Release Notes:
Version H.08.72 Software
for the ProCurve Series 2600, 2600-PWR Switches

"H" software versions are supported on these switches:

ProCurve Switch	H.07.5x	H.08.5x and newer
ProCurve Switch 2626 (J4900A)	✔	✔
ProCurve Switch 2626 (J4900B		✔
ProCurve Switch 2650 (J4899A)	✔	✔
ProCurve Switch 2650 (J4899B)		✔
ProCurve Switch 2626-PWR (J8164A)	✔	✔
ProCurve Switch 2650-PWR (J8165A)	✔	✔
ProCurve Switch 6108 (J4902A)	✔	

These release notes include information on the following:

- Downloading switch software and Documentation from the Web (page 1)
- Clarification of operating details for certain software features (page 8)
- Software Enhancements (page 11)
- A listing of software fixes included in releases H.07.02 through H.08.72 (page 36)

Caution: Startup-Config File Compatibility, Pre-H-08.5*x* Software

New features in release H.08.5*x* (or greater) do not exist in H.07.*xx* software. As a result, the startup-config file is NOT backward-compatible. Users are advised to save a copy of the pre-H.08.5*x* startup-config file, should you need to run H.07.*xx* software. See "Transferring Switch Configurations" in Appendix A of the *Management and Configuration Guide.*

Caution: Startup-Config File Compatibility, Pre-H-07.31 Software

The startup-config file saved under version H.07.31 or greater, is NOT backward-compatible with previous software versions. Users are advised to save a copy of the pre-H.07.31 startup-config file BEFORE UPGRADING to H.07.31 or greater, in case there is a need to revert to pre-H.07.31 software. Instructions are available in the "Transferring Switch Configurations" section of Appendix A in the *Management and Configuration Guide* (included in PDF format on the Product Documentation CD-ROM) shipped with the switch, and also available on the ProCurve Networking Web site. (Refer to "To Download Product Documentation:" on page 1.)

Publication Number

5990-6003
August, 2005

Applicable Products

ProCurve Switch 2626	(J4900A)
ProCurve Switch 2626	(J4900B)
ProCurve Switch 2650	(J4899A)
ProCurve Switch 2650	(J4899B)
ProCurve Switch 2626-PWR	(J8164A)
ProCurve Switch 2650-PWR	(J8165A)

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 HP 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 HP 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, vistit

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)

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

Contents

(This page is intentionally unused)

Software Management

Downloading Switch Documentation and Software from the Web

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

To Download a Software Version:

1. Go to theProCurve 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. (HP recommends version 5.0 or greater.)

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

Downloading Software to the Switch

Caution

The startup-config file generated by the latest software release may not be backward-compatible with the same file generated in your switch by earlier software releases. Refer to the "Caution: Startup-Config File Compatibility, Pre-H-07.31 Software" 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 the software 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).
- A switch-to-switch file transfer

Note

Downloading a new software version 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 and running the same software version.

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 **H_08_xx.swi** from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
HPswitch # copy tftp flash 10.28.227.103  H_08_xx.swi
Device will be rebooted, do you want to continue [y/n]?  y
00224K _
```

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

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

Figure 1. Message Indicating the Switch Is Writing the Downloaded Software to Flash Memory

3. After the switch writes the downloaded software to flash memory, you will see this screen:

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

System software written to FLASH.

You will need to reboot to activate.

<Press any key to continue>
```

Indicates that switch is ready for rebooting to activate the downloaded software.

Figure 2. Message Indicating the Switch Is Ready To Activate the Downloaded Software

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.

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** dropdown 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, use this command:

   ```
   HPswitch(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:

   ```
   HPswitch(config)# copy xmodem flash pc
   Device will be rebooted, do you want to 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.

   When the download finishes, the switch automatically reboots itself and begins running the new software version.

4. Use this command to confirm that the software downloaded correctly:

   ```
   HPswitch> show system
   ```

   (Check the **Firmware revision** line to verify that the switch downloaded the new software.)

```
HPswitch# show system

Status and Counters - General System Information

 System Name        : HPswitch
 System Contact     :
 System Location    :

 MAC Age Time (sec) : 300

 Time Zone          : 0
 Daylight Time Rule : None


 Firmware revision  : H.08.72          Base MAC Addr      : 000a57-cee840
 ROM Version        : H.08.02          Serial Number      : XX43783211

 Up Time            : 3 mins           Memory   - Total   : 19,964,696
 CPU Util (%)       : 9                           Free    : 16,275,576

 IP Mgmt  - Pkts Rx : 0                Packet   - Total   : 1998
            Pkts Tx : 279              Buffers    Free    : 1941
                                                  Lowest  : 1931
```

Firmware Revision

Figure 3. Example of Using the CLI 'show system' Command to Verify the Software Revision

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

   (Remember to return your terminal emulator to the same baud rate as the switch.)

Saving Configurations While Using the CLI

The switch operates with two configuration files:

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

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

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

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

ProCurve Switch Software Key

Software Letter	ProCurve Switch, Routing Switch, or Router
C	1600M, 2400M, 2424M, 4000M, and 8000M
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.07.50 and Earlier • H.08.55 and Greater
H	Switch 6108: H.07.xx and Earlier
I	Switch 2800 Series (2824 and 2848)
J	Secure Router 7000dl Series (7102dl and 7203dl)

Software Letter	ProCurve Switch, Routing Switch, or Router
M	Switch 3400cl Series (3400-24G and 3400-48G) and Series 6400cl (CX4 6400cl-6XG and X2 6400cl-6XG)
N/A	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 2600 Features

For Software Features. To view a tabular listing of major switch software features and the minimum software version each feature requires:

1. Visit the ProCurve Networking Web site at **http://www.procurve.com**.
2. Click on **Software updates**.
3. Click on **Minimum Software Version Required by Feature**.

If you are viewing this publication online, just click on the underlined text in step 3 to go directly to the " ProCurve Networking software updates" page. Click on **Minimum Software Version Required by Feature**.

For Series 2600 Switches and the Switch 6108 Hardware.

ProCurve Device	Minimum Supported Software Version
Switch 2626 (J4900A)	H.07.31
Switch 2626 (J4900B)	H.08.53
Switch 2650 (J4899A)	H.07.02
Switch 2650 (J4899B)	H.08.53
Switch 2626-PWR (J8164A)	H.07.41
Switch 2650-PWR (J8165A)	H.07.41

Clarifications

Port Monitoring

The following information updates and clarifies information in Appendix B, “Monitoring and Analyzing Switch Operation” in the *Management and Configuration Guide*—part number 5990-6023, October 2004 edition. Please refer to the section on "Port and Static Trunk Monitoring Features" for detailed information.

All 2600 Series models will support inbound (ingress) and outbound (egress) port monitoring with Version H.08.xx software; however, the 2650 and 2650-PWR require that the “mirror port” be within the same grouping as the monitored ports. On the 2650/2650-PWR switches, ports are grouped as follows: 1-24 + 49, and 25-48 + 50. These groupings represent the connections of ports to NetSwitch ASICs within the models.

OS/Web Browser/Java Compatibility Table

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

Operating System	Internet Explorer	Netscape Navigator	Java
Windows 2003 Server6 Windows 2000 SP4 Windows XP Professional XP SP1a	6.0, SP1	7.01	Sun Java 2 Runtime Environment, Ver. 1.4.2_03

IGMP

Note: the following information updates and clarifies information in Chapter 4, “Multimedia Traffic Control with IP Multicast (IGMP)” in the *Advanced Traffic Management Guide*—part number 5990-8853, October 2004. Please review this chapter for a detailed explanation of IGMP operation.

Supported Standards and RFCs

The following are supported:

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

The switch provides full IGMPv2 support as well as full support for IGMPv1 Joins. The switch is interoperable with IGMPv3 Joins as it forwards packets for the joined group from all sources. It does not support IGMPv3 “Exclude Source” or “Include Source” options in the Join Reports. The switch can operate in IGMPv2 Querier mode on VLANs with an IP address.

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

Using Delayed Group Flush

This feature continues to filter IGMP-Left groups for a specified additional period of time. This is beneficial in switches such as the Series 2600 or 4100gl, where Data-Driven IGMP is not supported. The delay in flushing the group filter prevents stale traffic from being forwarded by the server. Delayed Group Flush is enabled or disabled for the entire switch.

HP recommends that Delayed Group Flush be used whenever Fast Leave or Forced Fast Leave are enabled on the Series 2600 and 2600-PWR Switches. Note that this command must be executed in the configuration context.

Syntax: igmp delayedflush <*time period*>

Enables the switch to continue to flush IGMP-Left groups for a specified period of time (0 - 255 seconds). The default setting is **Disabled**. *To disable, reset the time period to zero.*

Syntax: Show igmp delayedflush

Displays the current setting for the switch.

Setting Fast-Leave and Forced Fast-Leave from the CLI

In previous software versions, Fast-Leave and Forced Fast-Leave options for a port were set through the MIB. The following commands now allow a port to be configured for Fast-Leave or Forced Fast-leave operation from the CLI. Note that these command must be executed in a VLAN context

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

Enables IGMP Fast-Leaves on the specified ports in the VLAN (the default setting). In the Config context, use the VLAN specifier, for example, **vlan <** *vid* **> ip igmp fastleave <***port-list***>**. *The "no" form disables Fast-Leave on the specified ports.*

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

Forces IGMP Fast-Leaves on the specified ports in the VLAN, even if they are cascaded.

To view the IGMP Fast-Leave status of a port use the **show running-config** or **show configuration** commands.

IGMP Operating Notes

- Use Delayed Group Flush on the Series 2600 and 2600-PWR Switches whenever Fast Leave or Forced Fast Leave are set on a port.
- Forced fast leave can be used when there are multiple devices attached to a port.

sFlow Support Clarification

The Series 2600 and 2600-PWR switches do not support sFlow.

IP Routing Interfaces

The Series 2600 and 2600-PWR Switches support a total of 32 routing interfaces (an IP address and a subnet mask). While the switch allows more than 32 IP interfaces to be created, for example, you could create 40 VLANs, each with its own IP address (for a total of 40 routing interfaces), only the first 32 of those interfaces are used for routing. The remaining 8 addresses can only be used to telnet to the switch from their respective VLANs.

Displaying Spanning Tree Configuration Detail

A new CLI command has been added to provide more detailed statistics on spanning tree operation.

Syntax: show spanning-tree <*port-list*> detail

Lists 802.1D and 802.1w port operating statistics for all ports, or those specified.

Enhancements

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

Release H.08.70 through Release H.08.72 Enhancements

Software fixes only; no new enhancements.

Release H.08.69Enhancements

IP Lockdown

Beginning with release H.08.69 you can use the “IP lockdown” utility to restrict incoming traffic on a port to a specific IP address/subnet, and deny all other traffic on that port for the HP Procurve Switch 2600 and 2800 series.

