Release Notes:
Version E.07.2x Software
for the HP Procurve Series 5300XL Switches

Release E.07.2*x* supports these switches:

- HP Procurve Switch 5304XL (J4850A)
- HP Procurve Switch 5308XL (J4819A)
- HP Procurve Switch 5348XL (J4849A) – 48-port bundle in Switch 5304XL chassis
- HP Procurve Switch 5372XL (J4848A) – 72-port bundle in Switch 5308XL chassis

These release notes include information on the following:

- Downloading switch software and Documentation from the Web
- Software features available in release E.07.2*x*
- Clarification of operating details for certain software features
- A listing of software fixes included in release E.06.01 through E.07.21

Caution

The startup-config file saved under version E.07.21 or greater, is NOT backward-compatible with previous software versions. Users are advised to save a copy of the pre-E.07.21 startup-config file BEFORE UPGRADING to E.07.21 or greater, in case there is ever a need to revert to pre-E.07.21 software. Instructions for saving a copy of the startup-config file are found 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 HP Procurve website. (Refer to “To Download Product Documentation:” on page 1.)

Publication Number

5990-3084
January 2003
Edition 1

Applicable Product

HP Procurve Switch 5304XL (J4850A)
HP Procurve Switch 5308XL (J4819A)
HP Procurve Switch 5348XL (J4849A)
HP Procurve Switch 5372XL (J4848A)

Trademark Credits

Microsoft, Windows, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems, Inc. Sun® and Java™ Virtual Machine are trademarks or registered trademarks 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.hp.com/go/hpprocurve

Disclaimer

The information contained in this document is subject to change without notice.

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.

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

Software Management

Downloading Switch Documentation and Software from the Web

You can download software updates and the corresponding product documentation from HP's Procurve website as described below.

To Download a Software Version:

1. Go to HP's Procurve website at:

   http://www.hp.com/go/hpprocurve.

2. Click on **software** (in the sidebar).
3. Under **latest software**, click on **switches**.

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

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

Downloading Software to the Switch

Caution

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

HP periodically provides switch operating system (OS) updates through the HP Procurve website (**http://www.hp.com/go/hpprocurve**). After you acquire the new OS file, you can use one of the following methods for downloading the operating system (OS) code 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).
- HP's SNMP Download Manager included in HP TopTools for Hubs & Switches
- A switch-to-switch file transfer

Note

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

This section describes how to use the CLI to download an OS to the switch. You can also use the menu interface for OS 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 an OS file named E_05_04.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  E_05_02.swi
Device will be rebooted, do you want to continue [y/n]?  y
00224K _
```

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

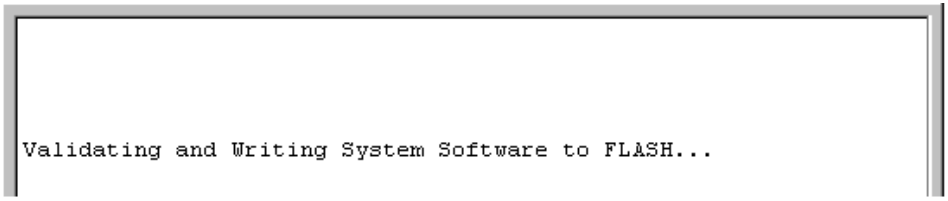

Figure 1. Message Indicating the Switch Is Writing the Downloaded Software to Flash Memory

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

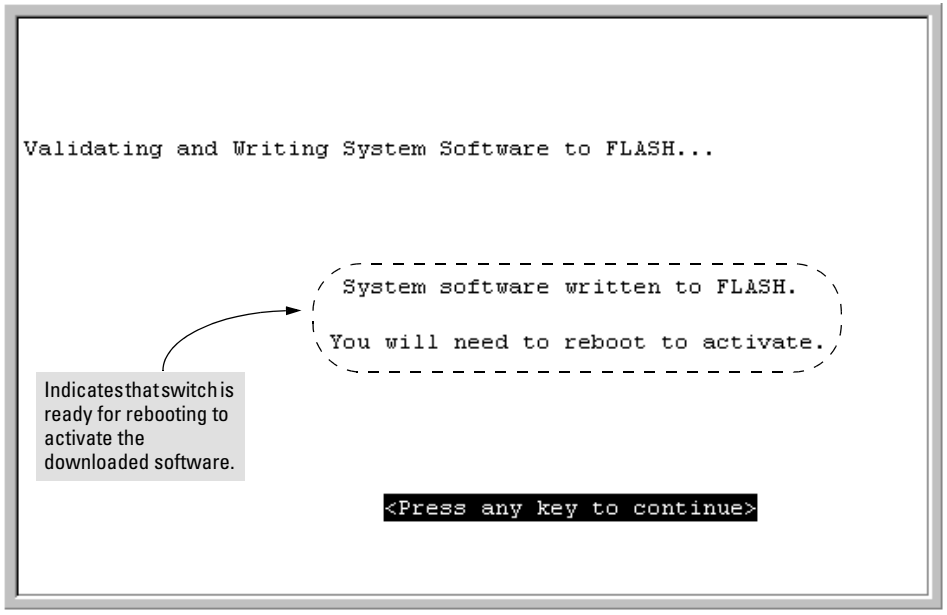

Figure 2. Message Indicating the Switch Is Ready To Activate the Downloaded Software

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 operating system (OS) 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 an OS file from a PC:

1. To reduce the download time, you may want to increase the baud rate in your terminal emulator and in the switch to a value such as 57600 bits per second. (The baud rate must be the same in both devices.) For example, to change the baud rate in the switch to 57600, execute this command:

   ```
   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 OS version.

4. To confirm that the operating system downloaded correctly:

   ```
   HPswitch> show system
   ```

   Check the **Firmware revision** line.

