoS (PR_4982) —** The output of the CLI command “show qos port-priority” may show an illegal state (“no priority”) for the Differentiated Services Codepoint (DSCP) policy. This problem may occur given this situation:
  1. Configure a DSCP policy on a port, and
  2. Remove module, and
  3. Reboot switch, and
  4. Delete DSCP policy, and
  5. Hot-swap module back into the switch
- **Crash (PR_4933) —** Switch may crash while hot swapping a module with a message similar to:
  ```
  -> Software exception in ISR@alloc_free.c:479
  ```

- **DHCP-Relay (PR_4551) —** Configuring an IP helper address on a VLAN does not automatically turn on the DHCP-relay function.
- **Extended RMON (PR_5083) —** When Extended RMON and Routing are enabled, the switch may duplicate packets on the network.
- **LACP (PR_5000) —** Link-up polling interval: A delay of up to 1.7 seconds between plugging in a cable (linkbeat established) and traffic being forwarded to and from that port may cause problems with some time sensitive applications. For example, AppleTalk dynamic address negotiation can be affected, resulting in multiple devices using the same AppleTalk address.
- **Mini-GBIC Link Connectivity Issue (PR_4957) —** A mini-GBIC Gigabit-SX/LX link between an ProCurve Switch 5300xl and an ProCurve Routing Switch 9300 may not be established when both sides are in the default configuration (Auto).
- **Radius (PR_4886) —** If using the TAB key while entering a username for the radius prompt, the switch may display an error message similar to:

```
->BAD CHARACTER IN ttyio_line: 0x9n
```

- **RIP (PR_4757) —** After the switch reboots and if a routing loop (3 or more routers) exists in the topology, RIP may age out its own connected routes (even though the routes are still valid).
- **RIP (PR_4965) —** Static routes are redistributed into RIP. [Fix: Static routes are no longer redistributed into RIP by default, only directly connected routes are redistributed.] [Old description: Changes to RIP route redistribution such that only connected routes are redistributed, not static configured routes.
- **RIP (PR_4987) —** If multiple IP addresses are configured for a VLAN and RIP is running on one or more of the secondary addresses, the CLI command “show ip rip vlan x” will only show information about the primary IP address.
- **Routing (PR_4977) —** If a default route is not configured and the switch receives a Layer 3 packet with an unknown source address, the packet will be routed by software even though an entry for the destination exists in the hardware routing table.
- **Static Routes (PR_5040) —** Reject static routes could not be created.
- **Web Browser Interface (PR_4976) —** The product Registration screen contains a typographical error. The phrase “...does not appears above...” is now “...does not appear above...”.

Release E.06.02

Problems Resolved in Release E.06.02

- **Performance (PR_5161)** — Certain high traffic levels may cause the switch to drop packets.

Release E.06.03

Problems Resolved in Release E.06.03

- **Packets not Forwarded (PR_5201)** — A synchronization issue between the switch chassis and modules after several weeks of continuous operation can result in packets being dropped by the switch instead of being forwarded.

Release E.06.05

Problems Resolved in Release E.06.05

- **Crash (PR_5471)** — The CLI command "show ip ospf neighbor" may cause the switch to crash with a message similar to:

```
Bus error: HW Addr=0x30008fa0 IP=0x001112a4 Task='mSess1' Task
ID=0x169b110
```

Release E.06.10

Problems Resolved in Release E.06.10

- **Crash (PR_5229) —** Greater than 100 hotswaps causes mesg buff crash.
- **Flow Control (PR_5215) —** Enabling Flow Control on a port does not enable Global Flow Control on the switch.
- **Security (PR_5226) —** Removed display of TACACS Server IP address during remote management logon.
- **Security (PR_5227) —** TCP Port 1506 access is closed when Telnet or Stacking is disabled.
- **Web-browser interface (PR_5052) —** Executing the CLI command "**no web-management**" does not disable access to the web-browser interface.

Release E.07.21

Problems Resolved in Release E.07.21

- **ARP (PR_5185) —** ARP has been enhanced to have a configurable timeout value, beyond the current default of 20 minutes.
- **CDP (PR_5054) —** CDP multicasts are not passed when CDP is disabled on the switch.
- **CLI (PR_5053) —** Setting the telnet inactivity timeout from the CLI does not indicate a reboot is necessary for changes to take effect.

- **CLI (PR_4984) —** The definition of default gateway following the “ip?” in the CLI is stated as “Add/delete default route to/from routing tale.”, which is incorrect. Clarified help text for 'ip default-gateway' CLI command to state that this parameter is only used if routing is not enabled on the switch.
- **CLI (PR_5242) —** Information in the command “show boot-history” is not in the order claimed (most recent first).
- **Crash (PR_4621) —** The switch may crash with a message similar to:

  ```
  NMI occurred: IP=0x00317d9c MSR:0x0000b000 LR:0x00013b88
  Task='eDrvPollRx' Task ID=0x1708f20 cr: 0x22000080 sp:0x01708e60 xer:
  ```

- **Crash (PR_5745) —** The switch may crash with a message similar to:

  ```
  -> Divide by Zero Error: IP=0x801400c0 Task='sal_dpc_hi'
     Task ID=0x80616690 fp:0x00000000 sp:0x80616600 ra:0x800140060
     sr:0x1000af01
  ```

- **Crash (PR_5635) —** The switch may crash with a message similar to:

  ```
  -> Assertion failed:0, file drvmem.c,  line 167
  ```

- **Crash (PR_5679) —** The switch may crash with a message similar to:

  ```
  -> Bus error: HW Addr=0x00000000 IP=0x00000000 Task='mNSR' Task
     ID=0x1725148 fp: 0x0000c4b0 sp:0x012e9780 lr:0x00330674
  ```

- **Crash (PR_5712) —** The switch may crash with a message similar to:

  ```
  -> TLB Miss: Virtual Addr=0x00000000 IP=0x8002432c Task='tSmeDebug'
  ```

- **Crash (PR_5725) —** The switch may crash with a message similar to:

  ```
  -> Assertion failed: nt, file dpc.c, line 169
  ```

- **Crash (PR_5846) —** WhatsUpGold telnet scan can cause switch to run out of memory and crash with error message similar to:

  ```
  -> malloc_else_fatal() ran out of memory
  ```

- **Crash (PR_5955) —** The switch may crash with a message similar to:

  ```
  Software exception at alpha_chassis_slot_sm.c:506
  ```

- **Crash (PR_4986) —** The switch may crash with a message similar to:

  ```
  -> Bus error: HW Addr=0x00ffffff IP=0x332c4530 Task='mSess1' Task
     ID=0x16a62f0 fp: 0x2e2e2e29 sp:0x016a61a0 lr:0x0010f028
  ```

  This crash can occur when eight transceiver modules are installed and the command “interface all” is typed in the configuration context.

- **Crash (PR_5418) —** The switch may crash with a message similar to:

  ```
  -> Software exception at rtsock.c:459 -- in 'tNetTask', task ID =
  0x1a225b0
  ```

- **Crash (PR_5635) —** The switch may crash with a message similar to:

  ```
  -> Assertion failed:0, file drvmem.c,  line 167
  ```

- **Crash (PR_5341) —** All three of the following steps must occur before the crash is exhibited:

  1. .A 1000-T port (without a link) is configured as a mirror destination port.
  2. Another blade/port traffic is mirrored to that destination port.
  3. Mirror destination port/blade will crash or hang after connecting, then disconnecting a 100T link with a message similar to:

     ```
     Software exception at nc_fd_fi.c:693 - in 'mPmSlvCtrl'task ID =
     0x405e9cc8 -> netchip_FIOutboundFlush: Timeout reached!
     ```

- **Crash (PR_5236) —** The switch may crash with a message similar to:

  ```
  -> AlphaSlaveAddrmgr.p 1021 this time
  ```

  This crash can occur when a module is hot-swapped after downloading new software to the switch without rebooting.

- **Date/Time (PR_5264) —** The timezone can cause the date to wrap if the timezone is set to a valid, but negative value (like -720) without previously configuring the switch's time. The switch may report an invalid year (i.e. 2126).

- **DHCP —** If a client moves without first releasing its IP address, it will not receive a NAK, resulting in the client's inability to get an IP address at its new location.

- **Event Log (PR_5154) —** When a module fails to download, the severity code is INFO instead of WARNING.

- **Fault Finder/CLI (PR_4696) —** Setting fault finder sensitivity always resets action configuration to 'warn', when it should remain 'warn and disable'.

- **FFI/Port Counters (PR_5429) —** No errors are reported by the FFI or port counters when linking at 100 HDX on a Gigabit port with a duplex mismatch.

- **FFI/Port counters (PR_5280) —** FFI and port counters don't have consistent values.

- **Filter (PR_5132) —** Source port Filter on Dyn1 LACP trunk creates Multicast Filter entry that cannot be deleted.