Operating Rules for IP Lockdown

- Users cannot specify that certain subnets be denied while others are permitted.
- Users cannot filter on protocol or destination IP address.
- The lockdown feature applies to inbound traffic on a port only.
- There is no logging functionality for this feature, i.e. no way to determine if IP address violations occur..
- The same subnet mask must be used for all ports within an 8 port block (1-8, 7-16, etc), for example:
  - If you configure Port 1 with: `ip-lockdown 192.168.0.1/24`
  - Then configure Port 2 with: `ip-lockdown 50.0.0.0/24`
    This is an acceptable subnet for port 2
  - Then configure Port 3 with: `ip-lockdown 120.15.32.7/32`
    This command would return an error and not be configured due to the differing subnet mask.

Using the IP Lockdown Command

The IP lockdown command operates as follows:

Syntax: ip-lockdown <*subnet mask/ips* >

Defines the subnet and related IP addresses allowed for incoming traffic on the port.

The following example will prevent traffic from all IP addresses other than those specified in subnet 192.168.0.1/24 from entering the switch on interface 1.

HP Procurve Switch 2626 (config) # `interface 1`

HP Procurve Switch 2626 (eth-1) # `ip-lockdown 192.168.0.1/24`

HP Procurve Switch 2626 (eth-1) # `exit`

Release H.08.66 through Release H.08.67 Enhancements

Software fixes only; no new enhancements.

Release H.08.65 Enhancements

Named Source-Port Filters

This discussion assumes that you are familiar with source-port filters, as described in the chapter titled “Traffic/Security Filters” in the Access Security Guide for your switch.

Beginning with software release H.08.65 you can specify named source-port filters that may be used on multiple ports and port trunks. As before, a port or port trunk can only have one source-port filter, but by using this new capability you can define a source-port filter once and apply it to multiple ports and port trunks. This can make it easier to configure and manage source-port filters on your switch. The commands to define, configure, apply, and display the status of named source-port filters are described below.

Operating Rules for Named Source-Port Filters

- A port or port trunk may only have one source-port filter, named or not named.
- A named source-port filter can be applied to multiple ports or port trunks.
- Once a named source-port filter is defined, subsequent changes only modify its action, they don’t replace it.
- To change the named source-port filter used on a port or port trunk, the current filter must first be removed, using the **no filter source-port named-filter <filter-name >** command.
- A named source-port filter can only be deleted when it is not applied to any ports.

Defining and Configuring Named Source-Port Filters

The named source-port filter command operates from the global configuration level.

Syntax: [no] filter source-port named-filter <*filter-name*>

Defines or deletes a named source-port filter. The *filter-name* may contain a maximum of 20 alpha-numeric characters (longer names may be specified, but they are not displayed). A *filter-name* cannot be a valid port or port trunk name.

The maximum number of named source-port filters that can be used is equal to the number of ports on a switch.

A named source-port filter can only be removed if it is not in use (use the **show filter source-port** command to check the status). Named source-port filters are not automatically deleted when they are no longer used.

Use the **no** option to delete an unused named source-port filter.

Syntax*:* filter source-port named-filter <*filter-name* > drop < *destination-port-list* >

Configures the named source-port filter to drop traffic having a destination on the ports and/or port trunks in the < *destination-port-list* >. Can be followed by the **forward** option if you have other destination ports or port trunks previously set to **drop** that you want to change to **forward**. For example:

filter source-port named-filter <*filter-name* > drop < *destination-port-list* > forward < *destination-port-list*>

The ***destination-port-list*** may contain ports, port trunks, and ranges (for example 3-7 or trk4-trk9) separated by commas.

Syntax: filter source-port named-filter <*filter-name* > forward < *destination-port-list* >

Configures the named source-port filter to forward traffic having a destination on the ports and/or port trunks in the < ***destination-port-list*** >. Since "forward" is the default state for destinations in a filter, this command is useful when destinations in an existing filter are configured for "drop" and you want to change them to "forward". Can be followed by the **drop** option if you have other destination ports set to **forward** that you want to change to **drop**. For example:

filter source-port named-filter <*filter-name* > forward < *destination-port-list* > drop < *destination-port-list* >

A named source-port filter must first be defined and configured before it can be applied. In the following example two named source-port filters are defined, **web-only** and **accounting**.

```
HPswitch(config)# filter source-port named-filter web-only
HPswitch(config)# filter source-port named-filter accounting
```

By default, these two named source-port filters forward traffic to all ports and port trunks.

To configure a named source-port filter to prevent inbound traffic from being forwarded to specific destination switch ports or port trunks, the **drop** option is used. For example, on a 26-port switch, to configure the named source-port filter **web-only** to drop any traffic except that for destination ports 1 and 2, the following command would be used:

```
HPswitch(config)# filter source-port named-filter web-only drop 3-26
```

A named source-port filter can be defined and configured in a single command by adding the **drop** option, followed by the required destination-port-list.

Viewing a Named Source-Port Filter

You can list all source-port filters configured in the switch, both named and unnamed, and their action using the **show** command below.

Syntax: show filter source-port

Displays a listing of configured source-port filters, where each filter entry includes a Filter Name, Port List, and Action:

Filter Name: The *filter-name* used when a named source-port filter is defined. Non-named source-port filters are automatically assigned the port or port trunk number of the source port.

Port List: Lists the port and port trunk destinations using the filter. Named source-port filters that are not in use display **NOT USED**.

Action: Lists the ports and port trunks dropped by the filter. If a named source-port filter has been defined but not configured, this field is blank.

[*index*] For the supplied index (IDX) displays the action taken (Drop or Forward) for each destination port on the switch.

Using Named Source-Port Filters

A company wants to manage traffic to the Internet and its accounting server on a 26-port switch. Their network is pictured in Figure 1. Switch port 1 connects to a router that provides connectivity to a WAN and the Internet. Switch port 7 connects to the accounting server. Two workstations in accounting are connected to switch ports 10 and 11.

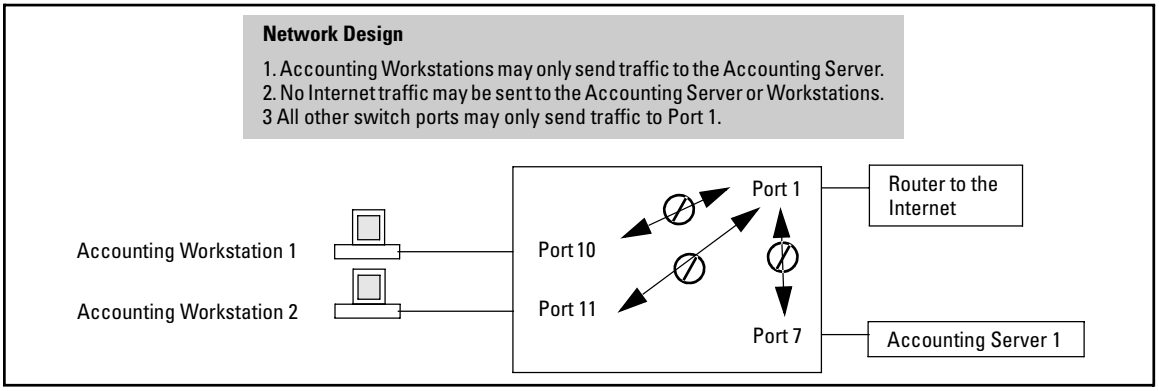

Figure 1. Network Configuration for Named Source-Port Filters Example

The company wants to use named source-port filters to direct inbound traffic only to the Internet while allowing only the two accounting workstations and the accounting server to communicate with each other, and not the Internet.

Defining and Configuring Example Named Source-Port Filters. While named source-port filters may be defined and configured in two steps, this is not necessary. Here we define and configure each of the named source-port filters for our example network in a single step.

```
HPswitch(config)# filter source-port named-filter web-only drop 2-26
HPswitch(config)# filter source-port named-filter accounting drop 1-6,8,9,12-26
HPswitch(config)# filter source-port named-filter no-incoming-web drop 7,10,11

HPswitch(config)# show filter source-port

 Traffic/Security Filters

 Filter Name          | Port List          | Action
 -------------------- + ------------------- + ---------------------------
 web-only             | NOT USED           | drop 2-26
 accounting           | NOT USED           | drop 1-6,8-9,12-26
 no-incoming-web      | NOT USED           | drop 7,10-11

HP ProCurve Switch 2626(config)#
```

Ports and port trunks using the filter. When **NOT USED** is displayed the named source-port filter may be deleted.

Lists the ports and port trunks dropped by the filter. Ports and port trunks not shown are forwarded by the filter.

To remove a port or port trunk from the list, update the named source-port filter definition using the **forward** option.

Applying Example Named Source-Port Filters.

Once the named source-port filters have been defined and configured we now apply them to the switch ports.

```
HPswitch(config)# filter source-port 2-6,8,9,12-26 named-filter web-only
HPswitch(config)# filter source-port 7,10,11 named-filter accounting
HPswitch(config)# filter source-port 1  named-filter no-incoming-web
HPswitch(config)#
```

The **show filter** command shows what ports have filters applied.

```
HPswitch(config)# show filter

 Traffic/Security Filters

 IDX Filter Type   | Value
 --- ------------- + --------------------
 1   Source Port   | 2
 2   Source Port   | 3
 3   Source Port   | 4
 4   Source Port   | 5
 5   Source Port   | 6
 6   Source Port   | 8
 7   Source Port   | 9
 8   Source Port   | 12
  .       .          .
 20  Source Port   | 24
 21  Source Port   | 25
 22  Source Port   | 26
 23  Source Port   | 7
 24  Source Port   | 10
 25  Source Port   | 11
 26  Source Port   | 1
```

Indicates the port number or port-trunk name of the source port or trunk assigned to the filter.

An automatically assigned index number used to identify the filter for a detailed information listing. A filter retains its assigned IDX number for as long as the filter exists in the switch. The switch assigns the lowest available IDX number to a new filter. This can result in a newer filter having a lower IDX number than an older filter if a previous (source-port or named source-port) filter deletion created a gap in the filter listing.