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

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

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] ?
```

HP Procurve Switch Software Key

Software Letter	HP Procurve Switch
C	1600M, 2400M, 2424M, 4000M, 8000M
E	Series 5300XL (5304XL and 5308XL)
F	Series 2500 (2512 and 2524)
G	Series 4100GL (4104GL and 4108GL)
H	Switch 2650 and Switch 6108

Clarifications

Clarification of Time Zone Issue

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

Clarification of Heterogenous Switch Meshing

When the Series 5300XL switches are placed in backward-compatibility mode, they can operate in switch mesh domains that include HP Procurve 1600M, 2400M, 2424M, 4000M, and 8000M switches. However, such domains must be free of duplicate MAC addresses on multiple switches and different VLANs. Refer to figures 3 and 4:

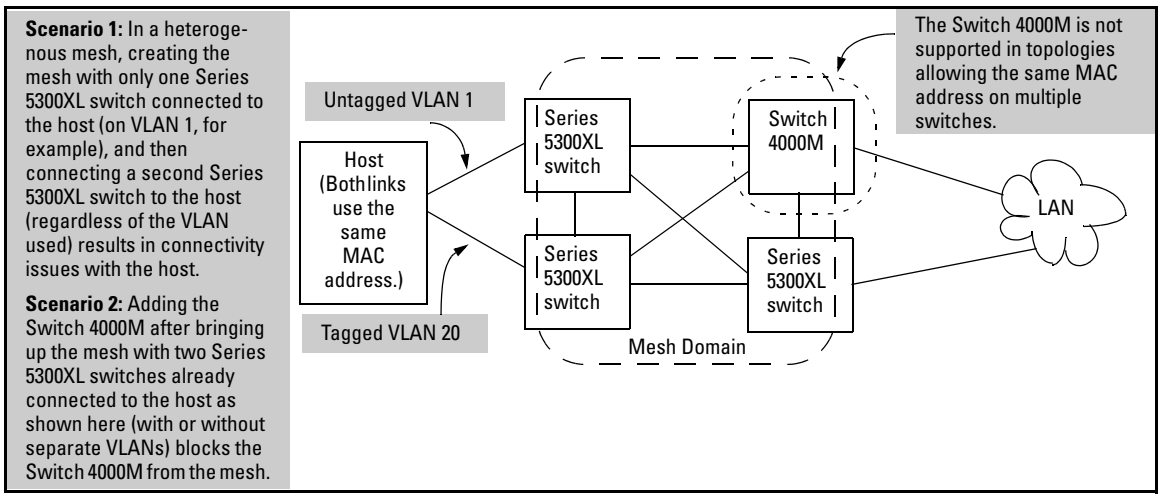

Figure 3. Example of an Unsupported Heterogenous Topology Where Duplicate MAC Addresses Come Through Different Switches (Regardless of the VLANs Used)

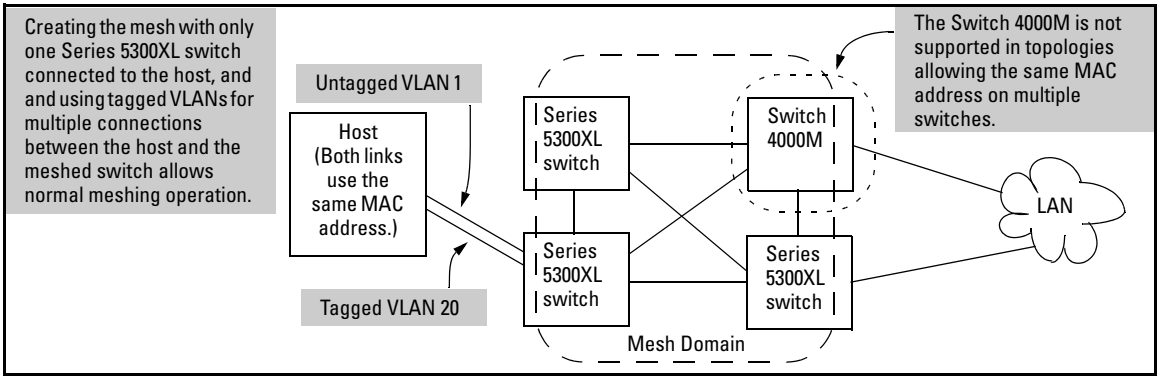

Figure 4. Example of a Supported Heterogenous Topology Where Duplicate MAC Addresses Come Through Different VLANs on the Same Switch

Note that in figures 3 and 4, if all switches are Series 5300XL switches, then you can use either topology.

Web Agent May Not Respond To JVM 1.3 or 1.4

The HP Procurve web browser interface may not respond to the Sun® Java™ Virtual Machine 1.3 or 1.4. The switch web agent supports the following combinations of browsers and virtual machines:

Operating System	Browser	Virtual Machine
Windows NT 4.0 SP6	Internet Explorer 5.00.3502.1000 SP3	Microsoft VM 5.00 Build 5.0.3809.0
Windows NT 4.0 SP6	Internet Explorer 5.50.4807.2300CO SP2	Microsoft VM 5.00 Build 5.0.3809.0
Windows NT 4.0 SP6	Internet Explorer 6.0.2800.1106 SP1	Microsoft VM 5.00 Build 5.0.3809.0
Windows 2000 SP3	Internet Explorer 5.00.3502.1000 SP3	Microsoft VM 5.00 Build 5.0.3809.0
Windows 2000 SP3	Internet Explorer 5.50.4807.2300CO SP2	Microsoft VM 5.00 Build 5.0.3809.0
Windows 2000 SP3	Internet Explorer 6.0.2800.1106 SP1	Microsoft VM 5.00 Build 5.0.3809.0
Windows XP SP1	Internet Explorer 6.0.2800.1106 SP1	Microsoft VM 5.00 Build 5.0.3809.0

Enhancements

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

Release E.07.21 Enhancements

To Locate Documentation Supporting E.07.21 Features:

1. Go to HP's ProCurve website at **http://www.hp.com/go/hpprocurve.**
2. Click on **technical support**, then **manuals**.
3. Click on the name of the product for which you want documentation.
4. Select the document indicated in the enhancement description (below) for the desired feature.

(HP recommends periodically visiting the HP Procurve website to keep up-to-date with the latest documentation available for HP Procurve Series 5300XL switch products.)

- **Access Control Lists (ACLs) —** Layer 3 IP filtering with ACLs enables you to improve network performance and restrict network use by creating policies for switch management access and application access security. (Refer to the *Manual Suplement for the HP Procurve Series 5300XL Switches*, Edition 1—5990-3083, January 2003.)
- **Debug and Syslog Messaging Operation —** These features provide a method for recording messages you can use to hellp in debugging network-level problems such as routing misconfigurations and other network protocol details. (Refer to the *Manual Suplement for the HP Procurve Series 5300XL Switches*, Edition 1—5990-3083, January 2003.)
- **SNMPv3 —** The Series 5300XL switches now support SNMPv3 to enhance the security of SNMPv3 traffic. It include authentication and/or encryption of Management traffic configurable at the operators discretion. (Refer to the *Management and Configuration Guide for the HP Procurve Series 5300XL Switches*, Edition 5 — 5990-3016, January 2003.)
- **Meshing improvements —** The Series 5300XL switches now have improved meshing features. They include greater configuration checks for meshes with (only) Series 5300XL and backwards compatibility mode for reduced connect times with legacy meshing devices. (Refer to the *Management and Configuration Guide for the HP Procurve Series 5300XL Switches*, Edition 5 — 5990-3016, January 2003.)

  Note: If upgrading to this version of code the user must enter the backward compatibility mode command if connected to legacy devices.

- **OSPF Authentication —** Adds MD5 encryption for authenticating OSPF packets. Encryption keys are managed by a centralized Key Management System (KMS). (Refer to the *Management and Configuration Guide for the HP Procurve Series 5300XL Switches*, Edition 5 — 5990-3016, January 2003.)
- **IGMPv3 —** Adds support for the IGMPv3 Join request. (Refer to the *Management and Configuration Guide for the HP Procurve Series 5300XL Switches*, Edition 5 — 5990-3016, January 2003.)
- **SSHv2 —** Updates SSH to support SSHv2. This allows for the use of PEM encoded keys and greater compatibly to SSH client software. (Refer to the *Access Security Guide for the HP Procurve Series 5300XL Switches*, Edition 2—5990-3031, January 2003.)
- **SSL —** The Series 5300XL Switches now support Secure Socket Layer transactions for Web management access. This allows the switch to authenticate itself to the user and to establish a secure connection. There is support for self-signed and CA signed certificates to allow the administrator to choose the level of security required. (Refer to the *Access Security Guide for the HP Procurve Series 5300XL Switches*, Edition 2—5990-3031, January 2003.)
- **XRRP —** The feature used by the HP Procurve Series 5300XL switches to provide router redundancy or fail-over – a backup router in case one fails. XRRP is similar to the industry standard VRRP (Virtual Router Redundancy Protocol), although the details of the operation are different. (Refer to the *Management and Configuration Guide for the HP Procurve Series 5300XL Switches*, Edition 5 — 5990-3016, January 2003.)

Release E.06.10 Enhancements

Adds support for the J4852A HP Procurve Switch XL 100-FX MTRJ module.

Release E.06.05 Enhancements

There are no new enhancements in release E.06.05.

Release E.06.03 Enhancements

There are no new enhancements in release E.06.03.

Release E.06.02 Enhancements

There are no new enhancements in release E.06.02.

Release E.06.01 Enhancements

This section describes the features and feature changes added in release E.06.01. For information on other features available in your switch, refer to the following publications:

- *Management and Configuration Guide for the HP Procurve Series 5300GL Switches*
- *Access Security Guide for the HP Procurve Series 5300GL Switches*

For copies of the above guides, refer to either the *Product Documentation CD-ROM* shipped with the switch or (for the latest version of any HP switch documentation) visit the HP Procurve website. (See "To Download Product Documentation:" on page 1.)

Enhancement	Overview	Page
HP J4860A LH-LC Mini-GBIC	New mini-GBIC support for Series 5300XL switches.	11
New Flow Control Command	The Series 5300XL switches enable per-port flow control. Beginning with release E.06.0x, use the (global) Flow Control command to enable flow control on the switch, then enable flow control on the desired port(s).	11
Change in Default for RIP Redistribution of Connected Routes	Formerly, RIP redistributed both static and connected routes by default.	12
Change in Default State DHCP-Relay and Helper-Addresses	Changes the factory-default state of DHCP-Relay and describes how to determine the current state, as well as how to list Helper addresses.	13
Show Tech	Enhancements to this command enable more output options for troubleshooting information.	14
Trace Route	Provides a new feature for tracking the path of a packet between the switch and a destination IP address.	15
IP Address Command Change	This change simplifies multinetting on VLANs.	17
802.1x Open VLAN Mode (Authorized-Client and Unauthorized-Client VLANs)	Provides more flexibility for authenticating clients lacking 802.1x supplicant software, and an additional provision for controlling VLAN access by authenticated clients.	19

Support Added for the Long-Haul Mini-GBIC

Beginning with release E.06.0x, the Series 5300XL switches now support the HP J4860A LH-LC Mini-GBIC. To use this mini-GBIC, install it in the (optional) HP ProCurve Mini-GBIC XL module (J4878A) and install the module in an HP ProCurve Series 5300XL switch running software release E.06.0x (or greater). For installation instructions, refer to the *HP ProCurve Switch XL Modules Installation Guide* shipped with the module.

Enable (Global) Flow Control on the Switch Before Enabling Per-Port Flow Control

Flow control operates on a per-port basis. However, beginning with release E.06.0x, you must enable flow control globally on the switch before enabling it on individual ports. In the factory-default configuration, flow control is disabled.

Note

If you have enabled flow-control on individual ports while using software version E.05.04, but then downloaded software version E.06.01 (or greater) and rebooted the switch, flow control will be disabled globally on the switch (the default) and therefore will not operate on the individual ports previously configured to allow flow control. To resume the configured per-port flow-control activity, you must enable global flow control.

To enable flow control, use these commands:

Syntax: [no] flow-control

Execute this command on the global config level to enable flow-control on the switch.

[no] interface [e] < ***port-list*** > flow-control

After you enable global flow control on the switch, execute this command on a per-port basis to enable flow-control on individual ports.

show flow-control

Indicates whether global flow-control is enabled or disabled.

show config

Includes a listing of ports configured for flow control operation.

For example, if flow control is not enabled globally (the default) in the switch's current configuration and you wanted to enable flow control on ports B15 - B18, you would do the following:

```
HPswitch(config)# flow-control
HPswitch(config)# interface e b15-b18 flow-control
— or —
HPswitch(config)# interface e b15-b18
HPswitch(eth-b15-b18)# flow control
```

To disable flow control globally on the switch, you must first disable flow control on the individual ports. For example:

`HPswitch(eth-b15-b18)# no flow-control`

Disables flow control on the ports for which it is currently configured.

`HPswitch(eth-b15-b18)# exit`

Returns switch to global configuration level.

`HPswitch(config)# no flow-control`

Disables flow control on the switch. (Per-Port Flow Control must already be disabled for all ports.)

`HPswitch(config)# write memory`

Saves the configuration change to the startup-config file.

IP Routing Features

Change in Default Operation for RIP Redistribution of Static Routes

In software release E.05.04 (the initial Series 5300XL software), the factory-default RIP operation automatically redistributes both connected routes and static routes. Beginning with software release E.06.0x, the factory-default RIP operation automatically redistributes connected routes, but not static routes. To enable redistribution of static routes, use this command sequence:

```
HPswitch(config)# router rip
HPswitch(rip)# redistribution static
HPswitch(rip)# write memory
```

To view the currently configured RIP Redistribution, use this command:

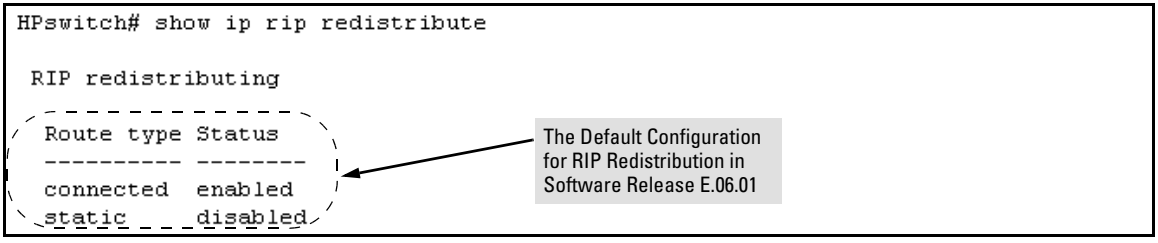

Figure 5. Listing the Current Configuration for RIP Redistribution

Change and Clarification for DHCP-Relay

Change in Factory-Default Configuration. In software release E.05.04 (the initial Series 5300XL software), the factory-default configuration *disables* DHCP-Relay. Also, with DHCP-Relay disabled, the show config command did not list this state (because it was the default state for DHCP-Relay).

Beginning with release E.06.01, the opposite is true. That is, the factory-default configuration *enables* DHCP-Relay. Also, with DCHP-Relay enabled, the **show config** command does not list this state because it is now the default state for DHCP-Relay.

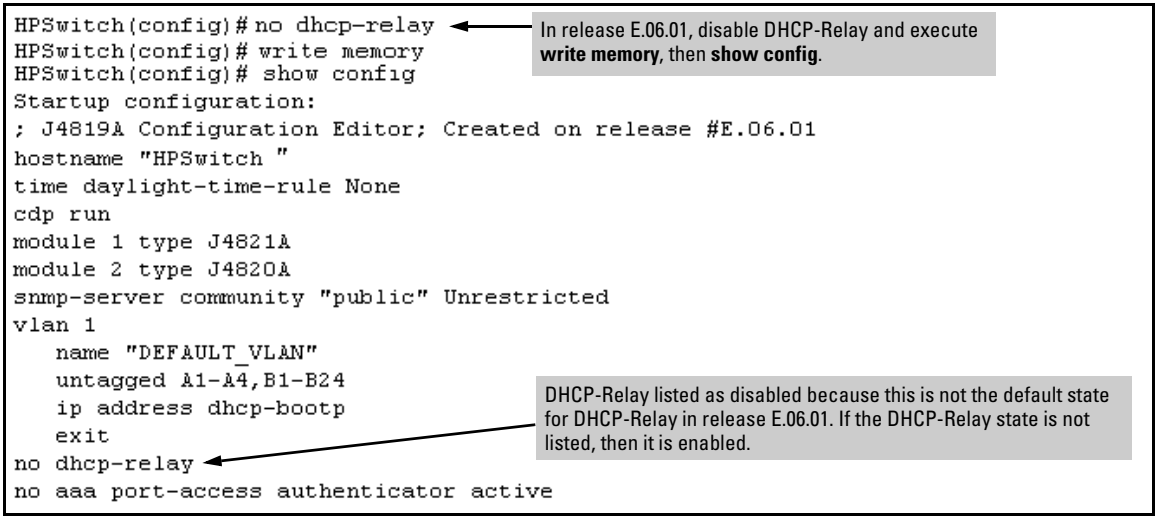

Figure 6. DHCP-Relay State Appears in Show Config Output when Disabled

With DHCP-Relay disabled, if you upgrade from release E.05.04 to E.06.01, then reboot the switch, DHCP-Relay becomes enabled. (However, to use DHCP-Relay, you will still need to configure IP Helper addresses.)

Listing DHCP-Relay Helper Addresses.

Syntax: show ip helper-address < ***vlan-id*** >

This command shows the currently configured IP Helper addresses, regardless of whether DHCP-Relay is enabled. For example:

```
HPswitch(config)# show ip helper-address vlan 1
 IP Helper Addresses
  IP Helper Address
  -----------------
  10.28.227.97
  10.29.227.53
```

Figure 7. Example of Listing for IP Helper Addresses

To determine the current state (enabled or disabled) for DHCP-Relay, refer to figure 6.

Enhancements for Troubleshooting

The **show tech** command generates output that Hewlett-Packard Support staff may request when troubleshooting networking problems. Release E.06.01 provides four new enhancements to this command:

Syntax: show tech

[all]

Generates general system-level and feature information useful to HP support staff for analyzing various areas of switch operation.

[buffers]

Generates packet and message buffer information useful to HP support staff for analyzing chassis and slot operation.

[mesh]

Generates meshing-related information useful to HP support staff for analyzing meshing operation.

[route]

Generates routing-related output useful to HP support staff for analyzing routing operation.

If requested by HP support staff, execute show tech and its options at the Manager level in the CLI. For example:

```
HPswitch# show tech
```

To copy the output to a text file, use **copy command-output < tftp | xmodem >**. (Refer to the "Trouble-shooting" appendix in the *Management and Configuration Guide* for your switch. This guide is included on the Documentation CD-ROM shipped with the switch, and is also available on the HP ProCurve website—refer to “Downloading Switch Documentation and Software from the Web” on page 1.)

Traceroute Command

The new **traceroute** command enables you to trace the route from the switch to a host address.

This command outputs information for each (router) hop between the switch and the destination address. Note that every time you execute **traceroute**, it uses the same default settings unless you specify otherwise for that instance of the command.

Syntax: traceroute < ***ip-address*** >

Lists the IP address of each hop in the route, plus the time in microseconds for the **traceroute** packet reply to the switch for each hop.

To halt an ongoing tracerout search, press the [illegible] keys.

[minttl < 1-255 >]

For the current instance of **traceroute**, *changes the minimum number of hops allowed for each probe packet sent along the route. If* **minttl** *is greater than the actual number of hops, then the output includes only the hops at and above the* **minttl** *threshold. (The hops below the threshold are not listed.) If* **minttl** *matches the actual number of hops, only that hop is shown in the output. If* **minttl** *is less than the actual number of hops, then all hops are listed. For any instance of* **traceroute,** *if you want a* **minttl** *value other than the default, you must specify that value. (Default: 1)*

[maxttl < 1-255 >]

For the current instance of **traceroute**, *changes the maximum number of hops allowed for each probe packet sent along the route. If the destination address is further from the switch than* **maxttl** *allows, then* **traceroute** *lists the IP addresses for all hops it detects up to the* **maxttl** *limit. For any instance of* **traceroute,** *if you want a* **maxttl** *value other than the default, you must specify that value. (Default: 30)*

[timeout < 1-120 >]

For the current instance of **traceroute**, *changes the timeout period the switch waits for each probe of a hop in the route. For any instance of* **traceroute,** *if you want a* **timeout** *value other than the default, you must specify that value. (Default: 5 seconds)*

[probes < 1-5 >

For the current instance of **traceroute**, *changes the number of queries the switch sends for each hop in the route. For any instance of* **traceroute,** *if you want a* **probes** *value other than the default, you must specify that value. (Default: 3)*

A Low Maxttl Causes Traceroute To Halt Before Reaching the Destination Address. For example, executing **traceroute** with its default values for a destination IP address that is four hops away produces a result similar to this:

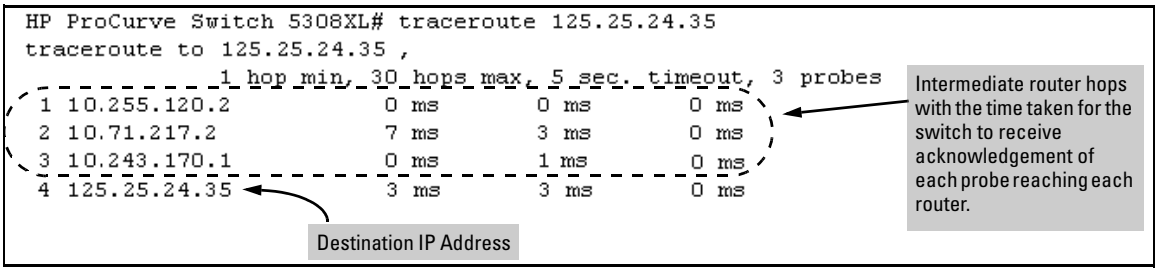

Figure 8. Example of a Completed Traceroute Enquiry

Continuing from the previous example (figure 8, above), executing **traceroute** with an insufficient **maxttl** for the actual hop count produces an output similar to this:

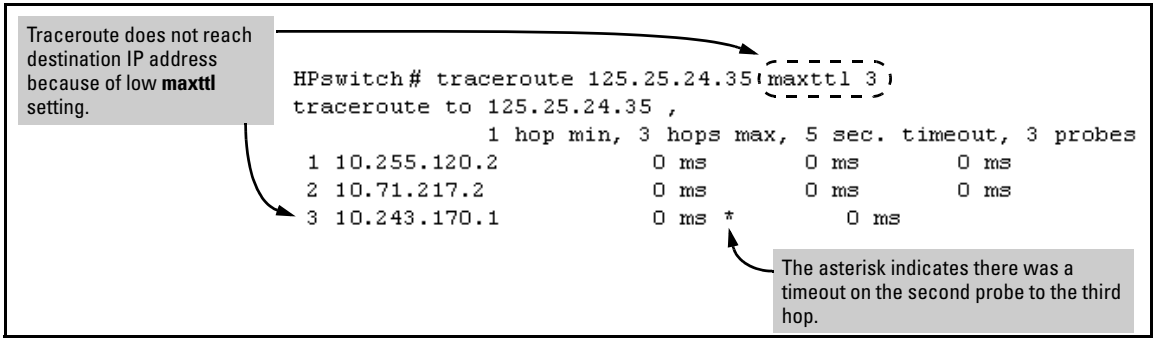

Figure 9. Example of Incomplete Traceroute Due to Low Maxttl Setting

If A Network Condition Prevents Traceroute from Reaching the Destination. Common reasons for Traceroute failing to reach a destination include:

- Timeouts (indicated by one asterisk per probe, per hop; see figure 9, above.)
- Unreachable hosts
- Unreachable networks
- Interference from firewalls
- Hosts configured to avoid responding

Executing traceroute where the route becomes blocked or otherwise fails results in an output marked by timeouts for all probes beyond the last detected hop. For example with a maximum hop count of 7 (**maxttl** = 7), where the route becomes blocked or otherwise fails, the output appears similar to this:

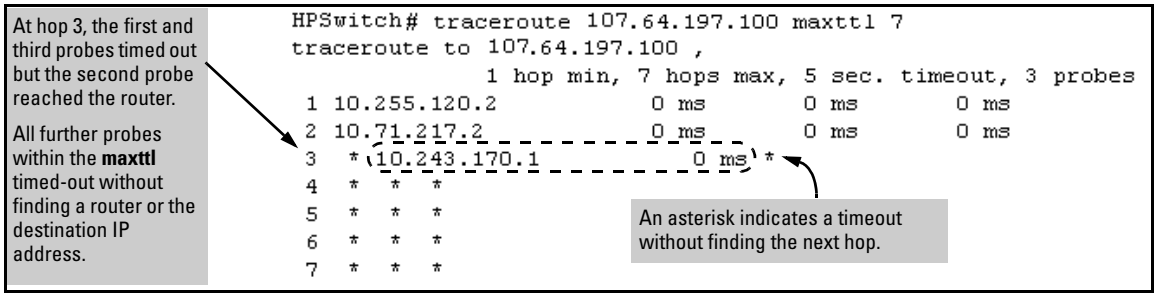

Figure 10. Example of Traceroute Failing to Reach the Destination Address

Change in Command for Configuring Multiple IP Addresses on a VLAN (Multinetting)

The method for configuring multiple IP addresses on a VLAN (multinetting) has changed. In release E.05.04, **secondary** was appended to the **ip address** command to add addresses after the primary address. Beginning with release E.06.01, the command for configuring the primary address and additional addresses is the same.

1. The first IP address you configure on a VLAN is the primary address.
2. Any other IP addresses you subsequently configure on the same VLAN are secondary.

Also, the **show ip secondary** command has been removed.

Syntax: vlan < ***vlan-id*** > ip address < ***ip-address*** >/< ***mask-length*** >

Configures an IP address and subnet mask. (The mask is specified by octets, such as 255.255.252.0).

vlan < ***vlan-id*** > ip address < ***ip-address*** >/< ***mask-bits*** >

Configures an IP address and subnet mask. (The mask is specified by total bits in the mask, such as 22 for a mask using these octets: 255.255.252.0).

show ip

Displays the current IP address configuration for all VLANs configured in the switch.

Note that the Internet (IP) Service screen in the Menu interface displays only the primary IP address for each VLAN. You must use the CLI to display the full IP address listing for multinetted VLANs.

For example, to configure a primary IP address for VLAN 1, and then multinet the VLAN with two more IP addresses, you would execute commands similar to the following:

```
HPswitch(config)# vlan 1 ip address 10.10.10.1/255.255.252.0
HPswitch(config)# vlan 1 ip address 10.10.20.1/255.255.252.0
```

To list all IP addresses configured on all VLANs in the switch, use **show ip**. For example:

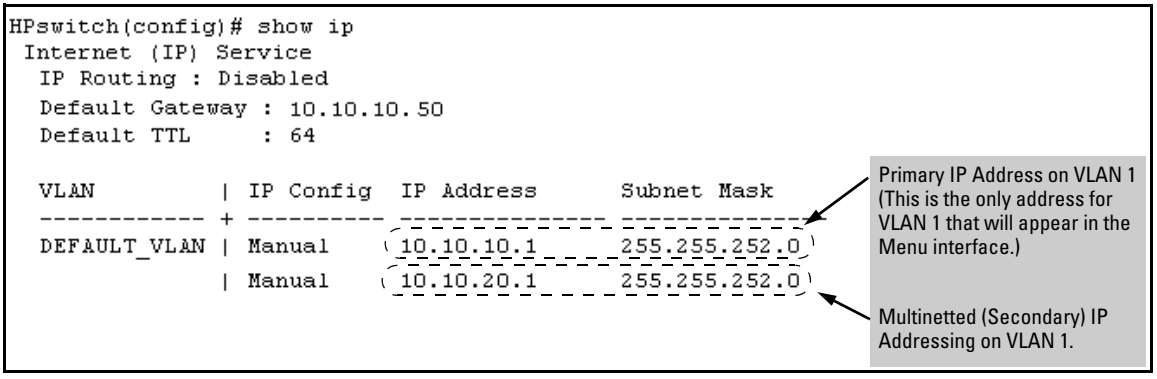

Figure 11. Example of IP Address Listing for a Multinetted VLAN

You can configure up to eight IP addresses per VLAN; one primary and up to seven secondary, or multinetted addresses. The switch allows up to 512 secondary subnet address assignments. For more information, refer to the chapter titled "Configuring IP Addressing" in the *Management and Configuration Guide* for your switch. (A copy of this manual is included on the *Documentation CD-ROM* shipped with the switch and also available from the HP ProCurve website. See “Downloading Switch Documentation and Software from the Web” on page 1.)

Note

In the **show ip** listing, the primary IP address for any VLAN is always the first address listed for that VLAN. In figure 11, the primary IP address is 10.10.10.1.

DHCP and Bootp configure only a primary IP address, and not any secondary addresses. If the switch receives an IP address from a DHCP or Bootp server, it assigns the address to the Primary VLAN. In the switch’s default configuration, the Primary VLAN and the Default VLAN (VID = 1) are the same VLAN.

802.1x Open VLAN Mode (Unauthorized-Client and Authorized-Client VLANs)

This section describes how to use the new Open VLAN Mode on ports configured as 802.1x authenticators. For more information on 802.1x, refer to the *Access Security Guide* included on the *Documentation CD-ROM* shipped with your switch and also available on the HP ProCurve website. (See "Downloading Switch Documentation and Software from the Web" on page 1.)

Note

Using this feature requires an understanding of 802.1x Authentication operation on your switch, as well as VLAN operation. If you are unfamiliar with these topics, refer to the *Access Security Guide* and the *Management and Configuration Guide* included on the *Documentation CD-ROM* shipped with your switch and also available on the HP ProCurve website. (To view or download the latest version, see "Downloading Switch Documentation and Software from the Web" on page 1.)

Command	Page	Type
[no] aaa port-access authenticator [e] < ***port-list*** >	29	Original
unauth-vid < ***vlan-id*** >	29	Enhancement
auth-vid < ***vlan-id*** >	29	Enhancement
show port-access authenticator < ***port-list*** >	30	Changed
show vlan < ***vlan-id*** >	31	Changed

Introduction

Configuring the 802.1x Open VLAN Mode on a port changes how the port responds when it detects a new client. Prior to release E.06.01, a "friendly" client computer not running 802.1x supplicant software could not be authenticated on a port protected by 802.1x access security. As a result, the port would become blocked and the client could not access the network. This prevents the client from:

- Acquiring IP addressing from a DHCP server
- Downloading the 802.1x supplicant software necessary for an authentication session

The 802.1x Open VLAN Mode solves this problem by temporarily suspending the port's static, untagged VLAN membership and placing the port in a designated *Unauthorized-Client VLAN*. In this state the client can proceed with initialization services, such as acquiring IP addressing and 802.1x

software, and starting the authentication process. Following authentication, the port drops its temporary (untagged) membership in the Unauthorized-Client VLAN and joins (or rejoins) *one* of the following as an *untagged* member:

- **1st Priority:** A VLAN to which the port has been assigned by a RADIUS server during authentication
- **2nd Priority:** If RADIUS authentication does not include assigning a VLAN to the port, then use the VLAN entered in the port's 802.1x configuration as an *Authorized-Client* VLAN
- **3rd Priority:** If the port does not have an Authorized-Client VLAN, but does have a static, untagged VLAN membership in its configuration, then use this VLAN.

If the port is not configured for any of the above, then it must be a tagged member of at least one VLAN. In this case, if the client is capable of operating in a tagged VLAN, then it can access that VLAN. Otherwise, the connection will not work.

Caution

If a port is a tagged member of a statically configured VLAN, 802.1x Open VLAN Mode does not prevent unauthenticated client access to such VLANs if the client is capable of operating in a tagged VLAN environment. To avoid possible security breaches, HP recommends that you not allow a tagged VLAN membership on a port configured for 802.1x Open VLAN Mode unless you use the tagged VLAN as the Unauthorized-Client VLAN.

Terminology

Authorized-Client VLAN: Like the Unauthorized-Client VLAN, this is a conventional, static VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network services that are not available on either the port's statically configured VLAN memberships or any VLAN memberships that may be assigned during the RADIUS authentication process. While an 802.1x port is a member of this VLAN, the port is untagged. When the client connection terminates, the port drops its membership in this VLAN.

Friendly Client: A client that does not pose a security risk if given access to the switch and your network.

PVID (Port VID): This is the VLAN ID for the untagged VLAN to which an 802.1x port belongs..

Tagged VLAN Membership: This type of VLAN membership allows a port to be a member of multiple VLANs simultaneously. If a client connected to the port has an operating system that supports 802.1q VLAN tagging, then the client can access VLANs for which the port is a tagged member. If the client does not support VLAN tagging, then it can access only a VLAN for which the port

is an untagged member. (A port can be an untagged member of only one VLAN at a time.) 802.1x Open VLAN Mode does not affect a port's tagged VLAN access unless the port is statically configured as a member of a VLAN that is also configured as the Unauthorized-Client or Authorized-Client VLAN. See also "**Untagged VLAN Membership**".

Static VLAN: A VLAN that has been configured as "permanent" on the switch by using the CLI **vlan < *vid* >** command or the Menu interface.

Unauthorized-Client VLAN: A conventional, static VLAN previously configured on the switch by the System Administrator. It is used to provide access to a client prior to authentication. It should be set up to allow an unauthenticated client to access only to the initialization services necessary to establish an authenticated connection, plus any other desirable services whose use by an unauthenticated client poses no security threat to your network. (Note that an unauthenticated client has access to all network resources that have membership in the VLAN you designate as the Unauthorized-Client VLAN.) An Unauthorized-Client VLAN for a given port does not have to have that port statically configured as a tagged or untagged member, as long as at least one port on the switch does have either a tagged or untagged membership in the VLAN.

Untagged VLAN Membership: A port can be an untagged member of only one VLAN. (In the factory-default configuration, all ports on the switch are untagged members of the default VLAN.) An untagged VLAN membership is *required* for a client that does not support 802.1q VLAN tagging. A port can simultaneously have one untagged VLAN membership and multiple tagged VLAN memberships . Depending on how you configure 802.1x Open VLAN Mode for a port, a statically configured, untagged VLAN membership may become unavailable while there is a client session on the port. See also "**Tagged VLAN Membership**".

Options for the 802.1x Open VLAN Mode

You can apply the 802.1x Open VLAN Mode in more than one way. Depending on your use, you will need to create one or two static VLANs on the switch for exclusive use by per-port 802.1x Open VLAN Mode authentication:

- **Unauthorized-Client VLAN:** Configure this VLAN when unauthenticated, friendly clients will need access to some services before being authenticated.
- **Authorized-Client VLAN:** Configure this VLAN for authenticated clients when the port is not statically configured as an untagged member of a VLAN you want clients to use, or when the port is statically configured as an untagged member of a VLAN you do not want clients to use. (A port can be configured as untagged on only one VLAN. When an Authorized-Client VLAN is configured, it will always be untagged and will block the port from using a statically configured, untagged membership in another VLAN.)

Table 1. 802.1x Open VLAN Mode Options

802.1x Per-Port Configuration	Port Response
No Open VLAN Mode:	The port automatically blocks a client that cannot initiate an authentication session.
Open VLAN Mode with both of the following configured:	
Unauthorized-Client VLAN	• When the port detects a client, it automatically becomes an untagged member of this VLAN. If you previously configured the port as a static, tagged member of the VLAN, membership temporarily changes to untagged while the client remains unauthenticated. • If the port already has a statically configured, untagged membership in another VLAN, then the port temporarily closes access to this other VLAN while in the Unauthorized-Client VLAN. • To limit security risks, the network services and access available on the Unauthorized-Client VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as a tagged member of any other VLANs, access to these VLANs remains open, even though the client may not be authenticated. Refer to the Caution on page 20.
Authorized-Client VLAN	• After the client is authenticated, the port drops membership in the Unauthorized-Client VLAN and becomes an untagged member of this VLAN. **Note:** if RADIUS authentication assigns a VLAN, the port temporarily becomes a member of the RADIUS-assigned VLAN — instead of the Authorized-Client VLAN—while the client is connected. • If the port is statically configured as a tagged member of a VLAN, and this VLAN is used as the Authorized-Client VLAN, then the port temporarily becomes an untagged member of this VLAN when the client becomes authenticated. When the client disconnects, the port returns to tagged membership in this VLAN. • If the port is statically configured as a tagged member of a VLAN that is not used by 802.1x Open VLAN Mode, an unauthenticated client capable of operating in tagged VLANs has access to this VLAN. Refer to the Caution on page 20.

802.1x Per-Port Configuration	Port Response
Open VLAN Mode with Only an Unauthorized-Client VLAN Configured:	
	• When the port detects a client, it automatically becomes an untagged member of this VLAN. To limit security risks, the network services and access available on this VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as an untagged member of another VLAN, the switch temporarily removes the port from membership in this other VLAN while membership in the Unauthorized-Client VLAN exists. • After the client is authenticated, and if the port is statically configured as an untagged member of another VLAN, the port's access to this other VLAN is restored. • If the port is statically configured as a tagged member of a VLAN that is not used by 802.1x Open VLAN Mode, an unauthenticated client capable of operating in tagged VLANs can access this VLAN. Refer to the Caution on page 20. **Note:** If RADIUS authentication assigns a VLAN to the port, this assignment overrides any statically configured, untagged VLAN membership on the port (while the client is connected).
Open VLAN Mode with Only an Authorized-Client VLAN Configured:	