- **Filter (PR_4833) —** Creating a source port filter for a port, moving the port into a trunk, and then reloading the saved TFTP configuration file results in a corrupted download file error.
- **Flow Control (PR_5102) —** Setting a port “X1” in 10-HDX, then attempting to turn on flow control returns an error similar to: “Error setting value fl for port X2”. The error should read “X1”.
- **GVRP (PR_5284) —** Port does not register VLAN even though advertisements are received.
- **Hot-swap (PR_4900) —** Hot-swapping a transceiver logs a message requesting to reboot the switch in order to enable the port, which is not necessary.
- **IGMP (PR_5736) —** If IGMP is turned on for multiple VLANs, and is then turned off for a single VLAN, the Data-Driven Mcast filters for that VLAN are not flushed.
- **IP (PR_5408) —** IP is causing the driver to apply source port filters incorrectly to non-routed packets.
- **IRDP (PR_5923) —** When running the 'rdisc' router discovery tool under Redhat 8.0 or 7.3, Linux reports “ICMP Router Advertise from <IP>: Too short 16 40” when a IRDP packet is received.
- **LACP/Port Security (PR_5059) —** With LACP on, the command “port-sec a1 l c action send-alarm” fails with a message similar to “learn-mode: Inconsistent value”.
- **Link Toggle Corruption (PR_5527) —** Addressed issue whereby toggling ports with active, bi-directional traffic could result in corrupted packets within the system.
- **Link-up Polling Interval (PR_5000) —** A delay of up to 1.7 seconds between plugging in a cable (linkbeat established) and traffic being forwarded to and from that port may cause problems with some time sensitive applications. For example, AppleTalk dynamic address negotiation can be affected, resulting in multiple devices using the same AppleTalk address.
- **Menu (PR_5346) —** The one-line help text below the password entry field, displays the message "`Enter up to 16 characters (case sensative), or just press <Enter> to quit`". It should read "`...sensitive...`".
- **Meshing (PR_4969) —** Traffic on oversubscribed mesh links will migrate to other mesh links too slowly.
- **Meshing (PR_4980) —** Meshing does not maintain priority on encapsulated packets that are sent out non-mesh ports.
- **Multicast Filters (PR_4741) —** Any static multicast filters configured once the limit has been reached, would appear in the output of the “show filter” CLI command with only partial information. Switch now correctly returns error message “Unable to add filter” once limit has been reached.

- **OSPF (PR_88611) —** When configured for authentication-key type “simple passwords”, the switch does not include the password in OSPF packets.
- **Port Configuration (PR_5444) —** When interchanging 10/100-TX modules J4862A and J4862B, the port configuration of the module originally installed in the switch is lost.
- **Port counters (PR_5013) —** Hardware port counter filters for dot1dTpPortInDiscards not implemented.
- **Port counters (PR_5171) —** The “Total RX Error” counter is incorrect when the port has heavy 10HDx traffic.
- **Port counters (PR_5204) —** The Runt Rx counter in the detail port counter screen, does not increment when there are fragments.
- **Port counters (PR_5400) —** The 64-bit counter for the highest numbered port on a given module, does not update properly.
- **RADIUS (PR_4886) —** Pressing the tab key gives error message similar to “BAD CHARACTER IN ttyio_line: 0x9n” when entering a username for the radius prompt.
- **RSTP (PR_5449) —** There is a delay in the switch relearning MAC addresses when an RSTP port transitions from Blocking to Forwarding.
- **Self Test (PR_5113) —** There are intermittent port failures reported on ProCurve switch xl 100/1000-T modules (J4821A) while performing a packet self test, which was due to the packet test not seeing the very first packet.
- **SNMP (PR_5349) —** The switch does not send SNMP packets larger than 484 bytes.
- **SNTP/TIMEP (PR_5018) —** SNTP still runs when TIMEP is enabled.
- **Source Port Filters (PR_4669) —** Source port filters for illegal ports and trunk port members cannot be deleted from the CLI.
- **Source Port Filters (PR_4719) —** The switch does not automatically remove a source port filter for a trunk that has been deleted.
- **System Information (PR_5169) —** Up Time displayed is not correct.
- **TACACS (PR_5226) —** During TACACS Authentication the TACACS Server's IP address is shown on the switch's 'splash screen'.
- **TCP (PR_5227) —** TCP port 1506 is always open. Fix is to close TCP port 1506.
- **TFTP (PR_5034) —** Trying to TFTP a config onto the switch causes the switch to not complete its reload process. The switch hangs and does not come up.
- **VLANs (PR_4405) —** The VIDs of deleted VLANs are not removed from the switch's VLAN table, causing the switch to not allow new VLANs to be created (once the VID table is full).

- **Web (PR_5455) —** Bad URL was being mirrored back to the user following Nessus script attack test.
- **Web-Browser Interface (PR_5199) —** Having a ProCurve switch 4100gl series as a commander, and a ProCurve switch 4000m as a member of the stack, the stack commander was not checking security when doing passthrough.
- **Web-Browser Interface (PR_5052) —** The CLI does not disable the web-browser interface.
- **Web-Browser Interface (PR_5055) —** Missing firmware/ROM information in Web UI.
- **Web-Browser Interface (PR_5158) —** When clicking on the Web UI System Info "Apply Changes" button, a character appears under the "VLAN Configuration" tab.
- **Web-Browser Interface (PR_4976) —** Mis-spelled word on the product registration screen of the WEB UI. The phrase "...does not appears above..." is now "...does not appear above..."
- **Web-Browser Interface (PR_4996) —** When using a ProCurve Switch 4108 as a commander switch in the stack, a ProCurve Switch 2424M is not shown in the device view of the stack closeup in the web UI. The message "Device view, HP2424M, not supported by firmware of commander" is present instead of the device view.
- **Web-Browser Interface (PR_4904) —** When a transceiver is removed from the switch, its configuration is not cleared on the Status->port status screen of the web UI. The transceiver type will still show until a new transceiver is inserted.
- **Web-browser Interface (PR_4235) —** Web-browser port utilization label does not display the bandwidth number. Shows x% of 0Mb instead of x% of 100Mb or x% of 1Gb.
- **Web-Browser Interface (PR_4495 —** Administrator password can be used in combination with the operator username.

Release E.07.22

Problems Resolved in Release E.07.22

- **Meshing/Packet Buffer Depletion (PR_88694) —** Certain mesh topologies may cause packet buffers to be depleted on the switch. In this state the switch will generate an "`Out of pkt buffers`" Event Log message.
- **OSPF (PR_88718) —** In topologies where the switch has redundant routes (via a directly connected link and via an OSPF learned route) to the same network, the switch does not learn the alternate route via OSPF when the directly connected link goes down.

- **Port Hang (Packet Not Forwarded) (PR_88613) —** Under certain traffic load conditions, ports that are toggling on the mini-GBIC module (J4878A) may stop transmitting packets.

Release E.07.27

Problems Resolved in Release E.07.27

- **Enhancement (PR_90365) —** Modifications have been made to the switch meshing code to allow limited mesh interoperability between E.07.*x* and pre-E.07.*x* software to allow easier upgrades of all switches in a mesh. (Current implementation does not allow switches running pre-E.07.*x* software to participate with meshed switches running E.07.*x* or greater.)
- **IGMP (PR_82491) —** A Group-Specific Query (GSQ) timeout is currently .2 to .6 seconds, rather than the specified default of 1 second.
- **IGMP (PR_90376) —** In some cases, the switch would display "0.0.0.0" for the output of the CLI command "show ip igmp".
- **Meshing (PR_88689) —** A 12-switch mesh may cause the switch to temporarily run out of packet buffers.
- **Telnet (PR_82522) —** Switch TELNET connections were not closed properly resulting in new TELNET sessions being established which could result in the switch reaching its maximum number (3) of TELNET sessions.
- **Web-Browser Interface (PR_82530) —** A client using Sun java 1.3.X or 1.4.X to access the Web-Browser Interface of the switch, may cause the switch's CPU utilization to increase causing agent processes (such as console, telnet, STP, ping, etc.) to stop functioning.

Release E.07.29

Problems Resolved in Release E.07.29

- **ACL (No PR)** — The switch allows a user to execute a "no access-list" command for a non-existent ACE without responding with an appropriate error message.
- **ACL (PR_90250)** — Packets that match a "denied" ACL entry may cause the switch's CPU to run at full utilization.
- **ACL (PR_90415)** — On ACL entries such as "permit/deny tcp any any" the switch will incorrectly permit/deny UDP traffic. The same is inversely true for ACL entries such as "permit/deny udp any any" resulting in TCP traffic being permitted/denied.
- **ACL Performance (PR_90366)** — Addressed potential performance issues of cached TCP and UDP ACL entries.

- **Config (PR_88753)** — A 1000-FDX port setting in the switch config file is not processed properly, resulting in Gigabit-SX ports remaining in an "auto" port configuration. This is most often seen when reloading or TFTP'ing a config file to the switch.
- **Port-sec (PR_88612)** — Static MAC addresses are set up under port security with learn-mode "configure specific" to allow those MAC addresses to communicate through the switch. If one of those MAC addresses is removed via the Web interface of the switch and then re-entered, the owner of that MAC address cannot communicate through the switch.
- **Routing (PR_90554)** — Cached routing information was only updated by IP routable datagrams, and was not being updated by Layer-2 traffic such as ARP.
- **Self Test (PR_90777)** — A self test error may occur when a Gigabit-SX, or LX mini-GBIC module is inserted into the switch while powered on.
- **Spanning Tree (PR_90412)** — Enhancements made to 802.1w operation to address version 3 BPDU communication issues.

Release E.07.30

Problems Resolved in Release E.07.30

- **Agent Performance (PR_81861)** — The switch may get into a state where end nodes and other network devices cannot contact (ping, telnet, SNMP, etc.) the switch's agent.
- **Routing (PR_90802/91236)** — The switch may route packets out the wrong port due to a mismatch between the source and destination MAC addresses.

Release E.07.34

Problems Resolved in Release E.07.34

- **Agent Hang (PR_92802)** — The switch may become unresponsive or hang due to UDP port 1024 broadcast packets never being freed, after the TIMEP and SNTP clients are disabled on the switch.
- **Crash (PR_92659)** — Software exception at memrpt.c:1153 -- in 'mInstCtrl', task ID = 0x1455a30
- **IPv6 (PR_93171)** — The switch does not forward IPv6 Router Solicitation/Advertisements when IGMP is enabled.
- **Routing / Agent Performance (PR_95009)** — Routing performance may be degraded due to the aging of host route entries. In this scenario, traffic will be routed through the switch software, thereby resulting in lower performance of routing and agent access (TELNET, SNMP, ping, etc.) operations.