Using the **IDX** value in the **show filter** command, we can see how traffic is filtered on a specific port (**Value**).The two outputs below show a non-accounting and an accounting switch port.

```
HPswitch(config)# show filter 4

 Traffic/Security Filters

  Filter Type : Source Port
  Source Port : 5

  Dest Port Type       | Action
  --------- --------- + -------
  1         10/100TX   | Forward
  2         10/100TX   | Drop
  3         10/100TX   | Drop
  4         10/100TX   | Drop
  5         10/100TX   | Drop
  6         10/100TX   | Drop
  7         10/100TX   | Drop
  8         10/100TX   | Drop
  9         10/100TX   | Drop
  10        10/100TX   | Drop
  11        10/100TX   | Drop
  12        10/100TX   | Drop
   .           .          .
```

```
Pswitch(config)# show filter 24

 Traffic/Security Filters

  Filter Type : Source Port
  Source Port : 10

  Dest Port Type       | Action
  --------- --------- + -------
  1         10/100TX   | Drop
  2         10/100TX   | Drop
  3         10/100TX   | Drop
  4         10/100TX   | Drop
  5         10/100TX   | Drop
  6         10/100TX   | Drop
  7         10/100TX   | Forward
  8         10/100TX   | Drop
  9         10/100TX   | Drop
  10        10/100TX   | Drop
  11        10/100TX   | Drop
  12        10/100TX   | Drop
   .           .          .
```

The same command, using IDX 26, shows how traffic from the Internet is handled.

```
HPswitch(config)# show filter 26

 Traffic/Security Filters

  Filter Type : Source Port
  Source Port : 1

  Dest Port Type       | Action
  --------- --------- + -------
  1         10/100TX   | Forward
  2         10/100TX   | Forward
  3         10/100TX   | Forward
  4         10/100TX   | Forward
  5         10/100TX   | Forward
  6         10/100TX   | Forward
  7         10/100TX   | Drop
  8         10/100TX   | Forward
  9         10/100TX   | Forward
  10        10/100TX   | Drop
  11        10/100TX   | Drop
  12        10/100TX   | Forward
   .            .          .
```

As the company grows, more resources are required in accounting. Two additional accounting workstations are added and attached to ports 12 and 13. A second server is added attached to port8.

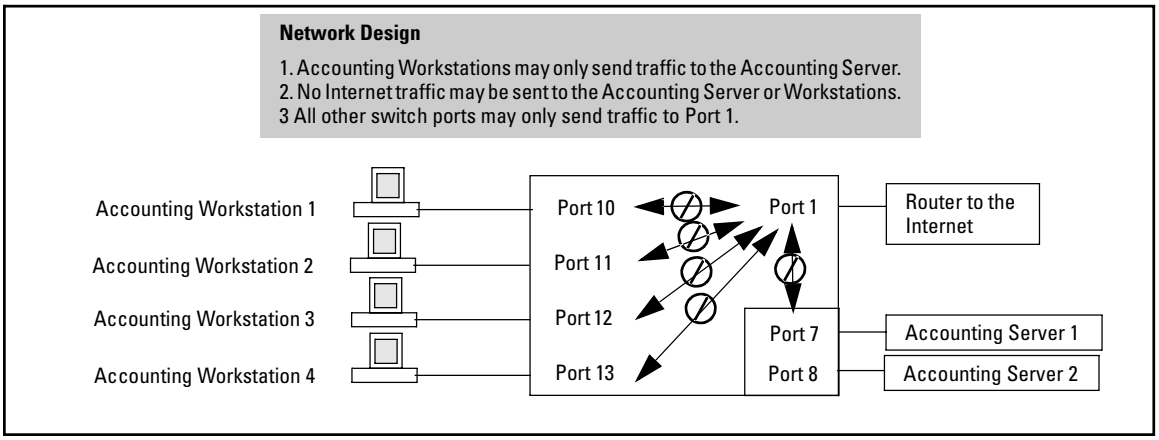

Figure 2. Expanded Network Configuration for Named Source-Port Filters Example

The following revisions to the named source-port filter definitions maintain the desired network traffic management, as shown in the **Action** column of the **show** command.

```
HPswitch(config)# filter source-port named-filter accounting forward 8,12,13
HPswitch(config)# filter source-port named-filter no-incoming-web drop 8,12,13
HPswitch(config)#
HPswitch(config)# show filter source-port

 Traffic/Security Filters

 Filter Name          | Port List            | Action
 -------------------- + -------------------- + ---------------------------
 web-only             | 2-6,8-9,12-26        | drop 2-26
 acconting            | 7,10-11              | drop 1-6,9,14-26
 no-incoming-web      | 1                    | drop 7-8,10-13

HPswitch(config)#
```

We next apply the updated named source-port filters to the appropriate switch ports. As a port can only have one source-port filter (named or not named), before applying the new named source-port filters we first remove the existing source-port filters on the port.

```
HPswitch(config)# no filter source-port 8,12,13
HPswitch(config)# filter source-port 8,12,13 named-filter accounting
HPswitch(config)#
```

The named source-port filters now manage traffic on the switch ports as shown below, using the **show filter source-port** command.

```
HPswitch(config)# show filter source-port

 Traffic/Security Filters

 Filter Name          | Port List            | Action
 -------------------- + -------------------- + ---------------------------
 web-only             | 2-6,9,14-26          | drop 2-26
 accounting           | 7-8,10-13            | drop 1-6,9,14-26
 no-incoming-web      | 1                    | drop 7-8,10-13

HPswitch(config)#
```

Release H.08.59 through Release H.08.64 Enhancements

Software fixes only; no new enhancements.

Release H.08.58 Enhancements

DHCP Option 82

Introduction

The routing switch can operate as a DHCP relay agent to enable communication between a client and a DHCP server on a different subnet. Without Option 82, DHCP operation modifies client IP address request packets to the extent needed to forward the packets to a DHCP server. Option 82 enhances this operation by enabling the routing switch to append an *Option 82 field* to such client requests. This field includes two suboptions for identifying the routing switch (by MAC address or IP address) and the routing switch port the client is using to access the network. A DHCP server with Option 82 capability can read the appended field and use this data as criteria for selecting the IP addressing it will return to the client through the usual DHCP server response packet. This operation provides several advantages over DHCP without Option 82:

- An Option 82 DHCP server can use a relay agent's identity and client source port information to administer IP addressing policies based on client and relay agent location within the network, regardless of whether the relay agent is the client's primary relay agent or a secondary agent.
- A routing switch operating as a primary Option 82 relay agent for DHCP clients requesting an IP address can enhance network access protection by blocking attempts to use an invalid Option 82 field to imitate an authorized client, or by blocking attempts to use response packets with missing or invalid Option 82 suboptions to imitate valid response packets from an authorized DHCP server.
- An Option 82 relay agent can also eliminate unnecessary broadcast traffic by forwarding an Option 82 DHCP server response only to the port on which the requesting client is connected, instead of broadcasting the DHCP response to all ports on the VLAN.

Note

The routing switch's DHCP Relay Information (Option 82) feature can be used in networks where the DHCP server(s) are compliant with RFC 3046 Option 82 operation. DHCP Servers that are not compliant with Option 82 operation ignore Option 82 fields. For information on configuring an Option 82 DHCP server, refer to the documentation provided with the server application.

Some client applications can append an Option 82 field to their DHCP requests. Refer to the documentation provided for your client application.

It is not necessary for all relay agents on the path between a DHCP client and the server to support Option 82, and a relay agent without Option 82 should forward DHCP packets regardless of whether they include Option 82 fields. However, Option 82 relay agents should be positioned at the DHCP policy boundaries in a network to provide maximum support and security for the IP addressing policies configured in the server.

Option 82 Server Support

To apply DHCP Option 82, the routing switch must operate in conjunction with a server that supports Option 82. (DHCP servers that do not support Option 82 typically ignore Option 82 fields.) Also, the routing switch applies Option 82 functionality only to client request packets being *routed* to a DHCP server. DHCP relay with Option 82 does not apply to *switched* (non-routed) client requests.

For information on configuring policies on a server running DHCP Option 82, refer to the documentation provided for that application.

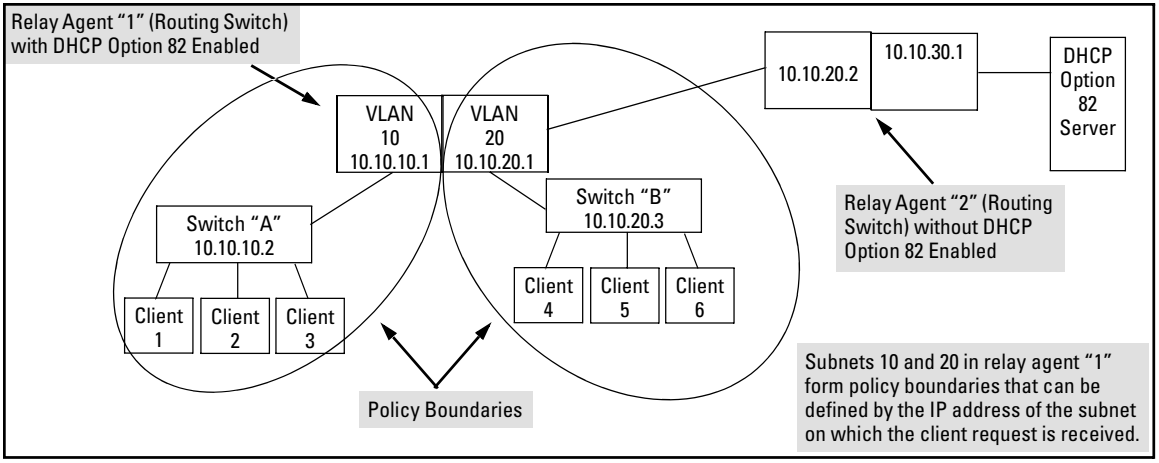

Figure 3. Example of a DHCP Option 82 Application

Terminology

Circuit ID: In Option 82 applications, the number of the port through which the routing switch receives a DHCP client request. On ProCurve fixed-port switches, the Circuit ID of a given port corresponds to the port number appearing on the front of the switch for that port. On ProCurve chassis switches, the port number for a given port corresponds to the internal ifIndex number

for that port. This value is included as a suboption in an Option 82 field that the relay agent appends to a Client DHCP request before forwarding the request toward a DHCP server. (For more on Circuit ID, refer to "Circuit ID" in the bulleted list on page 24.)

DHCP Policy Boundary: For Option 82 applications, an area of a network as defined by connection to a given routing switch or subnet and/or a specific port belonging to the routing switch or subnet.

DHCP relay agent: See Relay Agent.

Forwarding Policy: The Option 82 method the routing switch uses to process incoming client DHCP requests. For a given inbound DHCP client request, the forwarding policy determines whether the routing switch will add Option 82 information, replace existing Option 82 information, or leave any existing information unchanged. The policy also determines whether the routing switch will forward the client request toward a DHCP server or drop the request. For a DHCP server response to an Option 82 client request, the routing switch can optionally perform a validation check to determine whether to forward or drop the response. Each Option 82 relay agent in the path between a DHCP client and an Option 82 DHCP server can be configured with a unique forwarding policy, which enhances DHCP policy control over discrete areas of a network.

Primary Relay Agent: In the path between a DHCP client and a DHCP server, the first routing switch (configured to support DHCP operation) that a client DHCP request encounters in the path from the client to a DHCP server.

Relay Agent: A routing switch that is configured to support DHCP operation.