	• Port automatically blocks a client that cannot initiate an authentication session. • If the client successfully completes an authentication session, the port becomes an untagged member of this VLAN. • If the port is statically configured as a tagged member of any other VLANs, an authenticated client capable of operating in a tagged VLAN environment can access these VLANs. **Note:** if RADIUS authentication assigns a VLAN, the port temporarily becomes a member of the RADIUS-assigned VLAN —instead of the Authorized-Client VLAN—while the client is connected.

Operating Rules for Authorized-Client and Unauthorized-Client VLANs

Condition	Rule
Static VLANs used as ***Authorized-Client*** or ***Unauthorized-Client*** VLANs	These must be configured on the switch before you configure an 802.1x authenticator port to use them. (Use the **vlan < *vlan-id* >** command or the VLAN Menu screen in the Menu interface.)
VLAN Assignment Received from a RADIUS Server	If the RADIUS server specifies a VLAN for an authenticated supplicant connected to an 802.1x authenticator port, this VLAN assignment overrides any Authorized-Client VLAN assignment configured on the authenticator port. This is because both VLANs are untagged, and the switch allows only one untagged VLAN membership per-port. For example, suppose you configured port A4 to place authenticated supplicants in VLAN 20. If a RADIUS server authenticates supplicant "A" and assigns this supplicant to VLAN 50, then the port can access VLAN 50 for the duration of the client session. When the client disconnects from the port, then the port drops these assignments and uses only the VLAN memberships for which it is statically configured.
Temporary VLAN Membership During a Client Session	• Port membership in a VLAN assigned to operate as the Unauthorized-Client VLAN is temporary, and ends when the client receives authentication or the client disconnects from the port, whichever is first. • Port membership in a VLAN assigned to operate as the Authorized-Client VLAN is also temporary, and ends when the client disconnects from the port.If a VLAN assignment from a RADIUS server is used instead, the same rule applies.
Effect of Unauthorized-Client VLAN session on untagged port VLAN membership	• When an unauthenticated client connects to a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Unauthorized-Client VLAN (also untagged). (While the Unauthorized-Client VLAN is in use, the port does not access the static, untagged VLAN.) • When the client either becomes authenticated or disconnects, the port leaves the Unauthorized-Client VLAN and reacquires its untagged membership in the statically configured VLAN.
Effect of Authorized-Client VLAN session on untagged port VLAN membership.	• When a client becomes authenticated on a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Authorized-Client VLAN (also untagged). While the Authorized-Client VLAN is in use, the port does not have access to the statically configured, untagged VLAN. • When the authenticated client disconnects, the switch removes the port from the Unauthorized-Client VLAN and moves it back to the untagged membership in the statically configured VLAN.

Condition	Rule
Multiple Authenticator Ports Using the Same Unauthorized-Client and Authorized-Client VLANs	You can use the same static VLAN as the Unauthorized-Client VLAN for all 802.1x authenticator ports configured on the switch. Similarly, you can use the same static VLAN as the Authorized-Client VLAN for all 802.1x authenticator ports configured on the switch. ***Caution: Do not use the same static VLAN for both the unauthorized and the Authorized-Client VLAN. Using one VLAN for both creates a security risk by defeating the isolation of unauthenticated clients.***
Effect of Failed Client Authentication Attempt	When there is an Unauthorized-Client VLAN configured on an 802.1x authenticator port, an unauthorized client connected to the port has access only to the network resources belonging to the Unauthorized-Client VLAN. (There can be an exception to this rule if the port is also a tagged member of a statically configured VLAN. Refer to the **Caution** on page 20.) This access continues until the client disconnects from the port. (If there is no Unauthorized-Client VLAN configured on the authenticator port, the port simply blocks access for any unauthorized client that cannot be authenticated.)
Sources for an IP Address Configuration for a Client Connected to a Port Configured for 802.x Open VLAN Mode	A client can either acquire an IP address from a DHCP server or have a preconfigured, manual IP addressing before connecting to the switch.
802.1x Supplicant Software for a Client Connected to aPort Configured for 802.1x Open VLAN Mode	A friendly client, without 802.1x supplicant software, connecting to an authenticator port must be able to download this software from the Unauthorized-Client VLAN before authentication can begin.

Note:

If you use the same VLAN as the Unauthorized-Client VLAN for all authenticator ports, unauthenticated clients on different ports can communicate with each other. However, in this case, you can improve security between authenticator ports by using the switch's Source-Port filter feature. For example, if you are using ports B1 and B2 as authenticator ports on the same Unauthorized-Client VLAN, you can configure a Source-Port filter on B1 to drop all packets from B2 and vice-versa.

Setting Up and Configuring 802.1x Open VLAN Mode

Preparation. This section assumes use of both the Unauthorized-Client and Authorized-Client VLANs. Refer to Table 1 on page 22 for other options.

Before you configure the 802.1x Open VLAN Mode on a port:

- Statically configure an "Unauthorized-Client VLAN" in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to unauthenticated clients. (802.1x authenticator ports do not have to be members of this VLAN.)

Caution

Do not allow any port memberships or network services on this VLAN that would pose a security risk if exposed to an unauthorized client.

- Statically configure an Authorized-Client VLAN in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to authenticated clients. 802.1x authenticator ports do not have to be members of this VLAN. (Note that if an 802.1x authenticator port is an untagged member of another VLAN, the port's access to that VLAN will be temporarily removed while an authenticated client is connected to the port.)
- If you expect friendly clients to connect without having 802.1x supplicant software running, provide a server on the Unauthorized-Client VLAN for downloading 802.1x supplicant software to the client, and a procedure by which the client initiates the download.
- A client must either have a valid IP address configured before connecting to the switch, or download one through the Unauthorized-Client VLAN from a DHCP server. In the latter case, you will need to provide DHCP services on the Unauthorized-Client VLAN.
- Ensure that the switch is connected to a RADIUS server configured to support authentication requests from clients using ports configured as 802.1x authenticators. (The RADIUS server should not be on the Unauthorized-Client VLAN.)

  Note that as an alternative, you can configure the switch to use local password authentication instead of RADIUS authentication. However, this is less desirable because it means that all clients use the same passwords and have the same access privileges.

Caution

Ensure that you do not introduce a security risk by allowing Unauthorized-Client VLAN access to network services or resources that could be harmed by a hostile client.

Configuring the switch's general 802.1x Operation: These steps enable 802.1x authentication, and are required before you can configure 802.1x VLAN operation.

1. Enable 802.1x authentication on the individual ports you want to serve as authenticators. (The switch automatically disables LACP on the ports on which you enable 802.1x.) On the ports you will use as authenticators with VLAN Operation, ensure that the (default) port-control parameter is set to **auto**. This setting requires a client to support 802.1x authentication (with 802.1x supplicant operation) and to provide valid credentials to get network access.

   Syntax: aaa port-access authenticator e < ***port-list*** > control auto

   Activates 802.1x port-access on ports you have configured as authenticators.

2. Configure the 802.1x authentication type. Options include:

   Syntax: aaa authentication port-access < local | eap-radius | chap-radius >

   Determines the type of RADIUS authentication to use.

   local

   Use the switch's local username and password for supplicant authentication (the default).

   eap-radius

   Use EAP-RADIUS authentication. (Refer to the documentation for your RADIUS server.

   chap-radius

   Use CHAP-RADIUS (MD5) authentication. (Refer to the documentation for your RADIUS server application.)

3. If you selected either **eap-radius** or **chap-radius** for step 2, use the **radius host** command to configure up to three RADIUS server IP address(es) on the switch.

   Syntax: radius host < ***ip-address*** >

   Adds a server to the RADIUS configuration.

   [key < ***server-specific key-string*** >]

   Optional. Specifies an encryption key for use with the specified server. This key must match the key used on the RADIUS server. Use this option only if the specified server requires a different key than configured for the global encryption key.

   radius-server key < ***global key-string*** >

   Specifies the global encryption key the switch uses for sessions with servers for which the switch does not have a server-specic key. This key is optional if all RADIUS server addresses configured in the switch include a server- specific encryption key.

4. Activate authentication on the switch.

   Syntax: aaa port-access authenticator active

   Activates 802.1x port-access on ports you have configured as authenticators.

5. Test both the authorized and unauthorized access to your system to ensure that the 802.1x authentication works properly on the ports you have configured for port-access.

Note

If you want to implement the optional port security feature on the switch, you should first ensure that the ports you have configured as 802.1x authenticators operate as expected. Then refer to the chapter titled "Configuring Port-Based Access Control (802.1x)" in the Access Security Guide for your switch. (See the subsection in that chapter on the optional use of port security.

After you complete steps 1 and 2, the configured ports are enabled for 802.1x authentication (without VLAN operation), and you are ready to configure VLAN Operation.

Configuring 802.1x Open VLAN Mode. Use these commands to actually configure Open VLAN Mode. For a listing of the steps needed to prepare the switch for using Open VLAN Mode, refer to "Preparation" on page 26.

Syntax: aaa port-access authenticator [e] < port-list >

[auth-vid < vlan-id >]

Configures an existing, static VLAN to be the Authorized-Client VLAN.

[< unauth-vid < vlan-id >]

Configures an existing, static VLAN to be the Unauthorized-Client VLAN.

For example, suppose you wanted to configure 802.1x port-access on the switch and configure Open VLAN Mode on ports A10 - A20 with the following provisions:

- Assume that these two static VLANs already exist on the switch:
  - UnAuth, VID = 80
  - Auth, VID = 81
- Your RADIUS server has an IP address of 10.28.127.101. The server uses **rad4all** as a server-specific key string. The server is connected to a port on the Default VLAN.
- Assume that the switch's default VLAN is configured with an IP address of 10.28.127.100 and a network mask of 255.255.255.0