- **VLAN (PR_92466)** — The switch may experience a Bus error related to 802.1X/unauthorized VLAN. The Bus error is similar to:

  ```
  Bus error:  HW Addr=0x3861000c IP=0x002df470 Task='mAdMgrCtrl'Task
  ID=0x16e616 0 fp: 0x006a090c sp:0x016e5df0 lr:0x0021d6d8
  ```

Release E.07.37

Problems Resolved in Release E.07.37

- **Crash (PR_90217)** — The switch may crash under high stress in a very large mesh topology with a message similar to:

  ```
  Bus error:  HW Addr=0x08040010 IP=0x002c8b48 Task='eDrvPoll' Task
  ID=0x177fdb0 fp: 0x01682e38 sp:0x0177f9e8 lr:0x002c8ae0.
  ```

- **Crash (PR_90374)** — The J4878A mini-GBIC module may cause the switch to crash with a message similar to:

  ```
  "Slot B SubSystem 0 went down:  01/01/90 13:05:41 Software exception
  at dmaRx.c:211 -- in 'tDevPollRx', task ID = 0x40808b78 -> FAULTY INK
  PARTNER CONNECTED ON SLOT".
  ```

- **Crash (PR_94852)** — The switch may crash when in a mesh configuration with a message similar to:

  ```
  Bus error:  HW Addr=0xdc37e837 IP=0x002c944c Task='eDrvPoll'  Task
  ID=0x173fdb0 fp: 0x01054468 sp:0x0173fa50 lr:0x002c93c0.
  ```

- **Crash (PR_95284)** — If a user enters an invalid MAC address during the Port Security configuration within the CLI, the switch may crash with a message similar to:

  ```
  Software exception at exception.c:345 -- in 'mSess1', task ID = 0x141ae70
  -> Memory system error at 0x131b5a0 - memPartFree
  ```

- **Meshing (PR_96007)** — If a mesh link is broken then shortly followed by the learning of new MAC addresses, the switch may exhibit problems such as bus errors and/or improper communication with other mesh switches.

- **SNMP (PR_96999)** — When the switch is reset (or power-cycled) after configuring an SNMP Community Name with “Operator/Restricted” Rights, it will still allow SNMP sets (writes) to MIB objects.

Release E.07.40

Problems Resolved in Release E.07.40

- **Agent Hang (PR_97705)** — Agent processes (Ping, TELNET, SNMP, etc.) may stop functioning.
- **ARP (PR_92421/93008/97993)** — Default ARP aging time is 1,200 minutes when it should be 20 minutes. User-configured ARP aging times do work correctly.
- **Crash (PR_95293)** — The switch may crash with a message similar to:

  ```
  Bus error:  HW Addr=0x08000001 IP=0x00267cc4 Task='mIpAdMCtrl'  Task
  ID=0x150520 fp: 0x00000020 ip:0x01505100 lr:0x00267ca0
  ```

  This crash has been associated with traffic patterns generated by the Blaster and Welchia worms.
- **Crash (PR_96236)** — The switch may crash with a message similar to:

  ```
  "Software exception at ipaddrmgrSCtrl.c:2108 -- in 'mIpAdMUpCt'"
  ```
- **Crash (PR_97048/97083)** — The switch may crash with a message similar to:

  ```
  Bus error:  HW Addr=0x1bee13a8 IP=0x00267b68 Task='mIpAdMCtrl'  Task
  ID=0x14c2fe0 fp: 0x00000028 sp:0x014c2e98 lr:0x00267b58.  In QA code:
  Software exception at route.c:296. Attempt to free a null route.
  ```
- **Hang (PR_97031)** — Switch may hang (routing and console) due to infinite loop issue in ACL code.
- **Routing (PR_98494/97301)** — The switch may exhibit slower-than-normal routing performance due to route entries not being aged properly.
- **Routing (PR_98847)** — Under some conditions when there are more than 32 VLANs and IGMP enabled, the switch may not route.
- **X-modem (PR_95748)** — When trying to download a zero-length OS file to the switch, the switch may crash with a message similar to:

  ```
  Software exception at fileTransfer.c:552 -- in 'mftTask', task ID =
  0x1241ca8 -> Could not open file.
  ```

Release E.08.01

Problems Resolved in Release E.08.01

- **ACL (PR_94945)** — 5300 allows duplicate ACEs (Access Control Entries) to be entered within an ACL.
- **CERT (PR_96648)** — Applied OpenSSH patches to switch for CERT Advisory CA-2003-24 related problems.

- **CLI (PR_81948)** — There are currently two “enable” commands present within the “Interface Config” context; one is to enable the port, the other is to enter manager context. The “enable” command is now filtered when not in the Operator Context within CLI.
- **CLI (PR_82475)** — The help text displayed for source-route is incorrect when auto-extend is applied to the command “IP”.
- **CLI (PR_90302)** — The help text within CLI for the “Interfaces” command is grammatically incorrect.
- **Crash (PR_88831)** — The switch may crash with a message similar to:

  ```
  02/27/03 15:48:09 Bus error: HW Addr=0x02000000 IP=0x0013866c
  Task='mSess2' Task ID=0x1654700fp: 0x01654a40 sp:0x016533a0
  lr:0x0013874
  ```

- **Crash (PR_1000002979)** — The switch may crash with a message similar to:

  ```
  Software exception at rstp_port_role_sm.c:44 -- in 'mRstpCtrl', task
  ID = 0x1379a48-> ASSERT:  failed
  ```

- **Crash (PR_1000003288)** — The 10/100 Module (J4820A) under conditions of heavy port toggling may crash with a message similar to:

  ```
  Software exception @ dmaRx.c: 237.
  ```

- **Crash (PR_89847)** — The switch may crash with a message similar to:

  ```
  Software exception in ISR at alpha_hs_int.c:547

  -> NCI_INTERRUPT_ERROR. Slot 3 NCI_IntReg=0x4000
  ```

- **Enhancement (PR_81844)** — Enhancement to improve “Debug HELP” information provided via CLI.
- **IP (PR_1000000728)** — The switch does not notify the IP Address Manager when an RSTP topology change occurs.
- **Logging (PR_82509)** — The switch will reboot when an invalid IP address is assigned to the logging feature, while “Logging” is turned off.
- **Meshing (PR_82502)** — Improved meshing performance during network conditions when there are large volumes of Port “learns” and “moves”.
- **Routing (PR_93205)** — The switch incorrectly allows for a configuration in which a static route can be configured as 127.x.x.x.
- **RSTP (PR_1000001612)** — A port takes approximately 30 seconds to go into the Forwarding state.

- **Security (PR_90899)** — After configuring a port to be "learn-mode configured", the "show port security" output within the CLI lists "Static" as the learn mode, rather than “Configured”, as it should be.
- **Security (PR_91855)** — The switch may fail to forward authentication requests to a RADIUS server when an unauthorized VID is configured and “Port-Security” is set to 802.1x.
- **Syslog (PR_91123)** — The switch may fail to send messages to a configured Syslog server.
- **VLAN (PR_92426)** — Unable to delete a VLAN by name if the name is numeric within the CLI.
- **Web Agent (PR_82157)** — There is a missing graphic in the upper left hand corner of the “First time installation” pop up window.
- **Web UI (PR_90858)** — Unable to clear the “VLAN Name” text field after 12 characters are entered within the Web UI.
- **XRMON (PR_98199)** — The “BroadcastPackets” counters for MIB object 1.3.6.1.2.1.16.1.1.1.6 on the 53xx series switch are incorrect.

Release E.08.03

Problems Resolved in Release E.08.03

- **Crash (PR_1000007148)** — The switch may crash with a message similar to:

  ```
  Bus error: HW Addr=0x7c7343b2 IP=0x002c3e54 Task='mIpAdMCtrl'.
  ```

- **Crash (PR_1000007227)** — The switch may crash with a message similar to:

  ```
  Software exception at alloc_free.c:485 -- in 'tDevPollTx', task ID =
  0x17a3.
  ```

Release E.08.07

Problems Resolved in Release E.08.07

- **ACL (PR_1000006679)** — The configured ACL “Range” parameter may not function properly after a reboot.
- **CLI (PR_82086)** — The command **show mac <mac-address>** does not function.
- **CLI (PR_ 1000000560)** — The port security “Help” screen has been updated to include learn mode "Limited-Continuous".
- **CLI (PR_1000004025)** — After the switch is up for approximately 49 days, the “Up Time” from the **show system** command will not be accurate.

- **CLI (PR_1000095690)** — Error message improved when a user enters an Interface Name that is too long.
- **Crash (PR_1000004216)** — The switch may crash with a message similar to:

  ```
  Driver corrupted - Slave Bus Error: dmaTxPollPackets.c:724
  ```

- **Crash (PR_1000005210)** — The switch may crash with a message similar to:

  ```
  Exception in ISR at dmaRx.c:830
  ```

- **Crash (PR_1000005829)** — The switch may crash with a message similar to:

  ```
  Software exception at alphaHwRateLimits.c:84
  ```

- **Crash (PR_1000005902)** — In cases where a heartbeat failure may occur, the switch will provide more specific and informative crash information.
- **Crash (PR_1000006392)** — The switch may crash with a message similar to:

  ```
  Software exception at pmgr_util.c:1500 -- in 'mLACPCtrl'
  ```

- **Crash (PR_1000006427)** — The switch may crash with a message similar to:

  ```
  Software exception at lacp_util.c:1723 - in 'mLACPCtrl'
  ```

- **Crash (PR_1000006833)** — The switch may crash with a message similar to:

  ```
  Slave crash at AlphaSlaveLearn.c:1576
  ```

- **Crash (PR_1000006967)** — The switch may crash with a message similar to:

  ```
  Exception at sw_malloc.c:141  Out of Memory - SSH
  ```

- **Crash (PR_1000006988)** — The switch may crash with a message similar to:

  ```
  Slave crash in ISR @ dmaRx.c:838
  ```