Remote ID: In Option 82 applications on ProCurve switches, either the MAC address of a relay agent, or the IP address of a VLAN or subnet configured on a relay agent. This value is included as a suboption in an Option 82 field that the relay agent appends to a Client DHCP request before forwarding the request toward a DHCP server. (For more on Remote ID, refer to "Remote ID" in the bulleted list on page 24.)

Secondary Relay Agent: In the path between a DHCP client and a DHCP server, any routing switch (configured to support DHCP operation) other than the primary relay agent.

General DHCP Option 82 Requirements and Operation

Requirements. DHCP Option 82 operation is configured at the global config level and requires the following:

- IP routing enabled on the switch
- DHCP-Relay Option 82 enabled (global command level)
- routing switch access to an Option 82 DHCP server on a different subnet than the clients requesting DHCP Option 82 support
- one IP Helper address configured on each VLAN supporting DHCP clients

General DHCP-Relay Operation with Option 82. Typically, the first (primary) Option 82 relay agent to receive a client's DHCP request packet appends an Option 82 field to the packet and forwards it toward the DHCP server identified by the IP Helper address configured on the VLAN in which the client packet was received. Other, upstream relay agents used to forward the packet may append their own Option 82 fields, replace the Option 82 field(s) they find in the packet, forward the packet without adding another field, or drop the packet. (Intermediate next-hop routing switches without Option 82 capability can be used to forward—route—client request packets with Option 82 fields.) Response packets from an Option 82 server are routed back to the primary relay agent (routing switch), and include an IP addressing assignment for the requesting client and an exact copy of the Option 82 data the server received with the client request. The relay agent strips off the Option 82 data and forwards the response packet out the port indicated in the response as the Circuit ID (client access port). Under certain validation conditions described later in this section, a relay agent detecting invalid Option 82 data in a response packet may drop the packet.

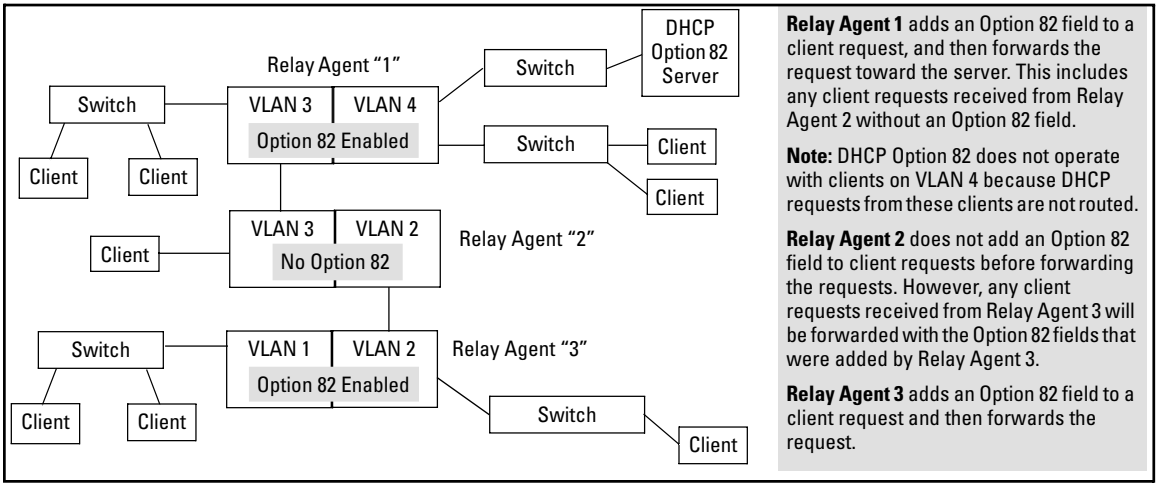

Figure 4. Example of DHCP Option 82 Operation in a Network with a Non-Compliant Relay Agent

Option 82 Field Content

The Remote ID and Circuit ID subfields comprise the Option 82 field a relay agent appends to client requests. A DHCP server configured to apply a different IP addressing policy to different areas of a network uses the values in these subfields to determine which DHCP policy to apply to a given client request.

- **Remote ID:** This configurable subfield identifies a policy area that comprises either the routing switch as a whole (by using the routing switch MAC address) or an individual VLAN configured on the routing switch (by using the IP address of the VLAN receiving the client request).
  - Use the IP address option if the server will apply different IP addressing policies to DHCP client requests from ports in different VLANs on the same routing switch.
  - Use the MAC address option if, on a given routing switch, it does not matter to the DHCP server which VLAN is the source of a client request (that is, use the MAC address option if the IP addressing policies supported by the target DHCP server do not distinguish between client requests from ports in different VLANs in the same routing switch)

    To view the MAC address for a given routing switch, execute the **show system-information** command in the CLI.

```
HPswitch(config)# show system-information

 Status and Counters - General System Information

  System Name        : HPswitch
  System Contact     :
  System Location    :

  MAC Age Time (sec) : 300

  Time Zone          : 0
  Daylight Time Rule : None


  Firmware revision  : I.08.60     Base MAC Addr      : 00110a-a50c20
  ROM Version        : I.08.05     Serial Number      : SG426NB048

  Up Time            : 32 mins     Memory   - Total   : 33,043,456
  CPU Util (%)       : 4                      Free    : 25,335,136

  IP Mgmt  - Pkts Rx : 0           Packet   - Total   : 1998
             Pkts Tx : 0           Buffers    Free    : 1748
                                              Lowest  : 1741
                                              Missed  : 0
```

Switch MAC Address

Figure 5. Using the CLI To View the Switch MAC Address

- **Circuit ID:** This nonconfigurable subfield identifies the port number of the physical port through which the routing switch received a given DHCP client request, and is necessary to identify if you want to configure an Option 82 DHCP server to use the Circuit ID to select a DHCP policy to assign to clients connected to the port. This number is the identity of the inbound port. On ProCurve fixed-port switches, the port number used for the Circuit ID is always the same as the physical port number shown on the front of the switch. On ProCurve chassis switches, where a dedicated, sequential block of internal port numbers are reserved

for each slot, regardless of whether a slot is occupied, the circuit ID for a given port is the sequential index number for that port position in the slot. (To view the Index number assignments for ports in the routing switch, use the **walkmib ifname** command.)