```
HPswitch(config)# aaa authentication port-access eap-radius
```

Configures the switch for 802.1x authentication using an EAP-RADIUS server.

```
HPswitch(config)# aaa port-access authenticator a10-a20
```

Configures ports A10 - A20 as 802.1 authenticator ports.

```
HPswitch(config)# radius host 10.28.127.101 key rad4all
```

Configures the switch to look for a RADIUS server with an IP address of 10.28.127.101 and an encryption key of rad4all.

```
HPswitch(config)# aaa port-access authenticator e a10-a20 unauth-vid 80
```

Configures ports A10 - A20 to use VLAN 80 as the Unauthorized-Client VLAN.

```
HPswitch(config)# aaa port-access authenticator e a10-a20 auth-vid 81
```

Configures ports A10 - A20 to use VLAN 81 as the Authorized-Client VLAN.

```
HPswitch(config)# aaa port-access authenticator active
```

Activates 802.1x port-access on ports you have configured as authenticators.

Viewing 802.1x Open VLAN Mode Status

Syntax: show port-access authenticator [e] < ***port-list*** >

Displays the current Open VLAN Mode configuration for the specified ports.

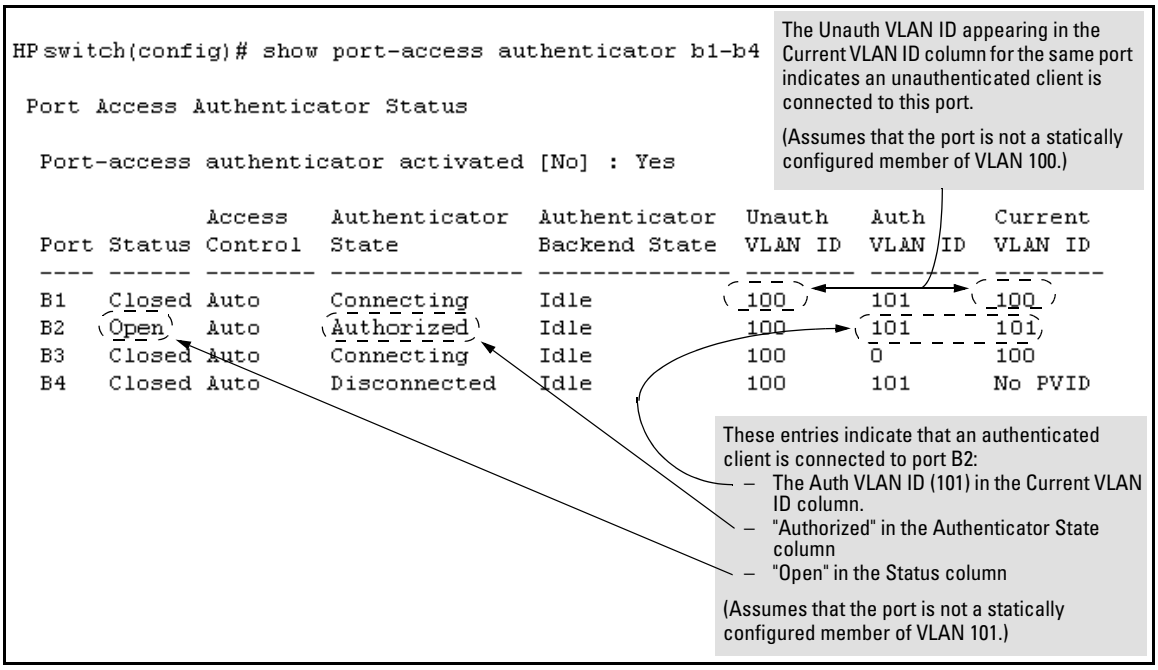

Figure 12. Example of Showing Ports Configured for Open VLAN Mode

Figure 12 demonstrates the following:

- In this case, the **Unauth VLAN ID** and the **Current VLAN ID** match on port B1. This indicates that an unauthenticated client is connected to the port and has access to the Unauthorized-Client VLAN. (See the footnoted comment in figure 12.)
- When the Auth VLAN ID and the Current VLAN ID match, an authenticated client is connected to the port. Because the Auth VLAN ID is untagged, this VLAN replaces any other untagged VLAN membership statically configured for this port.
- A "0" indicates that either an Unauth VLAN ID or an Auth VLAN ID is not configured for the indicated port.
- "No PVID" indicates that there is currently no untagged VLAN membership on the indicated port. In the case of port B4, above, Open VLAN Mode is configured on the port, but no client is connected.

Syntax: show vlan < ***vlan-id*** >

Displays the port status for the selected VLAN, including an indication of which port memberships have been temporarily overridden by Open VLAN Mode.

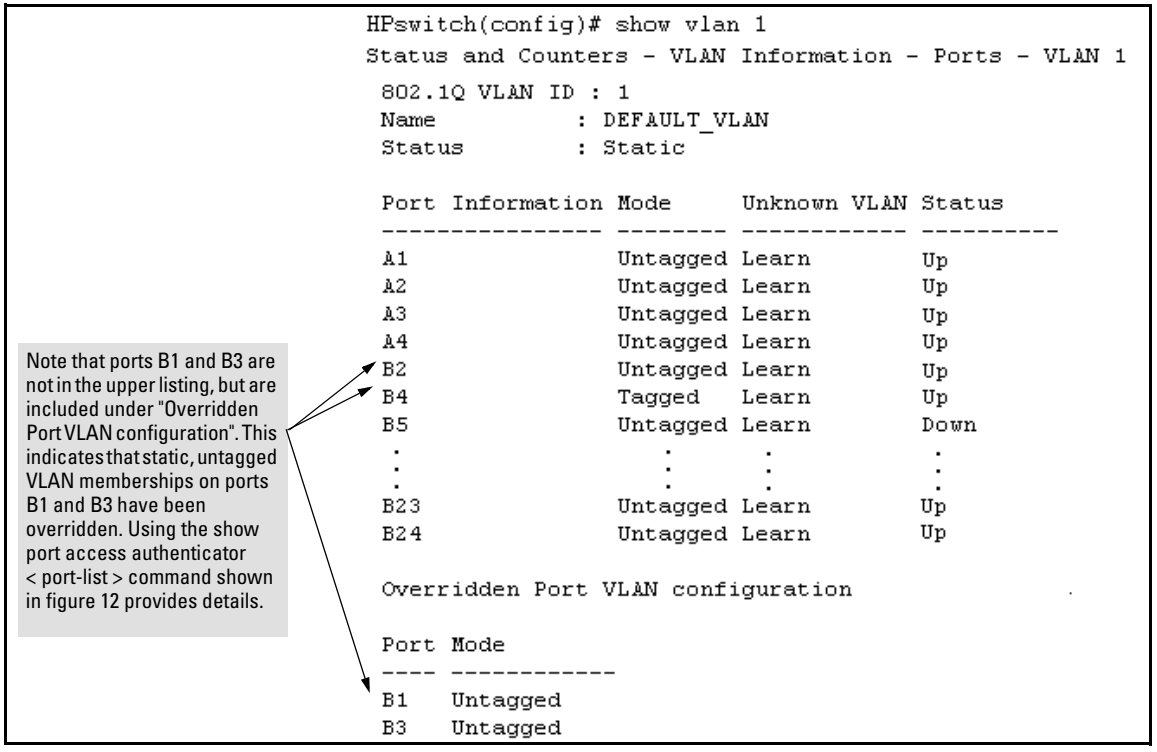

Figure 13. Example of Showing a VLAN with Ports Configured for Open VLAN Mode

Operating Notes

- Although it is possible to configure the same VLAN for both the Unauthorized-Client VLAN and the Authorized-Client VLAN, this is *not* recommended. Using the same VLAN for both purposes allows unauthenticated clients access to a VLAN intended only for authenticated clients, which poses a security breach.
- While an Unauthorized-Client VLAN is in use on a port, the switch temporarily removes the port from any other statically configured VLAN for which that port is configured as an untagged member. Note that the Menu interface will still display the port's statically configured VLAN.
- An Unauthorized-Client VLAN should not be statically configured on any switch port that allows access to resources that must be protected from unauthenticated clients.
- If a port is configured as a tagged member of a VLAN that is not used as an Unauthorized-Client, Authorized-Client, or RADIUS-assigned VLAN, then the client can access such VLANs only if it is capable of operating in a tagged VLAN environment. Otherwise, the client can access only the Unauthorized-Client VLAN (before authentication) and either the Authorized-Client or RADIUS-assigned VLAN after authentication. (In all three cases, membership will be untagged, regardless of any static configuration specifying tagged membership.) If there is no Authorized-Client or RADIUS-assigned VLAN, then an authenticated client can access only a statically configured, untagged VLAN on that port.
- When a client's authentication attempt on an Unauthorized-Client VLAN fails, the port remains a member of the Unauthorized-Client VLAN until the client disconnects from the port.
- During an authentication session on a port in 802.1x Open VLAN Mode, if RADIUS specifies membership in an untagged VLAN, this assignment overrides port membership in the Authorized-Client VLAN. If there is no Authorized-Client VLAN configured, then the RADIUS assignment overrides any untagged VLAN for which the port is statically configured.
- If an authenticated client loses authentication during a session in 802.1x Open VLAN Mode, the port VLAN membership reverts back to the Unauthorized-Client VLAN.

Software Fixes in Release E.06.*xx* and E.07.2x

Release E.05.04 was the first software release for the HP ProCurve Series 5300XL switches. Release E.06.01 is the second software release for these switches.

Release E.06.01

Problems Resolved in Release E.06.01

- **100/1000-T module —** Bringing a port up and down while the port is running at or near maximum throughput may cause the module to reset.
- **802.1x —** Support for 802.1x is not implemented in routing mode.
- **802.1x —** When changing an 802.1x port configuration, the switch does not correctly restore default VLAN ID after disconnecting the port.
- **ARP —** Switch incorrectly replied to an ARP packet with a header length ranging from 7 to 15 bytes. The switch now replies only if header length is equal to 6 bytes.
- **CDP —** CDP multicast packets are not passed through the switch when CDP is disabled on the switch.
- **CLI/RIP —** The CLI command 'show ip rip interface' results in the following:

  ```
  "RIP interface information for 0.0.0.0, RIP is not configured on this..."
  ```

- **CoS —** Cannot configure CoS on a trunk port. Also, enhancements to CoS error handling when moving ports in and out of a trunk.
- **CoS —** The output of the CLI command "show qos port-priority" may show an illegal state ("no priority") for the Differentiated Services Codepoint (DSCP) policy. This problem may occur given this situation:
  1. Configure a DSCP policy on a port, and
  2. Remove module, and
  3. Reboot switch, and
  4. Delete DSCP policy, and
  5. Hot-swap module back into the switch
- **Crash —** Switch may crash while hot swapping a module with a message similar to:

  ```
  -> Software exception in ISR@alloc_free.c:479
  ```

- **DHCP-Relay —** Configuring an IP helper address on a VLAN does not automatically turn on the DHCP-relay function.
- **Extended RMON —** When Extended RMON and Routing are enabled, the switch may duplicate packets on the network.

- **LACP —** Link-up polling interval: A delay of up to 1.7 seconds between plugging in a cable (linkbeat established) and traffic being forwarded to and from that port may cause problems with some time sensitive applications. For example, AppleTalk dynamic address negotiation can be affected, resulting in multiple devices using the same AppleTalk address.
- **Mini-GBIC Link Connectivity Issue —** A mini-GBIC Gigabit-SX/LX link between an HP ProCurve Switch 5300XL and an HP ProCurve Routing Switch 9300 may not be established when both sides are in the default configuration (Auto).
- **Radius —** If using the TAB key while entering a username for the radius prompt, the switch may display an error message similar to:

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

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

Release E.06.02

Problems Resolved in Release E.06.02

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

Release E.06.03

Problems Resolved in Release E.06.03

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

Release E.06.05

Problems Resolved in Release E.06.05

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

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

Release E.06.10

Problems Resolved in Release E.06.10

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

Release E.07.21

Problems Resolved in Release E.07.21

- **ARP —** ARP has been enhanced to have a configurable timeout value, beyond the current default of 20 minutes.
- **CDP —** CDP multicasts are not passed when CDP is diabled on the switch.
- **CLI —** Setting the telnet inactivity timeout from the CLI does not indicate a reboot is necessary for changes to take effect.
- **CLI —** The definition of default gateway following the "ip ?" in the CLI is stated as "Add/ delete defualt route to/from routing tale.", which is incorrect. Clarified help text for 'ip default-gateway' CLI command to state that this parameter is only used if routing is not enabled on the switch.
- **CLI —** Information in the command "show boot-history" is not in the order claimed (most recent first).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Filter —** Creating a source port filter for a port, moving the port into a trunk, and then reloading the saved TFTP configuration file results in a corrupted download file error.

- **Flow Control —** Setting a port "X1" in 10-HDX, then attempting to turn on flow control returns an error similar to: "Error setting value fl for port X2". The error should read "X1".

- **GVRP —** Port does not register VLAN even though advertisements are received.

- **Hot-swap —** Hot-swapping a transceiver logs a message requesting to reboot the switch in order to enable the port, which is not necessary.

- **IGMP —** If IGMP is turned on for multiple VLANs, and is then turned off for a single Vlan, the Data-Driven Mcast filters for that VLAN are not flushed.

- **IP —** IP is causing the driver to apply source port filters incorretly to non-routed packets.

- **IRDP —** When running the 'rdisc' router discovery tool under Redhat 8.0 or 7.3, Linux reports "ICMP Router Advertise from <IP>: Too short 16 40" when a IRDP packet is recieved.
- **LACP/Port Security —** With LACP on, the command "port-sec a1 l c action send-alarm" fails with a message similar to "learn-mode: Inconsistent value".
- **Link Toggle Corruption —** Addressed issue whereby toggling ports with active, bi-directional traffic could result in corrupted packets within the system.
- **Link-up Polling Interval —** A delay of up to 1.7 seconds between plugging in a cable (linkbeat established) and traffic being forwarded to and from that port may cause problems with some time sensitive applications. For example, AppleTalk dynamic address negotiation can be affected, resulting in multiple devices using the same AppleTalk address.
- **Menu —** The one-line help text below the password entry field, displays the message "`Enter up to 16 characters (case sensative), or just press <Enter> to quit`". It should read "...`sensitive`...".
- **Meshing —** Traffic on oversubscribed mesh links will migrate to other mesh links too slowly.
- **Meshing —** Meshing does not maintain priority on encapsulated packets that are sent out non-mesh ports.
- **Multicast Filters —** Any static muticast filters configured once the limit has been reached, would appear in the output of the "show filter" CLI command with only partial information. Switch now correctly returns error message "Unable to add filter" once limit has been reached.
- **OSPF —** When configured for authentication-key type "simple passwords", the switch does not include the password in OSPF packets.
- **Port Configuration —** When interchanging 10/100-TX modules J4862A and J4862B, the port configuration of the module originally installed in the switch is lost.
- **Port counters —** Hardware port counter filters for dot1dTpPortInDiscards not implemented.
- **Port counters —** The "Total RX Error" counter is incorrect when the port has heavy 10HDx traffic.
- **Port counters —** The Runt Rx counter in the detail port counter screen, does not increment when there are fragments.
- **Port counters —** The 64-bit counter for the highest numbered port on a given module, does not update properly.
- **RADIUS —** Pressing the tab key gives error message similar to "BAD CHARACTER IN ttyio_line: 0x9n" when entering a username for the radius prompt.

- **RSTP —** There is a delay in the switch relearning MAC addresses when an RSTP port transitions from Blocking to Forwarding.
- **Self Test —** There are intermittent port failures reported on hp procurve switch xl 100/1000-T modules (J4821A) while performing a packet self test, which was due to the packet test not seeing the very first packet.
- **SNMP —** The switch does not send SNMP packets larger than 484 bytes.
- **SNTP/TIMEP —** SNTP still runs when TIMEP is enabled.
- **Source Port Filters —** Source port filters for illegal ports and trunk port members cannot be deleted from the CLI.
- **Source Port Filters —** The switch does not automatically remove a source port filter for a trunk that has been deleted.
- **System Information —** Up Time displayed is not correct.
- **TACACS —** During TACACS Authentication the TACACS Server's IP address is shown on the switch's 'splash screen'.
- **TCP —** TCP port 1506 is always open. [Fix is to close TCP port 1506.]
- **TFTP —** Trying to TFTP a config onto the switch causes the switch to not complete its reload process. The switch hangs and does not come up.
- **VLANs —** The VIDs of deleted VLANs are not removed from the switch's VLAN table, causing the switch to not allow new VLANs to be created (once the VID table is full).
- **Web —** Bad URL was being mirrored back to the user following Nessus script attack test.
- **Web-Browser Interface —** Having a Procurve switch 4100gl series as a commander, and a Procurve switch 4000m as a member of the stack, the stack commander was not checking security when doing passthrough.
- **Web-Browser Interface —** The CLI does not disable the web-browser interface.
- **Web-Browser Interface —** Missing firmware/ROM information in Web UI.
- **Web-Browser Interface —** When clicking on the Web UI System Info "Apply Changes" button, a character appears under the "VLAN Configuration" tab.
- **Web-Browser Interface —** Mis-spelled word on the product registration screen of the WEB UI. The phrase "...does not appears above..." is now "...does not appear above..."
- **Web-Browser Interface —** When using a Procurve Switch 4108 as a commander switch in the stack, a Procurve Switch 2424M is not shown in the device view of the stack closeup in the web UI. The message "Device view, HP2424M, not supported by firmware of commander" is present instead of the device view.

- **Web-Browser Interface —** When a transceiver is removed from the switch, its configuration is not cleared on the Status->port status screen of the web UI. The transceiver type will still show until a new transceiver is inserted.
- **Web-browser Interface —** Web-browser port utilization label does not display the bandwidth number. Shows x% of 0Mb instead of x% of 100Mb or x% of 1Gb.
- **Web-Browser Interface —** Administrator password can be used in combination with the operator username.

HP Part Number: 5990-3084
Edition 1, January 2003

The information contained in this document is subject to change without notice.