- **Crash (PR_1000007148)** — The switch may crash with a message similar to:

  ```
  Bus error:  HW Addr=0x7c7343b2 IP=0x002c3e54 Task='mIpAdMCtrl'
  ```

- **Crash (PR_1000007221)** — The switch may crash with a message similar to:

  ```
  Slave crash in mPmSlvCtrl at nc:phy.c:594
  ```

- **Crash (PR_1000007227)** — The switch may crash with a message similar to:

  ```
  Software exception at alloc_free.c:485 -- in 'tDevPollTx', task ID =
  0x17a3c58'
  ```

- **Crash (PR_1000011477)** — The switch may crash with a message similar to:

  ```
  Bus error:  HW Addr=0x06836252 IP=0x00444f14 Task='mHttpCtrl'  Task
  ID=0x11257f8
  ```

- **Crash (PR_1000011517)** — The switch may crash with a message similar to:

  ```
  Slave crash in ISR at dmaRx.c:838
  ```

- **Crash (PR_1000013156)** — Addressed master crash problem in memory system.
- **IP Helper (PR_1000004029)** — Number of IP Helper addresses increased to 256 on the 5300.
- **MAC Authentication (PR_1000019250)** — The switch will crash if a MAC Authentication configured port is then configured for Trunking.
- **Meshing (PR_1000012101)** — A meshed switch may cause a broadcast loop on the network after a new module is inserted.
- **MDI/MDI-X (PR_1000001452)** - MDI/MDIX mode not described in help.
- **Port Monitoring (PR_1000012218)** — When port monitoring is configured, meshing protocol packets may be sent out the wrong meshed ports.
- **Port Security (PR_10000001437)** — Eavesdrop prevention.
- **RMON (PR_1000011690)** — When RMON thresholds in the switch are exceeded, no trap is generated.
- **STP (PR_1000005371)** — Unable to set spanning tree "hello-time" via CLI in STP mode.
- **VLAN (PR_1000006670)** — If a port resides only in a protocol VLAN, the menu will not allow the user so save changes from the VLAN configuration window within the menu.
- **Web UI (PR_1000000256)** — The Web UI may display a module as a "humpback module"
- **Web UI (PR_1000007144)** — The VLAN Configuration help link is not available within the Web UI.

Release E.08.30

Problems Resolved in Release E.08.30

- **Auto-TFTP (PR_20802)** — Configuring the **auto-tftp** command with an incorrect IP address for the TFTP server can cause the switch to reboot every 5-15 minutes.
- **CLI (PR_1000000769)** — **update** and **upgrade-software** should not be normal CLI commands.
- **CLI (PR_1000001384)** — Misspelling in CLI Help screen for the **static-mac** command.
- **CLI (PR_1000001897)** — Help screen for **logging** command does not mention ‘Major’ logs.

- **CLI (PR_1000001628)** — The CLI may incorrectly reject the adding of ports to a VLAN, and respond with an `Inconsistent Value` error message.
- **CLI (PR_1000005912)** — The slot/module identifications within the CLI are incorrect and show slots numerically, rather than alphabetically.
- **CLI (PR_1000097427)** — Extraneous columns in the **show authentication** command.
- **Config (PR_1000020659)** — ProCurve 24 port 10/100 POE module identified with part number J8151A rather than with the appropriate part number, J8161A.
- **CDP (PR_1000004099)** — CDP advertises the switch as being only a router when routing is enabled. Changes made so that the switch now advertises itself as both a router and a switch when routing is enabled.
- **Crash (PR_1000007319)** — The switch may crash with a message similar to:

  ```
  Software exception in ISR at dmaRx.c:830 -> No resources available
  ```

- **Crash (PR_1000019386)** — The switch may crash with a message similar to:

  ```
  NMI occured: IP=0x00466f68 MSR:0x0000b032 LR:0x00000000
  Task='eDMAEmg001' Task ID=0x1625f58 cr: 0x22000000 sp:0x01625eb0
  xer:0x00000000
  ```

- **Enhancement (PR_1000020429)** — Added the **show chassis-version** CLI command.
- **Help (PR_1000000560)** — Within the CLI, the Port Security Help file does not reference the learn mode "Limited-Continuous".
- **Help (PR_1000013464)** — The **show mac-address** Help text is too long and exceeds the 80 character limitation.
- **Monitoring Port (PR_1000012218)** — Port monitoring a mesh port can cause mesh packets to be transmitted out the wrong port.
- **PIM (PR_1000004117)** — "Expiry Time" changed to "Expire Time" following the **show ip PIM neighbor lists** command within the CLI.
- **PIM (PR_1000004818)** — PIM may not go into a forwarding state when a new neighbor that doesn't support state refresh connects.
- **PIM (PR_1000005019)** — PIM will forward state refresh that is not from the assert winner.
- **PoE (PR_1000019004)** — Extraneous `Power Denied` messages have been eliminated when EPS power has been lost.
- **Port Security (PR_1000013075)** — A port with Port Security enabled may learn addresses beyond its configured limit, and require a reboot to clear.

- **SSH (PR_1000003227)** — Need a special case for the SSH protocol-version configuration parameter to provide compatibility when back-revving to pre-E.08.*xx* code.
- **SSH (PR_1000004993)** — Memory corruption in SSH function.
- **SSL (PR_1000012823)** — SSL code modifications.
- **VLANs (PR_1000006670)** — Protocol VLANs configured in the CLI may not show up in the VLAN menu config screen and report that the member ports are orphaned.

Release E.08.42

Problems Resolved in Release E.08.42

- **ACL (PR_1000023119)** — An invalid VLAN ACL will remain in the configuration.
- **CLI (PR_1000002138)** — Incorrect message displayed in the CLI **aaa port-access** command.
- **CLI (PR_1000022443)** — Within the CLI Menu context, user unable to set a port as an untagged member of a VLAN.
- **CLI (PR_1000085477)** — The word "Specify" in 'ip route' is misspelled.
- **CLI (PR_1000085495)** — The word "unavailability" is spelled wrong for the "radius server dead-time" description within the CLI.
- **Crash (PR_1000021489)** — The switch may crash with a message similar to:
  `Software exception at i2cdriver.c:75 in 'swInitTask'`
- **Crash (PR_1000021567)** — The switch may crash with a message similar to:
  `Software exception @ ipaddrmgrSCtrl.c:565`
- **Crash (PR_1000022106)** — The switch may crash with a message similar to:
  `Exception hit in alphaSLaveLearn.c:1534`
- **Crash (PR_1000022814)** — The switch may crash with a message similar to:
  `Software exception at alpha_chassis_slot_sm.c:563 -- in 'eChassMgr', task ID = 0`
- **Crash (PR_1000086916)** — The switch may crash with a message similar to:
  `Software exception at if_ether.c:693 -- in 'tNetTask', task ID = 0x196d9b0 -> ASSERT:  failed`
- **Crash (PR_1000087055)** — The switch may crash with a message similar to:
  `Software exception at ssh_utils.c:973 -- 'mftTask'`
- **Hang (PR_1000006985)** — The switch management may hang due to a memory corruption.

- **Security (PR_1000021329)** — Within the Web UI, the "Address Limit" value was always displayed as **4** for a learn mode of **Limited**.
- **Security (PR_1000021732)** — A configured IP Authorized Manager will fail following a reboot.
- **Security (PR_1000085928)** — The **show port-access authenticator 1** CLI command shows all port-access configured, but should show information for specified ports only.
- **SFlow (PR_1000021518)** — SFlow returns **sysUpTime** in 100ths of seconds, rather than 1000ths.
- **SFlow (PR_1000021776)** — The SFlow **sysUpTime** is not in sync with the switch **sysUpTime**.
- **SSH (PR_1000087086)** — The switch does not report an error message after rejecting a public key file with more than 10 keys.
- **Web UI (PR_89899)** — The Web UI port statistic counters are overwriting one another.
- **Web UI (PR_1000021867)** — VLAN context within Web UI may not allow untagged ports to be added to a VLAN.
- **Web UI (PR_1000085927)** — The Help text is not available from the authorized manager screen.

Release E.08.53

Problems Resolved in Release E.08.53

- **IP Helper/DHCP Relay (PR 1*197046)** — May not handle "DHCP Inform" relay properly.
- **NAT (PR_1*199309)** — Routing to some end nodes fails when a cable is moved from one port to another or when the equivalent action happens due to XRRP fail-over or fail-back.
- **NAT (PR_1*203787)** — NAT problem when the switch has multiple VLANs configured on a port with routing enabled (that is, the one-armed router scenario)
- **SNMP/Authorized Manager (PR_1*86062)** — SNMP Sets allowed when in Operator mode and IP Authorized-Manager is set.

Release E.09.02 (Beta Only)

Problems Resolved in Release E.09.02

- **DMA Driver (PR_1000209595) —** ASSERT_RESOURCE prints `No resources available` if it fails.
- **IP Addmgr (PR_1000202539) —** ARP cache gets cleared whenever a port comes up.

- **IP Addmgr (PR_1000206356) —** Software exception at `ipamMAcl.c:712` -- host table filled with no ACLs.
- **MGR (PR_1000202237)** — VLAN MAC table flushing does not work.
- **Mirror Port (PR_1000204834) —** Mirror-Port adds a VLAN tag to untagged, monitored traffic.
- **NAT (PR_1000199309) —** NAT getting lost when cable moved.
- **Other (PR_1000204617) —** Port mirroring and ACLS cause blade assert at dmaRx.c:1319.
- **Other (PR_1000208358) —** Mac-to-Host route table mismatch.
- **Other (PR_1000092011) —** Software exception at `c:356 -- in 'mHttpCtrl'`.
- **Password (PR_1000201614) —** Non-Null terminated password causes bus error crash in setup menu.
- **Rate Limiting (PR_1000201978) —** Radius rate-limiting-ingress should allow greater than 100%.
- **RMON (PR_1000011690)** — When RMON thresholds in the switch are exceeded, no trap is generated.
- **Self-Test (PR_1000200371) —** Ports are not isolated during the selftest internal loopback testing.
- **SNMP (PR_1000196170) —** Traps are not buffered before the IP stack is initialized, causing the possibility of missing some traps generated during startup.
- **SNTP (PR_1000199632) —** NTP (SNTP) version 4 broadcast ignored by switch.
- **Tst.System (PR_1000204782) —** Bus error when copying a configuration to the switch.