For example, the circuit ID for a client connected to port 11 on a ProCurve 2650-PWR (J8165A) switch is “11”. However, the Circuit ID for port B11 on a ProCurve 5304xl (J4850A) is “37”. (See 6, below.)

```
HPswitch(config)# walkmib ifname
ifName.1 = A1
ifName.2 = A2
ifName.3 = A3
ifName.4 = A4
ifName.27 = B1
ifName.28 = B2
ifName.29 = B3
ifName.30 = B4
ifName.31 = B5
ifName.32 = B6
ifName.33 = B7
ifName.34 = B8
ifName.35 = B9
ifName.36 = B10
ifName.37 = B11
ifName.38 = B12
ifName.39 = B13
ifName.40 = B14
ifName.41 = B15
ifName.42 = B16
ifName.43 = B17
ifName.44 = B18
ifName.45 = B19
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

In this example, the 5304xl has a 4-port module installed in slot “A” and a 24-port module installed in slot “B”. Thus, the first port numbers in the listing are the Index numbers reserved for slot “A”. The first Index port number for slot “B” is “27”, and the Index port number for port B11 (and therefore the Circuit ID number) is “37”.

The Index (and Circuit ID) number for port B11 on a 5304xl routing switch.

Figure 6. Using Walkmib To Determine the Circuit ID for a Port on a ProCurve Chassis

For example, suppose you wanted port 10 on a given relay agent to support no more than five DHCP clients simultaneously, you could configure the server to allow only five IP addressing assignments at any one time for the circuit ID (port) and remote ID (MAC address) corresponding to port 10 on the selected relay agent.

Similarly, if you wanted to define specific ranges of addresses for clients on different ports in the same VLAN, you could configure the server with the range of IP addresses allowed for each circuit ID (port) associated with the remote ID (IP address) for the selected VLAN.

Forwarding Policies

DHCP Option 82 on ProCurve switches offers four forwarding policies, with an optional validation of server responses for three of the policy types (**append**, **replace**, or **drop**).

Table 1. Configuration Options for Managing DHCP Client Request Packets

Option 82 Configuration	DHCP Client Request Packet Inbound to the Routing Switch	
	Packet Has No Option 82 Field	Packet Includes an Option 82 Field
Append	Append an Option 82 Field	**Append** allows the most detail in defining DHCP policy boundaries. For example, where the path from a client to the DHCP Option 82 server includes multiple relay agents with Option 82 capability, each relay agent can define a DHCP policy boundary and append its own Option 82 field to the client request packet. The server can then determine in detail the agent hops the packet took, and can be configured with a policy appropriate for any policy boundary on the path. **Note:** In networks with multiple relay agents between a client and an Option 82 server, **append** can be used only if the server supports multiple Option 82 fields in a client request. If the server supports only one Option 82 field in a request, consider using the **keep** option.
Keep	Append an Option 82 Field	If the relay agent receives a client request that already has one or more Option 82 fields, **keep** causes the relay agent to retain such fields and forward the request without adding another Option 82 field. But if the incoming client request does not already have any Option 82 fields, the relay agent appends an Option 82 field before forwarding the request. Some applications for **keep** include: • The DHCP server does not support multiple Option 82 packets in a client request and there are multiple Option 82 relay agents in the path to the server. • The unusual case where DHCP clients in the network add their own Option 82 fields to their request packets and you do not want any additional fields added by relay agents. This policy does not include the **validate** option (described in the next section) and allows forwarding of all server response packets arriving inbound on the routing switch (except those without a primary relay agent identifier.)
Replace	Append an Option 82 Field	**Replace** replaces any existing Option 82 fields from downstream relay agents (and/or the originating client) with an Option 82 field for the current relay agent.. Some applications for **replace** include: • The relay agent is located at a point in the network that is a DHCP policy boundary and you want to replace any Option 82 fields appended by downstream devices with an Option 82 field from the relay agent at the boundary. (This eliminates downstream Option 82 fields you do not want the server to use when determining which IP addressing policy to apply to a client request.) • In applications where the routing switch is the primary relay agent for clients that may append their own Option 82 field, you can use **replace** to delete these fields if you do not want them included in client requests reaching the server.
Drop	Append an Option 82 Field	**Drop** causes the routing switch to drop an inbound client request with an Option 82 field already appended. If no Option 82 fields are present, **drop** causes the routing switch to add an Option 82 field and forward the request. As a general guideline, configure **drop** on relay agents at the edge of a network, where an inbound client request with an appended Option 82 field may be unauthorized, a security risk, or for some other reason, should not be allowed.

Multiple Option 82 Relay Agents in a Client Request Path

Where the client is one router hop away from the DHCP server, only the Option 82 field from the first (and only) relay agent is used to determine the policy boundary for the server response. Where there are multiple Option 82 router hops between the client and the server, you can use different configuration options on different relay agents to achieve the results you want. This includes configuring the relay agents so that the client request arrives at the server with either one Option 82 field or multiple fields. (Using multiple Option 82 fields assumes that the server supports multiple fields and is configured to assign IP addressing policies based on the content of multiple fields.)

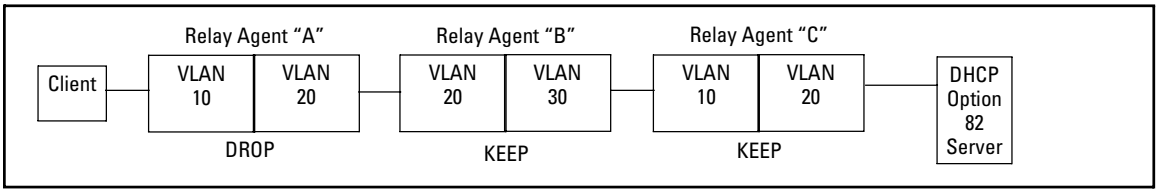

Figure 7. Example Configured To Allow Only the Primary Relay Agent To Contribute an Option 82 Field

The above combination allows for detection and dropping of client requests with spurious Option 82 fields. If none are found, then the drop policy on the first relay agent adds an Option 82 field, which is then kept unchanged over the next two relay agent hops ("B" and "C"). The server can then enforce an IP addressing policy based on the Option 82 field generated by the edge relay agent ("A"). In this example, the DHCP policy boundary is at relay agent 1.

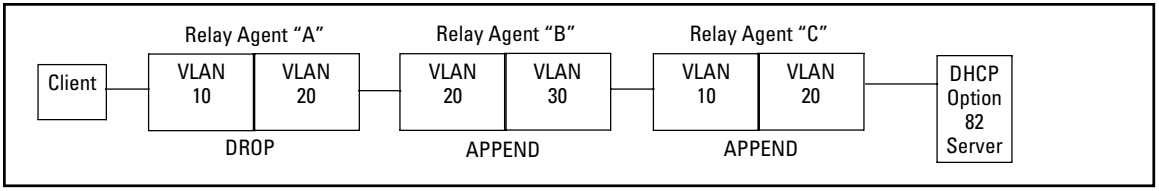

Figure 8. Example Configured To Allow Multiple Relay Agents To Contribute an Option 82 Field

This is an enhancement of the previous example. In this case, each hop for an accepted client request adds a new Option 82 field to the request. A DHCP server capable of using multiple Option 82 fields can be configured to use this approach to keep a more detailed control over leased IP addresses. In this example, the primary DHCP policy boundary is at relay agent "A", but more global policy boundaries can exist at relay agents "B" and "C".

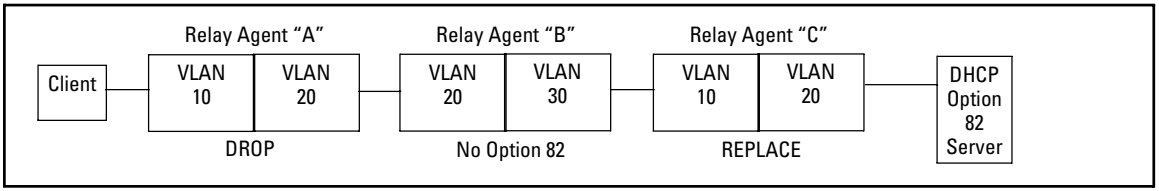

Figure 9. Example Allowing Only an Upstream Relay Agent To Contribute an Option 82 Field

Like the first example, above, this configuration drops client requests with spurious Option 82 fields from clients on the edge relay agent. However, in this case, only the Option 82 field from the last relay agent is retained for use by the DHCP server. In this case the DHCP policy boundary is at relay agent "C". In the previous two examples the boundary was with relay "A".

Validation of Server Response Packets

A valid Option 82 server response to a client request packet includes a copy of the Option 82 field(s) the server received with the request. With validation disabled, most variations of Option 82 information are allowed, and the corresponding server response packets are forwarded.

Server response validation is an option you can specify when configuring Option 82 DHCP for **append**, **replace**, or **drop** operation. (Refer to "Forwarding Policies" on page 26.) Enabling validation on the routing switch can enhance protection against DHCP server responses that are either from untrusted sources or are carrying invalid Option 82 information.

With validation enabled, the relay agent applies stricter rules to variations in the Option 82 field(s) of incoming server responses to determine whether to forward the response to a downstream device or to drop the response due to invalid (or missing) Option 82 information. Table 2, below, illustrates relay agent management of DHCP server responses with optional validation enabled and disabled.

Table 2. Relay Agent Management of DHCP Server Response Packets

Response Packet Content	Option 82 Configuration	Validation Enabled on the Relay Agent	Validation Disabled (The Default)
Valid DHCP server response packet without an Option 82 field.	**append**, **replace**, or **drop**[1]	Drop the server response packet.	Forward server response packet to a downstream device.
	keep[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.
The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a *Remote ID* and *Circuit ID* combination that did not originate with the given relay agent.	**append**	Drop the server response packet.	Forward server response packet to a downstream device.
	replace or **drop**[1]	Drop the server response packet.	Drop the server response packet.
	keep[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.
The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a *Remote ID* that did not originate with the relay agent.	**append**	Drop the server response packet.	Forward server response packet to a downstream device.
	replace or **drop**[1]	Drop the server response packet.	Drop the server response packet.
	keep[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.

Response Packet Content	Option 82 Configuration	Validation Enabled on the Relay Agent	Validation Disabled (The Default)
All other server response packets[3]	**append**, **keep**[2], **replace**, or **drop**[1]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.

[1]Drop is the recommended choice because it protects against an unauthorized client inserting its own Option 82 field for an incoming request.

[2]A routing switch with DHCP Option 82 enabled with the **keep** option forwards all DHCP server response packets except those that are not valid for either Option 82 DHCP operation (compliant with RFC 3046) or DHCP operation without Option 82 support (compliant with RFC 2131).

[3]A routing switch with DHCP Option 82 enabled drops an inbound server response packet if the packet does not have any device identified as the primary relay agent (*giaddr* = null; refer to RFC 2131).

Multinetted VLANs

On a multinetted VLAN, each interface can form an Option 82 policy boundary within that VLAN if the routing switch is configured to use IP for the remote ID suboption. That is, if the routing switch is configured with IP as the remote ID option and a DHCP client request packet is received on a multinetted VLAN, the IP address used in the Option 82 field will identify the subnet on which the packet was received instead of the primary IP address for the VLAN. This enables an Option 82 DHCP server to support more narrowly defined DHCP policy boundaries instead of defining the boundaries at the VLAN or whole routing switch levels. If the MAC address option (the default) is configured instead, then the routing switch MAC address will be used regardless of which subnet was the source of the client request. (The MAC address is the same for all VLANs configured on the routing switch.)

Note that all request packets from DHCP clients in the different subnets in the VLAN must be able to reach any DHCP server identified by the IP Helper Address(es) configured on that VLAN.

Configuring Option 82 Operation on the Routing Switch

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

append: *Configures the routing switch to append an Option 82 field to the client DHCP packet. If the client packet has any existing Option 82 field(s) assigned by another device, then the new field is appended to the existing field(s).*

The appended Option 82 field includes the switch Circuit ID (inbound port number) associated with the client DHCP packet, and the switch Remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN's IP address instead of the switch MAC address for the remote ID, use the* **ip** *option (below).*

replace: *Configures the routing switch to replace any existing Option 82 field(s) in an inbound client DHCP packet with one Option 82 field for the current routing switch.*

The replacement Option 82 field includes the switch circuit ID (inbound port number) associated with the client DHCP packet, and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN's IP address instead of the switch MAC address for the remote ID, use the* **ip** *option (below).*

drop: *Configures the routing switch to unconditionally drop any client DHCP packet received with existing Option 82 field(s). This means that such packets will not be forwarded. Use this option where access to the routing switch by untrusted clients is possible.*

If the routing switch receives a client DHCP packet without an Option 82 field, it adds an Option 82 field to the client and forwards the packet. The added Option 82 field includes the switch circuit ID (inbound port number) associated with the client DHCP packet, and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN's IP address instead of the switch MAC address for the remote ID, use the IP option (below).*

keep: *For any client DHCP packet received with existing Option 82 field(s), configures the routing switch to forward the packet as-is, without replacing or adding to the existing Option 82 field(s).*

**For more on identifying the inbound port number, refer to "Circuit ID" in the bulleted list on page 24.*

[validate]: *This option operates when the routing switch is configured with append, replace, or drop as a forwarding policy. With validate enabled, the routing switch applies stricter rules to an incoming Option 82 server response to determine whether to forward or drop the response. For more information, refer to "Validation of Server Response Packets" on page 28.*

[ip | mac]

This option specifies the remote ID suboption the routing switch will use in Option 82 fields added or appended to DHCP client packets. The choice of type depends on how you want to define DHCP policy areas in the client requests sent to the DHCP server. (Refer to "Option 82 Field Content" on page 24.)

ip: *Specifies the IP address of the VLAN on which the client DHCP packet enters the switch.*

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.) This is the default setting.*

Notes on Default Remote ID Selection: *Executing the Option 82 command without specifying either* **ip** *or* **mac** *configures the remote ID as the MAC address of the switch on which the packet was received from the client. The command options for viewing the routing switch MAC address are listed at the end of the "Remote ID" description that begins on page 24.*

Operating Notes

- This implementation of DHCP relay with Option 82 complies with the following RFCs:
  - RFC 2131
  - RFC 3046
- Moving a client to a different port allows the client to continue operating as long as the port is a member of the same VLAN as the port through which the client received its IP address. However, rebooting the client after it moves to a different port can alter the IP addressing policy the client receives if the DHCP server is configured to provide different policies to clients accessing the network through different ports.
- 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). (That is, the giaddr 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.
- DHCP request packets from multiple DHCP clients on the same relay agent port will be routed to the same DHCP server(s). Note that when using 802.1X on a 5300xl switch running software release E.09.xx or greater, a port's VLAN membership may be changed by a RADIUS server responding to a client authentication request. In this case the DHCP server(s) accessible from the port may change if the VLAN assigned by the RADIUS server has different DHCP helper addresses than the VLAN used by unauthenticated clients.
- Where multiple DHCP servers are assigned to a VLAN, a DHCP client request cannot be directed to a specific server. Thus, where a given VLAN is configured for multiple DHCP servers, all of these servers should be configured with the same IP addressing policy.
- Where routing switch "A" is configured to insert its MAC address as the Remote ID in the Option 82 fields appended to DHCP client requests, and upstream DHCP servers use that MAC address as a policy boundary for assigning an IP addressing policy, then replacing

switch "A" makes it necessary to reconfigure the upstream DHCP server(s) to recognize the MAC address of the replacement switch. This does not apply in the case where an upstream relay agent "B" is configured with **option 82 replace**, which removes the Option 82 field originally inserted by switch "A".

- Relay agents without Option 82 can exist in the path between Option 82 relay agents and an Option 82 server. The agents without Option 82 will forward client requests and server responses without any effect on Option 82 fields in the packets.
- If the routing switch is not able to add an Option 82 field to a client's DHCP request due to the message size exceeding the MTU (Maximum Transmission Unit) size, then the request is forwarded to the DHCP server without Option 82 information and an error message is logged in the switch's Event Log.

Release H.08.55, H.08.56, and H.08.57 Enhancements

Software fixes only; no new enhancements.

Release H.08.53 Enhancements

Enhancement	Overview
Supports 253 VLANs	Previously, themaximum number of VLANs was 30.
DiffServ Codepoint (DSCP) Marking - L3/L4	Provide support for the following DSCP modes: RFC2474 DiffServ Precedence, RFC2597 DiffServ Assured Forwarding (AF), and RFC2598 DiffServ Expedited Forwarding (EF). (Refer to: Chapter 6, "Quality of Service (QoS): Managing Bandwidth More Effectively on the Series 2600/2600-PWR and Series 2800 Switches" in the *Advanced Traffic Management Guide*—part number 5990-8853, October 2004— on the ProCurve Networking Web site.*)
802.1s Multiple Spanning-Tree	Adds the option for running 802.1s Multiple Spanning-Tree on the switch to enable multiple spanning-tree instances. Interoperates with legacy 802.1D (STP) and 802.1w (RSTP) spanning-tree. (Refer to: Chapter 5, "Spanning-Tree Operation" in the *Advanced Traffic Management Guide*—part number 5990-8853, October 2004— on the ProCurve Networking Web site.*)
Web Authentication	Web authentication adds a new securityoption that uses a Web page login to authenticate users via a RADIUS server for access to the network. (Refer to: Chapter 3, "Web and MAC Authentication for the Series 2600/2600-PWR and 2800 Switches" in the *Access Security Guide*—part number 5990-6024, October 2004— on the ProCurve Networking Web site.*)
MAC Authentication	MAC authentication adds a new security option that uses a device's MAC address to authenticate the device via a RADIUS server for access to the network. (Refer to: Chapter 3, "Web and MAC Authentication for the Series 2600/2600-PWR and 2800 Switches" in the *Access Security Guide*—part number 5990-6024, October 2004—on the ProCurve Networking Web site.*)

* To download switch documentation for software release H.08.*5X,* refer to "To Download Product Documentation:" on page 1.

Enhancement	Overview (Continued)
MAC Lockdown/Lockout	• MAC Lockdown enables the permanent assignment of a MAC address and VLAN to a specific port on the switch. • MAC Lockout causes the switch to drop any traffic to or from the specified MAC address(es). (Refer to: Chapter 9, "Configuring and Monitoring Port Security" in the *Access Security Guide*—part number 5990-6024, October 2004—on the ProCurve Networking Web site.*)
Secure Copy and Secure FTP	Enables use of a secure, encrypted SSH session for transferring files to or from the switch. (Refer to: Appendix A, "File Transfers" in the *Management and Configuration Guide*—part number 5990-6023, October 2004— on the ProCurve Networking Web site.*)
Source Port Filters	You can configure a traffic filter to either forward or drop all network traffic moving between an inbound (source) port or trunk and any outbound (destination) ports and trunks (if any) on the switch. (Refer to: Chapter 10, "Traffic/Security Filters" in the *Access Security Guide*—part number 5990-6024, October 2004—on the ProCurve Networking Web site.*)

* To download switch documentation for software release H.08.*5X,* refer to "To Download Product Documentation:" on page 1.

Front-Panel Security	Provides the optionfor enabling or disabling some of the functions of the Reset and Clear buttons on the switch's front panel. This feature also provides the ability to disable password recovery for situations requiring a higher level of security. (Refer to: Chapter 2, "Configuring Username and Password Security" in the *Access Security Guide*—part number 5990-6024, October 2004— on the ProCurve Networking Web site.*)
Auto-MDI-X manual mode	Provides CLI commands for changing the cable-configuration support on the switch's copper ports. The options include auto-MDIX (the default), MDI, and MDI-X. This also allows the manual configuration of port speed. (Refer to: Chapter 10, "Port Status and Basic Configuration" in the *Management and Configuration Guide*—part number 5990-6023, October 2004— on the ProCurve Networking Web site.*)
Egress Port Monitoring	You can designate a port for monitoringinbound (ingress) and outbound (egress) traffic of other ports and of static trunks on the switch. (Refer to: Appendix B, "Monitoring and Analyzing Switch Operation" in the *Management and Configuration Guide*—part number 5990-6023, October 2004— on the ProCurve Networking Web site.*)
Faster System Boot	BootROM version H.08.02.

* To download switch documentation for software release H.08.*5X*, refer to "To Download Product Documentation:" on page 1.

Release H.07.46, and H.07.50 Enhancements

Software fixes only; no new enhancements.

Release H.07.45 Enhancements

Release H.07.45 provides support for the HP ProCurve 600 Redundant and External Power Supply (J8168A). This enhancement only applies to the 2600-PWR switches (J8164A and J8165A). To use the EPS power support from an HP ProCurve 600, you must upgrade the software on your 2600-PWR switches to H.07.45 or later.

If an HP 600 EPS cable is connected to a 2600-PWR running software releases prior to H.07.45, the FAULT LED and EPS status LED will flash, and the error log will contain the following message:

```
W 01/01/90 00:01:25 chassis: EPS not supported by switch code. Please
update.
```

Release H.07.41 Enhancements

Release H.07.41 was the first release for the 2600-PWR Switches, 2626-PWR (J8164A) and the 2650-PWR (J8165A). The 2600-PWR Switches provides 802.3af compliant Power over Ethernet (PoE) capabilities. This software remains backward compatible and runs on the Series 2600 Switches and the Switch 6108.

Release H.07.32 Enhancements

Software fixes only; no new enhancements.

Release H.07.31 Enhancements

To Locate Publications Supporting H.07.31 Features:

1. Go to the ProCurve Networking Web site at **http://www.procurve.com**.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation.
4. Select the document indicated in the enhancement description (table 3) for the desired feature.

(ProCurve recommends periodically visiting the **ProCurve Web site** to keep up-to-date with the latest documentation available for the ProCurve Series 2600 Switches.)

Table 3. Release H.07.31 Enhancements

Enhancement	Overview
Software Support for New HP ProCurve Switch 2626	Release H.07.31 supports the new, stackable HP ProCurve 2626 Switch offering 24 auto-sensing 10/100 ports plus 2 dual personality ports for 10/100/1000 or mini-GBIC connectivity. If you are viewing this document online, **click here to visit the ProCurve Networking Web site for more information**.
SSL	Provides Secure Socket Layer (SSL) transactions for Web management access. This allows the switch to authenticate itself to the user and to establish a secure connection. Includes support for self-signed and CA signed certificates to allow administrators to choose the level of security required.[1]
SSHv2	Updates SSH to support SSHv2, allowing PEM-encoded keys and greater compatibly with SSH client software.[1]
802.1x Open VLAN Mode	Adds flexibility for clients lacking 802.1x supplicant software, plus an additional provision for controlling access by authenticated clients.[1]
Debug and Syslog Messaging Operation	The Debug/Syslog feature provides a method for recording messages useful for debugging network-level problems such as routing misconfigurations and other protocol details.[2]
Port-Security Option for Configuring Allowed MAC Addresses	Adds the **configured** option to **port-security learn-mode** to allow a port to add only specifically configured MAC addresses. Using this option, a switch port does not automatically learn non-specified MAC addresses from the network.[1]
SNMPv3 Access	The Series 2600 switches and the Switch 6108 now support SNMPv3 to enhance the security of SNMPv3 traffic. It includes authentication and/or encryption of management traffic configurable at the operator's discretion.[2]
IGMPv3 Support	Adds support for the IGMPv3 Join request.[2]
Additional Outbound Port Queue	Adds a fourth outbound port queue.[2]

[1] Refer to the *Access Security Guide* for the HP ProCurve Series 4100 Switches, Series 2600 Switches, and the Switch 6108, Edition 1—5990-5995, May 2003 (or later) on the ProCurve Networking Web site.

[2] Refer to the *Management and Configuration Guide* for the HP ProCurve Series 4100 Switches, Series 2600 Switches, and the Switch 6108, Edition 1 — 5990-5998, May 2003 (or later) on the ProCurve Networking Web site.

Release H.07.03 Enhancements

Software fixes only; no new enhancements.

Release H.07.02 Enhancements

Release H.07.02 was the original software released to support the HP ProCurve Switch 2650 and the Switch 6108.

Software Fixes in Releases H.07.02 - H.08.71

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

Release H.08.72

Problems Resolved in Release H.08.71

- **LLDP (PR_1000241315)** — The CLI command **show LLDP** does not display information correctly.
- **Web (PR_1000211978)** — On a Stack Management Commander, when using "stack access" to view members, the screen does not display correct information.

Release H.08.71

Problems Resolved in Release H.08.71

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

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

Release number H.08.70 was never released.

Problems Resolved in Release H.08.70

- **802.1s (PR_1000227432)** — Leaning flag is not set when CIST port states are transitioning.
- **802.1s (PR_1000233920)** — 802.1s blocks a port that is connected to an RSTP device.
- **Crash (PR_1000229656)** — Switch cannot reach RADIUS server and crashes with a message similar to:

  ```
  Software exception at exception.c:373-in 'tHttpd', task ID = 0x257dda8
  ->Memory system error at 0x24ea750 - memPartFree.
  ```

- **Web Authentication (PR_1000230444) —** Using port-based web authentication on the Switch will cause some users to never receive the web authentication screen. This occurs if a client receives the same unauthenticated DHCP address that a previous authorized client has used.
- **Web/Stack (PR_1000239924)** — As an IP Stack Management Commander, the Switch does not display the device view (back of box) for a switch which is a member.

Release H.08.69

Release number H.08.68 was never released.

Problems Resolved in Release H.08.69

- **CLI (PR_1000198460)** — In the CLI help menu for VLANs, the maximum number of VLANs displays incorrect information.
- **Console/TELNET (PR_1000195647) —** When a console or TELNET session hangs, issuing the **kill** command will also hang.
- **Counters (PR_1000221089) —** When accessing the 64 bit counters, the counters may not always be correct.
- **Crash (PR_1000193582)** — Software Exception when clicking on the Identity Tab of a member Switch in the Web user interface. The switch may crash with a message similar to:

  ```
  Software exception at http_state.c:1138 in 'mHttpCtrl' TaskID=0x1722cf8
  ```

- **Crash (PR_1000204782)** — Bus error when copying a configuration to the switch. The switch may crash with a message similar to:

  ```
  Bus error: HW Addr=0x594f5531 IP=0x004ff8a8 Task='mftTask'
  Task ID=0x126eba0 fp: 0x00000000 sp:0x0126e7d0 lr:0x001e655c.
  ```

- **QOS (PR_1000200746)** — Switch truncates the DSCP-map name after a reboot.
- **Syslog (PR_1000215699) —** Switch does not send all Event Log entries to the syslog server at switch boot..
- **Web UI (PR_1000214188)** — While working in the Status-Overview screen, the scroll bar does not display or respond correctly after resizing a window.

Release H.08.67

Release number H.08.66 was never released.

Problems Resolved in Release H.08.67

- **Trunk ports (PR_1000231897)** — The switch may duplicate broadcast packets across all ports on a trunk link.

Release H.08.65

- **Config (PR_1000215024)** — The switch may experience a memory leak when loading a configuration file several times.

Release H.08.64

Release number H.08.63 was never released.

Problems Resolved in Release H.08.64

- **Config (PR_1000207697)** — Loading a startup-configuration file fails when attempting to declare a VLAN in the configuration file as a management VLAN, and the VLAN does not currently exist on the switch. The switch indicates the downloaded file as being corrupted, listing the VID of the specified management VLAN as not being found.

Release H.08.62

Problems Resolved in Release H.08.62

- **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 H.08.61

Problems Resolved in Release H.08.61

- **Crash/Static Route (PR_1000217354)** — The switch may crash with a `Bus error in mSnmpCtrl` when adding a less-specific static route.
- **STP/Mirroring (PR_1000211360)** — A loop is created with STP enabled and monitoring port 50 while port 50 is Blocking.

Release H.08.60

Problems Resolved in Release H.08.60

- **Crash (PR_1000207542)** — The switch may crash with a bus error or a task hang.
- **Port Security (PR_1000203984)** — When the limit is reached the warning message is displayed: Number of configured addresses on port xx exceeds address-limit. The address will be saved and displayed in the address list of Show Port-security xx. Data from the added address is passed by the switch.

Release H.08.59

Problems Resolved in Release H.08.59

- **Config (PR_1000216051)** — Copying a previously saved startup-configuration with **stack join (mac address)** to a member switch of the IP stack will break the membership of that stack.
- **Crash (PR_1000201614)** — The switch may crash within the CLI **setup menu** if a 16-character manager password set.
- **Spanning Tree (PR_1000214598)** — The switch will not accept the **spanning-tree 1 mode fast** command within the CLI.

Release H.08.58

Problems Resolved in Release H.08.58

- **Crash (PR_1000205768)** — In some cases, if the user does not configure a System Name within the Web user interface, the switch may crash with the following message:

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

- **Open VLAN (PR_1000210932)** — A port configured for Open VLAN mode (Unauthorized VLAN) does not work with any Port-Security Learn-Mode setting.
- **Web UI (PR_1000191635)** — Within the Web UI "Port Counters" and "Port Status" pages, the "Port" column may be sorted incorrectly.
- **Web UI (PR_93721)** — The scroll bar within the "Web Status" page does not work.

Release H.08.57

Problems Resolved in Release H.08.57

- **Crash (PR_1000213744)** — Creating any source port filter to drop on port 26 on a switch 2626 may result in a crash with error message similar to:

  ```
  Assertion failed: BCM_PBMP_MEMBER(npbm,(B56_STACKING_PORT(unit))),
  file hp_standalone.c, line 7108.
  ```

- **MSTP (PR_1000207608)** — After the root bridge is agreed, the non-root switch continues to send out BPDUs claiming to be Root, resulting in possible instability in the STP topology.
- **SNMP (PR_1000212170)** — The switch will initially send out reboot traps with an agent address of 0.0.0.0 when the agent address is statically set.

Release H.08.56

Problems Resolved in Release H.08.56

- **CLI (PR_1000202435)** — When IGMP fast-leave is configured via the CLI, the configuration is not displayed in **show config**.
- **Config (PR_1000212686)** — A J4899B does not accept a configuration file created on a J4899A.

Release H.08.55

Release number H.08.54 was never released.

Problems Resolved in Release H.08.55

- **ACL (PR_1000207620)** — The switch sometimes incorrectly permits TCP and UDP traffic in spite of an ACL configuration.
- **CDP (PR_1000195343)** — Entering the command **show cdp neighbor detail x** (where x is the port number) displays details for all active ports with CDP neighbors whose numbers begin with x. Only occurs when the **detail** parameter is included.
- **Config (PR_1000211397)** — A J4900B does not accept a configuration file saved from a J4900A.
- **IP Helper/DHCP Relay (PR_1000197046)** — DHCP clients successfully acquire their IP address via DHCP. However, when attempting to access additional data from the DHCP server via DHCP Inform messages from the client, the transaction fails.
- **RMON (PR_1000196477)** — When RMON thresholds in the switch are exceeded, no trap is generated.
- **SNMP (PR_1000190654)** — Some of the fault finder events in the SNMP traps list a 0.0.0.0 IP address in the URL. This happens when the switch has the IP address configured on a VLAN other than the default.
- **SNMP (PR_1000196170)** — Switch does not send out SNMP traps for events that occur before the switch IP stack has completed initialization.
- **Web UI/Port Security (PR_1000195894)** — The Web user interface does not allow the user to select multiple ports when configuring port-security.

Release H.08.53

Release numbers H.08.01 through H.08.52 were never released.

Problems Resolved in Release H.08.53

- **802.1p (PR_1*20469)** — Port priority is not adopted as the traffic is forwarded on the appropriate outbound port.
- **CLI (PR_82258)** — **sh ip igmp** command shows blank lines mixed within the displayed table.
- **CLI (PR_1*18700)** — **Show ip route** "IP Route Entries" not centered in output.
- **CLI (PR_1*18755)** — Executing a **show power bri** command results in garbled output.
- **Config (PR_92346)** — Unable to delete empty VLAN.
- **Crash (PR_1*2177)** — 2600, switch may crash with a message similar to:

  ```
  Software exception at gamHwLearn.c:412 -- in 'tARL', task ID = 0x1893f08
  ```

- **Crash (PR_1*3433)** — Switch may crash with a message similar to:

  ```
  Assertion failed: SOC_MEM_BLOCK_VALID(unit, mem, copyno), file mem.c,
  line 326
  ```

- **Crash (PR_1*5469)** — 2600 crash during boot on top of tree.
- **Help (PR_98206)** — Help file is not consistent with the actual usage.
- **Help (PR_1*21395)** — Help text incorrect for some **ip icmp** commands.
- **Hot Swap (PR_1*18578)** — Dual personality ports hotswap out problem.
- **LACP (PR_1*6404)** — Dynamic LACP: Standby mode problem.
- **Routing (PR_91549) —** Addr manager using 0 based call to the soc_mem_xx layer.
- **Routing (PR_93481)** — 2650 software routes a packet when the DA MAC belongs to another VLAN.
- **SNMP (PR_88716)** — SNMP walk times out with large configuration.
- **SNMP (PR_1*3361)** — 'snmpv3' configtest failure.
- **Syslog (PR_97016)** — syslog word-complete options are not consistent with 6108 and 2800.
- **Web (PR_89899)** — Web UI port statistic counters are overwriting one another.
- **Web (PR_97621)** — 2650/H.07.32 | Sun Java 1.4.X: Unable to use Web browser.
- **Web (PR_1*12103)** — Garbage in the Web UI Status | Overview screen
- **Web (PR_1*1216)** — Web UI, log error.
- **Web (PR_1*21294)** — Stack Management Screen is blank.
- **Web (PR_1*3133)** — Web UI: Stack Access is not available.

Release H.07.56

Problems Resolved in Release H.07.56

- **Config (PR_1000216051)** — Returning a previously saved startup-configuration with **stack join (mac address)** to a member switch of the IP stack breaks the membership of that same stack. Commander hangs with member `mismatched`.
- **Open VLAN (PR_1000210932)** — open VLAN mode (Unauth VLAN) does not work with any Port-Security Learn-Mode
- **Web (PR_80857)** — A problem with IE4 and WebAgent. Recompiled the Web Agent with a new Java Development Kit (1.2 - was 1.1)

Release H.07.55

Problems Resolved in Release H.07.55

- **802.1X (PR 1000208530)** — Effects are unknown, but could include crashes such as bus errors.
- **CDP (PR_1000195343)** — Entering the command "**show cdp neighbor detail x**" displays incorrect information.
- **Config (PR_1000197097)** — When copying a configuration that doesn't have SNMP community names defined, the 6108 switch adds the 'public' community name with manager unrestricted rights.
- **Crash (PR_1000205768)** — "null" System Name in the Web user interface may crash with:

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

- **Crash (PR_1000201614)** — When the switch is set with a 16 character manager password, hitting the down arrow keys twice within the start of the setup menu, a 'Bus error' crash may occur. The bus errors vary.
- **Crash (PR_1000092011)** — The switch may crash while using the web user interface with a message similar to:

  ```
  Software exception at exception.c:356 -- in 'mHttpCtrl', task ID =
  0x139ba40.
  ```

- **DHCP Relay (PR_1000188635)** — DHCP Relay sometimes preserves the incoming MAC SA in relayed packets.
- **IGMP (PR_1000191237)** — IGMP will not process any incoming or outgoing IGMP protocol packets if user adds a port to VLAN with 257 groups.

- **RMON (PR_1000196477)** — When RMON thresholds in the switch are exceeded no trap is generated.
- **SNMP (PR_1000212170)** — The Switch transmits Warm and Cold Start traps with an agent address of 0.0.0.0.
- **SNMP (PR_1000190654)** — Some of the fault finder events in the SNMP traps list a 0.0.0.0 IP address in the URL. This happens when the switch has the IP address configured on a VLAN other than the default.
- **SNTP (PR_1000199632)** — NTP (SNTP) Some ProCurve switches on certain code levels will not accept a good NTP version 4 broadcast. Same switches can learn time from version 3 broadcast or version 4 unicast.
- **SNMP (PR_1000086062)** - SNMP Sets allowed in Operator mode and IP Authorized-Manager is set.
- **Web UI (PR_1000191635)** - The Port column may not be sorted correctly in all Web user interface screens.
- **Web UI (PR_93721)** - Scroll bar does not work in Web Status screen.
  In the web user interface, the Status screen does not display all ports.

Release H.07.54

Problems Resolved in Release H.07.54

- **Auto TFTP (PR_1000187649)** — Auto-TFTP will not allow a forced download of software after Auto-TFTP is Disabled.
- **Auto TFTP/Rebooting (PR_1000020802)** — Auto-TFTP causes constant rebooting, with no resulting crash files.
- **Switching (PR_1000022819)** — Bringing up a trunk port flushes the addresses in the MAC address table that are located on the next higher-numbered port, which results in unexpected flooding.

Release H.07.53

Release numbers H.07.51 and H.07.52 were never released.

Problems Resolved in Release H.07.53

- **Switching (PR_1000022819)** — Bringing up a trunk port flushes the addresses in the MAC address table that are located on the next higher-numbered port, which results in unexpected flooding.

- **TELNET (PR_1000019573)** — Switch reboots when TELNET is disabled and port 1506 is accessed. When the switch reboots there is no error listed in the log or in the boot history of the switch.

Release H.07.50

Release numbers H.07.47 through H.07.49 were never released.

Problems Resolved in Release H.07.50

- **CLI (PR_82086)** — Command **show mac <mac-address>** does not work.
- **CLI (PR_1000005082)** — If GVRP is enabled, an incorrect error message of `Commit Failed` is generated when trying to add more than the configured "max vlans" in the CLI. The proper error message should be `Maximum number of VLANs (max-vlans) has already been reached`. Dynamically created VLANs were not being included in the count.
- **Crash(PR_1000012823)** — OpenSSL vulnerability addressed.
- **Flow Control (PR_98957)** — Flow Control mechanism was not generating Pause frames.

  Limitations for this fix:

  Due to interactions with setting QoS priorities on inbound packets, some packets will be dropped in order to preserve the Queue Priorities when a 4:1 or higher oversubscription of 100- or 1000-Mbps ports have streams flowing to another 100- or 1000-Mbps port.

  100-Mbps ports to 10-Mbps ports works correctly.

  Workaround: Do not use Flow Control and QoS priorities simultaneously.

  2650 (J4899A) and 2650-PWR (J8165A) switches only:

  If an ingress port in the range of ports 1-24 and 49 are overflowing an egress port in the range of 25-48 and 50, a Pause Frame will NOT be generated out the ingress port.
- **Link (PR_1000020645)** — 2626 port 25 with a fiber link does not work after reset; also applies to the 6108 port 7.
- **PoE (PR_1000004040)** — Event log message `system: PoE controller selftest failure` occurs when a system is rebooting while powered by an external power supply (HP 600, J8168A).
- **RMON (PR_1000011690)** — When RMON thresholds in the switch are exceeded, no trap is generated.

- **Web (PR_1000003580)** — In the Diagnostics/LinkTest page, the Web interface allows broadcast/multicast MAC destination addresses. The CLI does not allow them. For consistency and because they should not be used, the Web interface should be changed to not allow them either.
- **Web (PR_1000004111)** — Stack Management view, scrolling problem.
- **Web (PR_1000007144)** — VLAN Configuration help link is not available.

Release H.07.46

Problems Resolved in Release H.07.46

- **(PR_1000004025)** — System Uptime counter wrapped in approx. 49 days.

Release H.07.45 (Never Released)

Release numbers H.07.42 through H.07.44 were never created.

Problems Resolved in Release H.07.45

- **CLI (PR_97671)** — Uncertain error message when trying to add more than the maximum VLANS
- **Crash (PR_95525)** — Switch is crashing with a bus error from the instrumentation data structure.

  Crash msg: `Bus error: HW Addr=0xe1f08796 IP=0x003a51b4 Task='mInstCtrl' Task I  D=0x1767af8  fp: 0x00000006 sp:0x01767988 lr:0x003979a4`
- **IP Stacking(PR_97323)** — back-of-box stacking support for all current stackable products
- **Port Security (PR_98193)** — "port-security learn-mode configured "is not working properly
- **RSTP (PR_1000001612)** — Port takes ~30 seconds to go into the Forwarding state
- **Web (PR_81848)** — Clear changes button does not work for the Default Gateway or VLAN selections
- **Web (PR_82039)** — When using the Web agent and you select GVRP mode, a user can select a port and then select nothing as an option for the port mode and all ports below the selected port disappear.
- **Web (PR_82199)** — VLAN port modification shows misleading mode
- **Web (PR_92078)** — After making changes under the Device Features tab, Web page never fully loads.

- **Web Mgmt Crash(PR_92826)** — Commander switch for IP-stack / Web Mgmt Crash of commander. With an eight switch IP stack, using the Web interface can cause the commander switch to crash. If the user-administrator using the WEB interface selects options too quickly or moves from one option to another, the Web agent can freeze and become unresponsive. The commander can also crash with a Bus Error. Telnet and console interfaces both can also become unresponsive.
- **Web (PR_97407)** — Port security error message is unclear with mac lockdown feature
- **Web (PR_98500)** — Browser window spontaneously closes
- **Web (PR_1000000452)** — when you reset a device using the Web Browser, the refreshed page returns to a incorrect URL.

Release H.07.41

Release numbers H.07.33 through H.07.40 were never created.

Problems Resolved in Release H.07.41

- **Bridge Management (PR_82358)** — Switch was not forwarding multicast packets with address of 01-80-C2-00-00-10 reserved for Bridge Management functions.
- **Crash (PR_95850)** — software exception in ISR at hardware.c:3871
- **Link (PR_ 96223/95598)** — Mini-GBIC ports that were configured to a forced speed/duplex (vs. 'auto' mode) were incorrectly reporting Link state when there were no fiber links connected.
- **Management (PR_92720)** — Switch 'show CPU' reports 136 percent busy. The calculation for CPU busy was being performed incorrectly.
- **Port Security (PR_88612)** — Port security enabled via the MIB hpSecPtLearnMode was improperly filtering a host MAC entry, when the entry was removed via the CLI, SNMP or Web interface.
- **Web (PR_82652)** — Web agent showing disabled ports as "Port Not Connected."

Release H.07.32

Problems Resolved in Release H.07.32

- **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.

- **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
  ```

- **Web Browser (PR_90068)** — There is a Netscape 4.7, 7.0, and 7.1 problem when changing any attribute in the stacking menu. After clicking 'OK', Netscape returns error "The document contains no data. Try again later."

Release H.07.31

Release numbers H.07.04 through H.07.30 were never created. Release H.07.31 is the first software release for the HP ProCurve Switch 2626.

Problems Resolved in Release H.07.31

- **CLI (PR_81948) —** A duplicate "enable" command is present in the Interface Configuration text within the CLI.
- **CLI (PR_82475) —** Within the CLI, the "ip" auto-extend help text for "source-route" is incorrect.
- **Config / Switch Management (PR_89846) —** When the "no web-management" command is executed, "no telnet-server" is also added to the running config. A loss of Telnet connectivity is only seen when the config file is saved to a TFTP server, then copied back.
- **IGMP (PR_90376) —** In some cases, the switch would display "0.0.0.0" for the output of the CLI command "show ip igmp."
- **IP Stack Mgmt/Web (PR_89753) —** A bus error occurs when accessing the close-up view of a 15-member stack (IP Stack Management) through the Web interface.
- **IP Routing (PR_90711) —** Switch incorrectly identifying packets routed from a trunk port across the stack link as port security violations. This resulted in overrunning the CPU queues and causing management problems.
- **QOS (PR_90937) —** Switch only utilizing three of the four available priority queues.
- **Spanning Tree (PR_90412) —** Enhancements to 802.1w operation to address version 3 BPDU communication issues.
- **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.
- **UI / CLI (PR_90302) —** Addressed grammatical errors for the "interfaces" command when "show <tab>" is executed.

- **UI (PR_81885) —** In the absence of a time server, the switch may report that it is the year "26".
- **Web/Stack Mgmt (PR_88743) —** Inverted IP address displayed in the Identity tab when the IP Stack Member switch is accessed through the IP Stack Commander switch.
- **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.
- **Web-Browser Interface (PR_82652) —** The Web agent is showing disabled ports as "Port Not Connected", rather than "Port Disabled."
- **Web-Browser Interface / Port Security (PR_88612) —** When static MAC addresses are configured under port security to allow PCs to communicate through the switch, and one of those MAC addresses is removed via the Web interface of the 2650 and then re-entered, the owner of that MAC address cannot communicate again until the link of that port is toggled.

Release H.07.03

Problems Resolved in Release H.07.03

- **Agent Unresponsive (PR_5903) —** The switch may get into a state where end nodes and other network devices cannot contact (ping, telnet, SNMP, etc) switch's agent.
- **Crash (PR_5877) —** When setting the host name to a very long (~20 characters) string, the switch may crash with a bus error similar to:

  ```
  -> Bus error:  HW Addr=0x29283030 IP=0x002086ac Task='mSnmpCtrl' Task
  ID=0x165ae00.
  ```

- **Crash (PR_5345) —** Switch may crash with a message similar to:

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

- **IGMP (PR_5991) —** If switch receives an IGMPv3 Join with a reserved Multicast address, or an invalid IP Multicast address, the switch may crash with a message similar to:

  ```
  -> Software exception at alloc_free.c:479 -- in 'tDevPollTx' Task ID =
  0x1900f18 buf_free: corrupted buffer
  ```

- **IGMP (PR_6001) —** When an IGMP v3 Join contains an invalid IP Multicast address or a reserved IP Multicast address in the IGMP Group Address field, the switch will attempt to stop processing the Join, and mistakenly double-free, or double-forward the Join packet. One possible symptom is a switch crash similar to:

  ```
  ->Software exception at alloc_free.c ... buf_free: corrupted buffer
  ```

- **SNMP (PR_6006) —** The ifAlias OID is defaulted to "not assigned", which may cause network management applications such as Network Node Manager to log error messages. [The fix is to default ifAlias to a zero-length string, as stated in the MIB.]

Release H.07.02

Release H.07.02 was the first software release for the HP ProCurve Switches 2650 and 6108.

Known Software Issues and Limitations

There are no known issues at this time.

Limitations

Displaying the Fast-Leave Setting on a Port

Use the **walkmib** command, below, to display this setting for all switch ports or the ports on a specified VLAN.

Syntax:

walkmib hpSwitchIgmpPortFastLeaveState<.*vlan number*>

```
HPswitch(vlan-1)# walkmib hpswitchigmpportfastleavestate.1
hpSwitchIgmpPortFastLeaveState.1.1 = 1
hpSwitchIgmpPortFastLeaveState.1.2 = 2
hpSwitchIgmpPortFastLeaveState.1.3 = 1
hpSwitchIgmpPortFastLeaveState.1.4 = 2
hpSwitchIgmpPortFastLeaveState.1.5 = 1
hpSwitchIgmpPortFastLeaveState.1.6 = 2
```

The **2** at the end of a port listing shows that Fast-Leave is **disabled** on the corresponding port.

The **1** at the end of a port listing shows that Fast-Leave is **enabled** on the corresponding port.

Internal VLAN Number for the Default VLAN

Note: Internal VLAN numbers reflect the sequence in which VLANs are created, and are not related to the unique VID assigned to each VLAN.

Sequential Port Numbers (not all ports shown here)

(This page is intentionally unused)

August 2005

Manual Part Number
5990-6003