Release E.09.03

Problems Resolved in Release E.09.03

- **SNMP Trap (PR_1000212170) —** Switch transmits Warm and Cold Start traps with an agent address of 0.0.0.0.
- **Telnet Hang (PR_1000215388) —** When a user executes the **show configuration <*filename*>** command in a Telnet session and the file is longer than a single screen, the user's Telnet session may hang.

Release E.09.04 (Beta Only)

Problems Resolved in Release E.09.04

- **PIM (PR_1000206791)** — With PIM enabled, an IGMP "leave" received from one subscriber causes all IP multicast streams to pause and then resume.

Release E.09.05 (Beta Only)

Problems Resolved in Release E.09.05

- **CLI/STP (PR_1000214598)** — Switch does not accept the "spanning-tree 1 mode fast" CLI command. Switch does accept and implement the span tree port mode fast setting via the menu options. However, the setting does not show up in the running configuration.
- **LLDP (PR_1000213942)** — Neighbor entry is deleted and re-learned when port admin-status is changed from rxonly to tx_rx.

Release E.09.06 (Beta Only)

Problems Resolved in Release E.09.06

- **Config/Stack (PR_1000216051)** — Copying a previously saved startup-configuration that has "stack join (mac address)" to a member switch of the IP stack breaks the membership of that same stack. Stack commander reports member "mismatched".
- **Web (PR_80857)** — Java files are JDK 1.1, which are not Win2k compliant. (For this fix they were recompiled using JDK 1.2.)
- **Web UI/Port Status (PR_93721)** — The Port Status screen does not display all ports in the Web user interface, and the scroll bar does not work.

Release E.09.07 (Beta Only)

Problems Resolved in Release E.09.07

- **QoS (PR_1000216179)** — QoS DSCP is not maintained when the switch routes the packet.

Release E.09.08 (Beta Only)

Problems Resolved in Release E.09.08

- **Crash (PR_1000207542)** — The switch may crash with a bus error or a task hang.

- **Port Security (PR_1000203984)** — Switch allows a user to enter more MAC addresses than the configured limit.

Release E.09.09 (Beta Only)

Problems Resolved in Release E.09.09

- **XRRP (PR_1000217651)** — XRRP may cause excessive event log messages.

Release E.09.10 (Not a General Release)

Problems Resolved in Release E.09.10

- **OSPF/Routing (PR_1000202847)** — Asymmetrical routing with equal-cost paths results in high CPU utilization and dropped packets. NOTE: This bug fix is NOT included in E.09.21, but it is in releases E.09.22 and later.

Release E.09.21 (Beta Only)

Problems Resolved in Release E.09.21

- **CLI/GVRP (PR_1000216305)** — The GVRP command **no VLAN <*vid*> forbid <*ports*>** incorrectly deletes ports configured for AUTO mode.
- **Crash (PR_1000216170)** —The switch will crash with an 'mftTask' Bus Error after uploading a startup-configuration from a TFTP server. The switch accepts the command with no errors. However, the system will immediately crash after the reboot.
- **Crash (PR_1000021764)** —The switch may crash with a message similar to:

  ```
  Software exception in dmaRx.c:839.
  ```

- **Crash/LLDP (PR_1000217480)** —The switch may crash with a Bus error specifying "Task = mlldpCtrl".
- **Crash/SSH (PR_1000192010)** —The switch may crash with a message similar to:

  ```
  Software exception at exception.c:328 -- in 'tSsh0', task ID = 0x101c590.
  ```

- **Crash/Static Route (PR_1000217354)** —The switch may crash with a `Bus error in mSnmpCtrl` when adding a less-specific static route.
- **LLDP (PR_1000202129)** — The command **show lldp info remote** does not provide correct information.

- **LLDP/Mesh (PR_1000216041)** — Switch does not issue an Event Log message if LLDP is configured inconsistently among mesh neighbors.
- **MAC Authorization (PR_1000212868)** — MAC Authorization ages out a client prematurely when the client passes traffic in multiple VLANs.
- **Port Security (PR_1000210932)** — Open VLAN mode (Unauthorized VLAN) does not work correctly with any port-security learn-mode.
- **SSH (PR_1000207275)** — The Codenomicon test tool causes memory leaks in SSH.
- **Virus Throttling (PR_1000213532)** — The command **show conn throttled-hosts** displays hosts on ports set to notify-only.
- **Web UI (PR_1000191635)** — Port column may not be sorted correctly in all Web user interface screens.

Release E.09.22

Problems Resolved in Release E.09.22

- **CLI (PR_1000223516)** — CLI hangs when entering certain port commands such as those involving Web MAC authentication or 802.1X.
- **MDI/MDI-X (PR_1000220687)** — Switch does not report the state of MDI/MDI-X correctly for ports on the J8161A PoE module.
- **RSTP (PR_99049)** — Switch does not detect and block network topology loops on a single port. For example, the port connects to a hub that has a loop or the port connects to an inactive node via IBM 'Type 1' cable.

Release E.09.23 (Beta Only)

Problems Resolved in Release E.09.23

- **802.1s (PR_1000207608) —** After the Spanning Tree Root Bridge is negotiated the non-root ProCurve Switch continues to send out BPDUs claiming to be the Spanning Tree Root, resulting in possible instability in the STP topology. Support: This is the 'Force10/yahoo' fix, merged from the 2800.
- **Config (PR_1000215024) —** Memory leak when loading a configuration file from a TFTP server.
- **MST (PR_1000222230) —** MSTP (802.1s) sometimes fails to block a loopback connection.
- **Web UI (PR_1000214188) —** Problems with scroll bar after resizing window.

- **Web UI (PR_1000223183) —** VLANs are not displayed in QoS configuration.
- **Web (PR_1000214188) —** Problems with the scroll bar after resizing window.
- **Web (PR_1000223183) —** VLANs are not displayed in QoS configuration screen.

Release E.09.24 (Beta Only)

Problems Resolved in Release E.09.24

- **XRRP (PR_1000217922) —** XRRP router in infinite-failback mode can sometimes give up IP address control.

Release E.09.25 (Beta Only)

Problems Resolved in Release E.09.25

- **Config (PR_1000233062) —** Download of Configuration to alternate configuration not working.
- **XRRP (PR_1000217922) —** There is a small possibility that the XRRP Router will fail back to the XRRP peer even if infinite failback is enabled when running 802.1d and XRRP routers are redundantly connected to a large switch domain.

Release E.09.26 (Beta Only)

Problems Resolved in Release E.09.26

- **Config (PR_1000228888) —** The console becomes unresponsive (“hangs” or “freezes”) when attempting to issue a configuration command, and then 802.1X and Web/MAC Authentication functions in the Switch do not operate.
- **Config (PR_1000229407) —** Edge ports on a switch with MSTP are lost when the configuration is TFTPed in from a TFTP server.
- **Hang (PR_1000228888) —** The Console becomes unresponsive (“hangs” or “freezes”) when attempting to issue a configuration command, resulting in 802.1X and Web/MAC Authentication functions in the Switch ceasing to operate.
- **MSTP (PR_1000229407) —** The Switch loses the MSTP 'edge-port' configuration when the user TFTPs the configuration file from a server.

Release E.09.29 (Beta Only)

Problems Resolved in Release E.09.29

- **Crash (PR_1000229656) —** When RADIUS server is unavailable, the following message appears:

  ```
  Software Exception at exception.c:373 -- in 'tHttpd', task ID =
  0x257dda8 -> Memory system error at 0x 24ea750 - memPartFree
  ```

- **Crash (PR_1000235856) — show tech**' causes:

  ```
  Software exception at dmaRx.c:868 -> ASSERT
  ```

- **Other (PR_1000221018) —** Menu leaves proxy-ARP configured when IP routing is disabled.
- **Other (PR_94943) —** The Setup screen allows an illegal configuration (Proxy-ARP). Using the “Setup” utility, you can toggle the Proxy-ARP entry (at the bottom of the screen) even though IP routing is NOT enabled on the system.
- **Proxy ARP (PR_94943) —** Setup screen allows illegal configuration (proxy-arp).
- **Proxy ARP (PR1000221018) —** Menu leaves proxy-arp configured when routing is disabled.
- **XRRP (PR_1000217922) —** XRRP router in infinite-failback mode can sometimes give up control of its IP address.

Release E.10.02

Problems Resolved in Release E.10.02

- **CLI (PR_1000223516) —** CLI hang when performing command involving 802.1X, Web/MAC authentication or port.
- **Config (PR_1000207697) —** Loading a startup-config file fails when file declares a new VLAN as a management VLAN.
- **Config (PR_1000215370) —** Configuration file upper/lower case is not consistent. When looking and viewing file there is inconsistencies between what is shown and what can be tab completed
- **Crash (PR_1000229613) —** A secondary flash update via PCM+ causes a bus error crash.
- **Crash (PR_1000243402) —** Null semaphore usage in SSH. (The switch may crash when “exit” is issued from slot context.)

- **Crash (PR_1000233993) —** A switch crash occurs after an **snmpgetnext** on the CDP MIB. Software exception at `exception.c:373 -- memory system error`.
- **Crash (PR_1000232283) —** Multiple TFTP requests from PCM cause a switch crash "`Software exception at fileTransferTFTP.c:182 -- in 'mftTask', task ID = 0x107ee0`.
- **Crash-OSPF (PR_1000234773) —** Within a VLAN configured with an OSPF key-chain 255, any time an external device is plugged into the VLAN on the 5300xl switch configured with the key-chain, the 5300xl switch crashes with an `ifInfo task: SubSystem 0` indicator.
- **J8162A (PR_1000219468) —** No Event Log message when user reboots J8162A Access Control Module without first shutting it down.
- **LLDP (PR_1000220937) —** LLDP advertises the base MAC address when no VLAN-IP exists. LLDP advertises "127.0.0.1" as the management TLV information on a port when no IP address is configured on any VLAN that this port belongs to. It should advertise the switch's base MAC address instead.
- **LLDP (PR_1000241315) — show lldp** issues:
  - Port descriptor may be corrupted, as displayed, if > 4.
  - PortID type of MAC-address is truncated.
  - ChassisId of type network-address is shown in MAC address format.
  - Remote Management Address type ethernet is shown in IP format.
  - Inconsistent name for PortDescr in detail view and summary ("PortDesc" vs "Port-Name").
- **MST (PR_1000227432) —** Learning flag is not set when CIST port states are transitioning.
- **Other (PR_1000214324) —** J8162A Access Controller module VLAN base configuration record. Should not create an "access-controller vlan-base" command in the remote configuration file if there is no J8162A blade in the system AND no J8162A has been configured for the switch. (There are no client VLANs on the switch.)
- **Other (PR_1000085508) —** A mini-GBIC is not recognized if the J4878A is hot-swapped during boot-up.
- **Other (PR_1000221089) —** The 64-bit counters are not correct.
- **Other (PR_1000227607) —** Problem with **show fault-finder**. The table contains two extra empty IDs.
- **Other (PR_1000235094) —** With HTTP/RADIUS, a username/password box appears for every switch between the manager and operator pages. If the Web user interface for the switch management is configured login/enable with either RADIUS/local or local/RADIUS, and local username/passwords are set and are not the same as for RADIUS, then a username/

password box/prompt appears for every instance where there is a switch between an operator-level Web page (such as Status) and a manager-level Web page (such as Configuration), and the reverse.

- **PIM-DM (PR_1000235581) —** PIM DM does not always prune when Switch receives a PIM Prune message.
- **Port Security (PR_1000244293) —** Web/MAC Authentication clients do not de-authenticate immediately.
- **RMON (PR_1000240752) —** The RMON and FFI severities need correct mapping. The FFI severity levels are from low to high, whereas the RMON severity levels are mapped from high to low.
- **SFTP (PR_1000227950) —** SFTP image "puts" to a switch low on memory does not succeed. The Event log shows

  ```
  update: Disabled RMON to retrieve memory for download
  ```

  on a 5300xl switch that has ~6.7M of free memory available. The transfer does not take place and the Event log message is displayed for every attempt.
- **STP (PR_1000234771) —** The switch does not do spanning-tree fast-aging when Web-authentication changes aging for LPORT.
- **Update (PR_1000227992) —** SFTP allows an image upload of firmware for a different platform (switch model).
- **Virus Throttling (PR_1000237928) —** Add port names to the rest of the virus throttling RMON messages. Three of the existing virus throttling messages do not have the LPORT information.
- **XRRP/802.1s (PR_1000240958) —** XRRP fail-over communication issues when MSTP is also configured.

Release E.10.03

Problems Resolved in Release E.10.03

- **MAC Auth/Web Auth (PR_1000244293)** - Web and MAC authentication clients do not de-authenticate immediately.
- **Config (PR_1000246102)** - The **show config** command indicates a configuration file named "config" already exists.

Release E.10.04

Problems Resolved in Release E.10.04

- **Console/TELNET (PR_1000278912)** - The 5300xl console will lock up when connected via the console port and attempting to establish a TELNET connection into a remote switch.
- **Meshing (PR_1000218463)** - If a mesh link goes down and a redundant (xSTP) link external to the mesh goes into a forwarding state, connectivity across the mesh may be lost for a previously learned MAC address.
- **SNMP (PR_1000003378)** - SNMP switch time may drift with event log updates occurring every 1.5 hours.

Release E.10.05

Problems Resolved in Release E.10.05

- **ACL (PR_1000283338)** - The commands "show port-access mac" and "show port-access web" incorrectly display the number of clients authenticated.
- **Crash (PR_1000282444)** - When enabling OSPF MD5, the switch may crash with a message similar to:

```
Software exception at exception.c:373 -- in 'mSess1'.
```

- **mini-GBIC (PR_1000283081)** — After hot-swapping a mini-GBIC, the Link and Activity LEDs do not turn on.
- **mini-GBIC (PR_1000283082)** — Some Gigabit LX mini-GBICs may fail when the mini-GBIC switch module is hot-swapped.
- **mini-GBIC (PR_1000283084)** — When a mini-GBIC is removed from the module, the Fault and Port LEDs will continue to flash.
- **RADIUS (PR_1000285456)** — If more than one RADIUS assigned vendor specific attribute (including Port-cos, rate-limiting-ingress, or ACLs) is configured with a non-vendor specific attribute, only the first vendor specific attribute may be recognized by switch.
- **Web UI/mini-GBIC (PR_1000279145)** — When using the web user interface, the switch will not display an indication of the Gigabit 1000Base-T mini-GBIC (J8177B) from the Configuration tab "Device View".
- **XRRP (PR_1000280213)** — When configuring a XRRP instance, the following error message is logged, although the particular subnet is configured properly

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

Release E.10.06

Problems Resolved in Release E.10.06

- **RSTP (PR_1000286883)** — Slow RSTP fail-over and fall-back time.

Release E.10.07

Problems Resolved in Release E.10.07

- **802.1X (PR_1000290453)** — 802.1X stops and restarts the accounting session during re-authentication.
- **802.1X (PR_1000216987)** — An 802.1X client may age out prematurely if it communicates in multiple VLANs.
- **802.1X (PR_1000235378)** — When client based authentication was introduced in E.09.02, the port based authentication mode, which allows an unlimited number of clients per port, was inadvertantly removed
- **Crash (PR_1000290428)** — When a non-genuine mini-GBIC is installed into the switch, the switch may crash with a message similar to:

  ```
  "chassis: Slot A Software exception at port_sm.c:316 -- in
  'mPmSlvCtrl', task ID = 0x4059c9d4."
  ```

- **Web-Authentication (PR_1000230444)** — Some clients may not receive a Web-Authentication screen when using port-based Web-Authentication. This may occur if a client receives the same unauthorized DHCP address that a previous authorized client had used.

Release E.10.08

Problems Resolved in Release E.10.08

- **Enhancement (PR_1000290489)** — Support for “Friendly Port Names” was added.

Release E.10.09

Problems Resolved in Release E.10.09

- **Config (PR_1000301498)** — The user cannot manually configure an IP address using the "setup" menu.
- **FEC/CDP (PR_1000285111) —** FEC and CDP transmit removal.

- **Routing (PR_1000297773) —** Certain types of traffic cause the switch to route very slowly and drop packets.
- **RSTP (PR_1000297195)** — The switch repeatedly flushes its MAC address table, resulting in intermittent flooding of all traffic.

Release E.10.10

Problems Resolved in Release E.10.10

FEC (PR_1000281715) — Switch has no FEC support but shows FEC information in help text.

Releases E.10.11 to E.10.19 were never built.

Release E.10.20

Problems Resolved in Release E.10.20

- **Key Management System (PR_1000287934)** — Some Key Management System (KMS) configuration commands have no effect.

Release E.10.21

Release E.10.21 was never released.

Release E.10.22

Problems Resolved in Release E.10.22 (Never released)

- **Event Log (PR_1000306769)** — When an OS upgrade causes an FEC trunk to be converted, the following messages are logged:

```
[datestamp] mgr: Config file converted due to OS upgrade

W [datestamp] mgr: Unsupported feature "FEC" for trunk configuration;
see release notes
```

- **Event Log/ARP (PR_1000293466)** — Generic Link Up message not showing up and unnecessary flushing of ARP cache.
- **LLDP (PR_1000301069)** — When LLDP admin status of a port changes from TX to DIS/RX, the switch does not always send out shutdown frames.
- **LLDP (PR_1000303500)** — Missing LLDP-MED information when using command: `"show lldp info remote-devices"`.

- **Meshing (PR_1000300756)** — Time delay in switch when reporting a mesh link being down.
- **Web Authentication (PR_1000302945)** — When a client fails authentication and is assigned to the Unauthorized VLAN, it cannot communicate with other clients on the Unauthorized VLAN.

Release E.10.23

Problems Resolved in Release E.10.23

- **CLI/DHCP (PR_1000286898)** — Under some conditions, the CLI may freeze or lock up when the DHCP relay agent is configured.
- **Crash (PR_1000307280)** — Inconsistent or incorrect STP data may cause the switch to crash with a message similar to:

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

- **IGMP (PR_1000301557)** — Data-driven IGMP does not prevent flooding when no IP address exists on a VLAN.
- **SNMP (PR_1000295753)** — Removing 'public' SNMP community generates an empty Event Log message.
- **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.
- **RSTP (PR_1000306227)** — RSTP TCNs cause high CPU utilization and slow software based routing.

Release E.10.24

Problems Resolved in Release E.10.24 (Never released)

Config (PR_1000238543) — The "Named Source-Port Filter" command would accept names up to 30 characters long, but the CLI could only display 20 characters. Name length limit is now changed to 20 characters.

Enhancement (PR_1000292455) — Rate display for ports on CLI. See description under "Release E.10.24 Enhancements" on page 12.

IDM (PR_1000310201) — The Switch fails to de-authenticate an 802.1X client after a corrupted configuration file is received from a RADIUS server.

Mini-GBIC (PR_1000308653) — On ProCurve Switch xl 16-port 10/100/1000 Module (J4907A), a dual-personality port will stop working after a mini-GBIC is hot-swapped out.

RSTP (PR_1000309683) — Temporary routing or switching problems may occur after RSTP is disabled.

Release E.10.25

Problems Resolved in Release E.10.25 (Never released)

Connection Rate Filter (PR_1000310834) — Memory leak found during ProCurve stress testing. A user may see a switch reboot or halt if using the CRF traps and runs the switch for a sufficiently long time between reboots.

Release E.10.26

Problems Resolved in Release E.10.26 (Never released)

- **SNMP Traps (PR_1000285195)** — Switch does not save the option to disable a "Link up/down" SNMP trap after a switch reboot.

Release E.10.27

Problems Resolved in Release E.10.27

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

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

- **LLDP (PR_1000310666)** — The command "show LLDP" does not display information learned from CDPv2 packets.

- **MSTP Enhancement (PR_1000317990)** — Implemented new CLI commands, "span legacy-mode" and "span legacy-path-cost".

- **RSTP (PR_1000307278)** — Replacing an 802.1D bridge device with an end node (non-STP device) on the same Switch port, can result in the RSTP Switch sending TCNs.

- **Web UI (PR_1000305944)** — The Port Configuration screen display is blank due to a Java error when using Windows Explorer 6.0.

- **Web UI (PR_1000311917)** — When the last port on the last card is configured in a trunk or mesh, and a user browses to a specific location in the Web user interface, the HTTP web server degrades the switch, causing the Web user interface to hang.

Releases E.10.28 and E.10.29 were never built.

Release E.10.30

Problems Resolved in Release E.10.30 (Not a general released)

- **Enhancement** — Added support for J9001A module.

Release E.10.31

Problems Resolved in Release E.10.31 (Not a general released)

- **Enhancement (PR_1000306695)** - Added show tech command, "show tech transceivers" to allow removable transceiver serial numbers to be read without removal of the transceivers from the switch. This command also reports failed transceiver numbers and the reasons for the failure.
- **Help Menu (PR_1000317711)** - In the VLAN menu Help text, the word 'default' is misspelled.
- **SNMP (PR_1000310841)** - User can assign illegal values for CosDSCPPolicy through SNMP. All other user-interfaces for configuring QoS (CLI, Web UI, ProCurve Manager and Radius) function correctly.
- **SNMP (PR_1000315054)** - SNMP security violations appear in syslog after a valid SNMPv3 "get" operation.
- **System (PR_1000318026)** - After a reboot, the Switch may provide a false error message that a module is unsupported or may be faulty.

Release E.10.32

Problems Resolved in Release E.10.32 (Never released)

- **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 for all DHCP requests received from various VLANs. For details, see "DHCP Option 82: Using the Management VLAN IP Address for the Remote ID" on page 14
- **Enhancement (PR_1000287679) —** Fast Boot CLI & SNMP Implementation. For details see "Using Fastboot To Reduce Boot Time" on page 14.
- **ICMP (PR_1000235905)** — Switch does not send a 'destination unreachable' response message when trying to access an invalid UDP port.
- **Menu (PR_1000318531)** — When using the 'Menu' interface, the Switch hostname may be displayed incorrectly.

Release E.10.33

Problems Resolved in Release E.10.33 (Never released)

- **Counters (PR_1000321097)** — Drop counters are displaying incorrect information.
- **Counters (PR_1000321476)** — SNMP counter may display incorrect information.
- **Enhancement (PR_1000330704)** — Added RADIUS Command Authorization and Accounting for the Command Line Interface.

Release E.10.34

Problems Resolved in Release E.10.34 (Not a general release)

- **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.
  ```

- **Module Fault (PR_1000331147)** — Switch modules J9001A (Switch xl Wireless EDGE Services Module) and J8162A (Switch xl Access Controller Module) will fault if Fast Boot is enabled and the log will report the following Major event:

  "HPESP: Access Controller XL Module x: incompatible BIOS version".

Release E.10.35

Problems Resolved in Release E.10.35 (Not a general release)

- **Event Log (PR_1000323203)** — MD5 hash mismatch log messages are triggered with VLAN toggles: "OSPF Drop pkt from:xxx.xxx.xxx.xxx md5-key-id:1 reason: md5 hash mismatch".
- **IDM (PR_1000334365)** — Using EAP/802.1x with IDM ACLs can result in memory leaks.
- **OSPF (PR_1000323201)** — OSPF does not always redistribute connected networks when MD5 authentication is enabled and connected subnets or VLANs are toggled.
- **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 E.10.36

Problems Resolved in Release E.10.36 (not a general release)

- **CLI (PR_1000322029)** — The command "show vlans" does not display data correctly in the status field.
- **Config/Security (PR_1000334412)** — Operator level can save Manager privilege level changes to the configuration.
- **Log (PR_1000323790)** — The switch detects a non-genuine ProCurve mini-GBIC as a port self test failure and subsequently disables the link.
- **sFlow Enhancement (PR_1000337714)** — Added new "show sflow" commands to the CLI. For details, see “SFlow Show Commands” on page 17.
- **Web UI (PR_1000331431)** — The QoS Configuration Tab is not working correctly when using the Web User Interface.

Release E.10.37

Problems Resolved in Release E.10.37

- **CLI (PR_1000330553)** — Garbage characters displayed in "show snmp-server" cli output.
- **Menu (PR_1000308364)** — In the Menu's Switch Configuration->System Information screen, the “SNTP Poll Interval” field is missing the poll interval descriptor.
- **STP/RSTP/MSTP (PR_1000330532)** — Improved the "show" commands display of STP ports detail information to assist in monitoring and troubleshooting the spanning tree protocol. See “Spanning Tree Show Commands” on page 20 for details.

Release E.10.38

Problems Resolved in Release E.10.38 (not a general release)

- **Enhancement (PR_1000338847)** — Added support for the Advanced Encryption Standard (AES) privacy protocol for SNMPv3.

Release E.10.39

Problems Resolved in Release E.10.39 (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/PCM (PR_1000343949)** — ProCurve Manager fails to map the wireless services module correctly, thus preventing access to telnet or the CLI for managing the device.
- **DHCP (PR_1000343149)** — A client cannot obtain an IP address when two DHCP servers are connected on different local networks.

Release E.10.40

Problems Resolved in Release E.10.40 (Never released)

- **CLI (PR_1000347788)** — The wrong error message is displayed in response to a non-authorized CLI command
- **Crash (PR_1000339551)** — When using the Menu to disable IP routing, the Switch may crash with a message similar to:

```
Bus Error in task 'msess1'. PPC Bus Error exception vector 0x300:
Stack-frame=0x0162e030 HW Addr=0x2e2e2e2d IP=0x00166b7c
Task='mSess2' Task ID=0x162e2c8
```

- **Crash (PR_1000348454)** — The switch may reboot with an NMI event when a loop is formed on the network. The crash task may vary by switch configuration.
- **Crash (PR_1000337443)** — Loading a config file larger then 64k via TFTP server crashes the switch with a message similar to:

```
Software exception in ISR at dmaRx.c:868 -> ASSERT: No resources
available!
```

- **Enhancement (PR_1000323618)** — If SCP or SFTP are enabled, TFTP is automatically disabled. TFTP cannot be enabled if either SCP or SFTP are enabled.

Release E.10.41

Problems Resolved in Release E.10.41 (Never released)

- **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 E.10.42

Problems Resolved in Release E.10.42 (Not a general release)

- **CLI (PR_1000344362)** — The CLI help text was updated in the areas of "ip igmp auto, forward and blocked"
- **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_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **Enhancement (PR_1000354170)** — 802.1X Controlled Directions enhancement. With this change, users will be able to use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.
- **SNMP (PR_1000312285)** — The old value of the SNMP LLDP-MED trap (lldpXMedRemDeviceClass) is supported.

Release E.10.43

Problems Resolved in Release E.10.43 (Not a general release)

- **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.
- **QoS (PR_1000304105)** — The maximum QoS rules limit is incorrect, internal to the switch.
- **UDLD (PR_1000355632)** — If the maximum number of source port filters (78) is allocated and UDLD is turned on, then it is possible that the last allocated source port filter may not work correctly, and/or UDLD may forward UDLD protocol packets to the wrong port.

Release E.10.44

Problems Resolved in Release E.10.44

- **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_1000360929)** — DHCP Protection enhancement for switch 5300xl.
- **LLDP (PR_1000308878)** — The CLI output for "show LLDP info remote <port>" is not displaying the correct format for the Chassis ID and Management Address.

Release E.10.45

Problems Resolved in Release E.10.45 (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_1000359913)** — When "aaa authorization commands radius" is configured, and a user tries to execute a command for which that user is not authorized, the following inaccurate error message is shown.

  ```
  Disable dhcp option 82 management option before disabling management
  vlan.
  ```

- **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
  ```

Release E.10.46

Problems Resolved in Release E.10.46 (Not a general release)

- **CLI (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.

- **Enhancement (PR_1000346164)** — RSTP/MSTP BPDU Protection enhancement. When this feature is enabled on a port and that port receives a spanning tree BPDU, the switch will disable (drop link) the port, log a message, and optionally, send an SNMP TRAP.
- **Enhancement (PR_1000365862)** — Addition to the RSTP/MSTP BPDU Protection enhancement. This portion of the enhancement added the option of configuring ports that had been previously disabled by BPDU Protection to be automatically re-enabled.

Release E.10.47

Problems Resolved in Release E.10.47 (Not a general release)

- **Crash (PR_1000368540)** — The switch may crash with a message similar to:

```
Software exception at parser.c:8012 -- in 'mSess2',
task ID = 0x90e10e0 -> ASSERT: failed.
```

- **Crash (PR_1000371265)** — A mini-GBIC hot swap on the J4878B module may crash the switch with a message similar to:

```
Software exception at buffers.c:2198 -- in 'mPpmgrCtrl'.
```

- **Hang (PR_1000368539)** — When Connection Rate Filtering is enabled, the switch may hang or become unresponsive under heavy virus load.
- **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.
- **XRRP (PR_1000368594)** — When XRRP infinite failback is enabled, the switch fails to forward packets after a reboot of the Master.

Release E.10.48

Problems Resolved in Release E.10.48 (Never released)

BPDU Protection (PR_1000374748) — This fix prevents the BPDU Protection enhancement from enabling a port if Loop Protection still has that port disabled.

Enhancement (PR_1000376406) — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.

Enhancement (PR_1000379804) — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

Release E.10.49

Problems Resolved in Release E.10.49 (Never released)

- **Enhancement (PR_1000336169)** — Added support for STP Per Port BPDU Filtering and related SNMP Traps.

Release E.10.50

Problems Resolved in Release E.10.50 (Never released)

- **CLI (PR_1000292887)** — The CLI command "aaa port-access web-based <port-list> redirect-url" accepts only the first 103 characters of the maximum allowed value of 127 characters.
- **CLI (PR_1000364628)** — The command output from "show ip rip peer" yields an improperly formatted peer IP address.
- **Enhancement (PR_1000335860)** — This enhancement provides a configuration option for the source IP address field of SNMP response and SNMP trap PDUs.
- **Web/RADIUS (PR_1000368520)** — Web Authentication doesn't authenticate clients due to a failure to send RADIUS requests to the configured server.

Release E.10.51

Problems Resolved in Release E.10.51 (Not a general release)

- **Enhancement (PR_1000385565)** — Port security static MAC address limit increased to 32.
- **SNMP (PR_1000388175)** — SNMP PDU configuration CLI commands are not working on 5300xl platform.

Release E.10.52

Problems Resolved in Release E.10.52

- **Enhancement (PR_1000374085)** — This enhancement expands the use of the Controlled Directions parameter to also support mac/web authentication.
- **MSTP (PR_1000385573)** — MSTP instability issue when root switch priority is changed. This causes other switches with better priority to each assert themselves to be root thus causing a root war to occur.
- **OSPF/ECMP (PR_1000377365)** — The switch does not support ECMP of type 5 External LSAs.

Release E.10.53

Problems Resolved in Release E.10.53 (never released)**.**

- **CLI/LLDP (PR_1000377191)** - Output from the CLI command, "show lldp info remote-device <port>" shows a blank field for the chassis ID.
- **CLI (PR_1000390042)** - Corrupted Spanning Tree Status/Configuration Menu screens
- **CLI (PR_1000380660)** - The "show tech transceivers" CLI command displays the wrong message when inserting an "A" version transceiver into a switch that only supports "B" version transceivers. Also, "B" version CX4 transceivers show up as "A" and "A" version SR, LR, and ER transceivers show up as "B" versions.
- **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:

  ```
  CCCCCline: 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_1000332725)** - ICMP rate limiting messages refer to ports as a port number rather than the slot/port numbers.
- **CLI (PR_1000390385)** - The CLI help text for "span bpdu-protection-timeout" is incorrect; it erroneously displays the help text for "span hello-time".
- **CLI/Config (PR_1000377413)** - The CLI does not prevent an invalid configuration from being loaded. With this fix, configurations with excess IP Address QoS entries will result in an error message and the config file will not load.
- **Crash (PR_1000382962)** - Executing the CLI command, "sho int" on a miniGBIC that isn't linked, may cause the switch to crash with a message similar to:

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

- **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
  ```

- **Enhancement (PR_1000376626)** — Enhanced CLI "qos dscp-map he" help and "show dscp-map" text to warn user that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.
- **Traceroute (PR_1000379199)** - The reported "traceroute" time is inaccurate; it is one decimal place off.
- **Trunking (PR_1000238829)** - Trunks numbered trk10 and greater cause the output from the CLI command "show span" output to be misaligned.
- **SNMP (PR_1000392847)** — RMON alarms that monitor port-specific OIDs are lost if the switch is rebooted.

Release E.10.54

Version E.10.54 software was never released.

Release E.10.55

Problems Resolved in Release E.10.55.

- **CLI (PR_1000395256)** — The "loop-protect PORT-LIST receiver-action <action>" command does not enable the ports as it should.
- **CLI (PR_1000240838)** — If an invalid time is entered using "clock set" command, the switch responds with an "invalid date" error.
- **CLI (PR_1000199785)** — The tab help function (command-completion) for "IP RIP authentication" is inaccurate. The help selection lists "OCTET-STR Set authentication key" when it should be "ASCII-STR Set RIP auhentication key (maximum 16 characters)".
- **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.
- **RIP (PR_1000393366)** — The switch does not process RIP (v2) responses containing subnets with a classful subnet mask, when the receiving RIP switch has a connected VLSM network defined that would fall within that classful range.
- **sFlow (PR_1000396889)** — If the Sflow skip count is set greater than the maximum skip count or less than minimum skip count, the switch returns an error, which prevents ProCurve Manager from collecting traffic sampling data.
- **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.

Release E.10.56

Problems Resolved in Release E.10.56 (never released)**.**

- **CLI (PR_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.
- **RSTP (PR_1000401394)** — When a dynamic LACP trunk transitions to either link-up or link-down, this action occasionally triggers RSTP instability within the switch. This can result in loops and broadcast storms.

Release E.10.57

Problems Resolved in Release E.10.57 (Not a general release)

- **Crash (PR_1000407542)** — Attempting to change the spanning-tree protocol version from STP to RSTP or MSTP may cause the switch to crash with a message similar to:

```
PPC Bus Error exception vector 0x300: Stack-frame=0x063d5de0
HW Addr=0x4b5a697c IP=0x0064c648 Task='mSnmpCtrl'
```

Releases E.10.58 and E.10.59 (Never built)

Releases E.10.58 and E.10.59 were never built.

Release E.10.60

Problems Resolved in Release E.10.60 (Not a general release)

- **QoS (PR_1000357102)** — QoS configuration allows invalid IP addresses.

Release E.10.61

Problems Resolved in Release E.10.61

- **BPDU Protection (PR_1000395569)** — BPDU-protection fails after module hot-swap.
- **Crash (PR_1000410959)** — If the snmpv3 user is deleted on the switch without deleting the associated parameters, then the switch is rebooted, it will repeatedly crash with a message similar to:

```
Software exception at exception.c:373 -- in 'mSnmpEvt',
task ID = 0x17d1818 -> Memory system error at
0x17c22e0 - memPartFree
```

- **Hotswap (PR_1000412501)** — Some modules fail to initialize following hotswap, but have no trouble initializing with warm or cold boot.

Release E.10.62

Problems Resolved in Release E.10.62.

- **IP Connectivity (PR_1000418378)** — The switch incorrectly updates its ARP table when a client that is configured with a valid IP address for a valid VLAN is connected to a port in another VLAN on the switch. This will result in the loss of connectivity for the valid client in the appropriate VLAN.
- **Crash (PR_1000421322)** — Following execution of config-related CLI commands (such as "show run" or "show tech") or when PCM attempts to retrieve the configuration file via TFTP from a switch having a large configuration file, the switch may crash with a message similar to:

  ```
  Software exception at exception.c:373 -- in 'tTftpDmn', task ID =
  0x11cfaa8 -> Memory system error at 0x1175550 - memPartFree
  ```

  The following related crash may also be addressed with this fix:

  ```
  PPC Bus Error exception vector 0x300: Stack-frame=0x016778b0 HW
  Addr=0x667c4c88 IP=0x004dbc88 Task='eChassMgr' Task ID=0x1677dd8 fp:
  0x667c4c88 sp:0x01677970 lrecpgyp
  ```

- **RSTP (PR_1000405368)** — When a primary link goes down and then comes back online, traffic continues on the redundant link and does not shift back to the primary link.

Release E.10.63

Problems Resolved in Release E.10.63 (never released)**.**

- **TFTP (PR_1000426821)** — TFTP transfers do not work when there is not an IP address configured for VLAN 1.
- **ROM Patcher (PR_1000422768)** — The ROM was updated from version E.05.04 to version E.05.05 to support product software greater than 4MB in size.

Release E.10.64

Problems Resolved in Release E.10.64 (never released)**.**

- **Crash (PR_1000430860)** — The switch may crash with a message similar to:

```
Software exception at termio.c:575 -- in 'mSesInp3', task ID =
0x111f1d8\n-> ASSERT: failed\n", pRegs=0x850000) at exception.c:212
```

- **Enhancement (PR_1000340292)** — Flash file system compaction improvements were completed.
- **Crash (PR_1000432587)** — When the J8162A and/or J9100A modules are present, the switch may crash with a message similar to:

```
NMI event SW:IP=0x00508d40 MSR:0x0000b032 LR:0x00508d40 Task='eChas-
sMgr' Task ID=0x1771eb8 cr: 0x42000042 sp:0x01771c38 xer:0x00000000
```

- **Enhancement (PR_1000433763)** — The Dynamic ARP Protection feature was added.

Release E.10.65

Problems Resolved in Release E.10.65 (never released)**.**

- **RMON (PR_1000424204)** — The ProCurve Manager RMON manager is failing to create alarms.

Release E.10.66

Problems Resolved in Release E.10.66.

- **Web UI (PR_1000414459)** — During configuration of the GVRP Mode via the Web interface (Configuration -> VLAN Configuration -> GVRP Mode), the port list does not show the last three port entries.

Release E.10.67

Problems Resolved in Release E.10.67.

- **ARP Protection (PR_1000438129)** — ARP and ARP protection data may not display correctly following a CLI or SNMP status query.
- **802.1X (PR_1000446227)** — Switch 802.1X authentication running over PAP does not work if RADIUS message authenticator attribute is required. This fix adds the message authenticator attribute to non-EAP RADIUS responses.

Part Number 5991-2127
August, 2007