Release Notes:

Version N.11.52 Software

for the HP Series 2810 Switches

These release notes include information on the following:

This software version supports these switches:

- HP Switch 2810-24G (J9021A)
- HP Switch 2810-48G (J9022A)

These release notes include information on the following:

Related Publications

For the latest versions of product documentation for your switch, visit **www.hp.com/networking/support/**.

Manual Part Number

5991-6273
November 2011

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 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 Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

http://www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

For HP warranty information, visit www.hp.com/networking/support/

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

Clarifications

Enhancements

Software Fixes

Software Management

Software Updates

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

Downloading Switch Documentation and Software from the Web

For the latest software versions and documentation, visit **www.hp.com/networking/support**.

To download an available software version:

1. In the first text box, type the product name (e.g. 2810) or product number.
2. Select an appropriate product that displays in the dropdown list.
3. Click the **Display Selected** button.
4. Click **Software downloads** and select from the list of software versions.

To download or view documentation:

1. In the first text box, type the product name (e.g. 2810) or product number.
2. Select an appropriate product that displays in the dropdown list.
3. Click the **Display Selected** button.
4. Click **Product support information.**
5. Click **Manuals**, then double-click the document you wish to view.
6. 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

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

- For a TFTP transfer from a server, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and use the (default) **TFTP** option.
  - Use the **copy tftp** command in the switch's CLI (see below).
- For an Xmodem transfer from a PC or Unix workstation, do either of the following:
  - Select **Download OS** in the Main Menu of the switch's menu interface and select the **Xmodem** option.
  - Use the **copy xmodem** command in the switch's CLI (page 3).
- Use the download utility in E-PCM+.

Note

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

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

TFTP Download from a Server

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

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

For example, to download a software file named L_10_0x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
Switch # copy tftp flash 10.28.227.103 N_10_0x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

2. When the switch finishes downloading the software file from the server, it displays the progress message shown in figure 1. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:

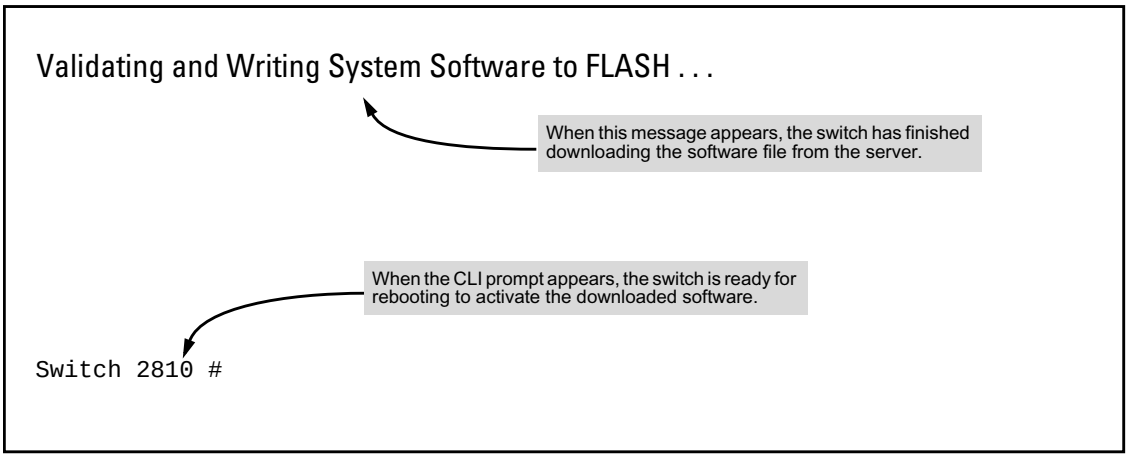

Figure 1. Message Indicating the Switch Is Ready To Activate the Downloaded Software

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

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

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

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

Syntax: copy xmodem flash [primary | secondary]

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

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

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

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

2. Execute the following command in the CLI:

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

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

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

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

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

6. Reboot the switch from the flash area that holds the new software (primary or secondary).

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

Saving Configurations While Using the CLI

The switch operates with two configuration files:

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

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

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

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

HP Switch, Routing Switch, and Router Products Software Keys

Software Letter	HP Products
A	Switch 2615-8-PoE and Switch 2915-8G-PoE
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.*xx* and earlier
I	Switch 2800 Series (2824 and 2848)
J	**J.*xx.xx*.biz** Secure Router 7000dl Series (7102dl and 7203dl)
J	**J.*xx.xx*.swi** Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
KA	Switch 3800 Series
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1810G (1810G-8, 1810G-24)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
PK	Switch 1810-48G
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
RA	Switch 2620 Series
S	Switch 2520 Series (2520-8-PoE, 2520-24-PoE)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
WA	HP Access Point 530
WM	HP Access Point 10ag
WS	HP Wireless Edge Services xl Module and the HP Redundant Wireless Services xl Module
WT	HP Wireless Edge Services zl Module and the HP Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	HP 6120G/XG and 6120XG Blade Switches
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

OS/Web/Java Compatibility Table

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

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

Clarifications

HP Security Policy and Release Notes

Per HP policy, a Security Bulletin must be the first published notification of a security defect. Fixes to security defects are not documented in release notes, also by HP policy.

The official communication for security defect fixes will always be through HP Security Bulletins. For more information on security bulletins, and information on how to subscribe to them, please see **http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02645131/c02645131.pdf**.

Visit the HP Networking Web site for more information on security and HP products:

http://h17007.www1.hp.com/us/en/solutions/security/index.aspx

Enhancements

This section lists only the software versions that contain enhancements. Enhancements are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each new software version includes all the enhancements added in previous versions.

Version N.10.05 Enhancements

Version N.10.05 contains the following enhancements:

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

Version N.10.06 Enhancements

Version N.10.06 contains the following enhancements:

- Historical information about MAC addresses that have been moved has been added to the **show tech** command output.

Version N10.07 Enhancements

Version N.10.07 includes the following enhancements:

- **Enhancement (PR_1000365862)** — This enhancement added the option of configuring ports that had been previously disabled by BPDU Protection to be automatically re-enabled.
- **Enhancement (PR_1000373226)** — Support was added for the J9054B 100-FX SFP-LC transceiver.

Version N10.08 Enhancements

Version N.10.08 includes the following enhancements:

- **Protected Ports**: To provide internet access to users but prevent them from accessing each other, use the **protected-ports** command. The command applies per-port and filters the outbound traffic from the port. See "Configuring Protected Ports" in the "Configuring and Monitoring Port Security" chapter of the *Access Security Guide* for more information.
- **Show tech transceivers**: The show tech transceivers command allows you to remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its slot. Additionally, the command displays real-time status information about all installed transceivers, including non-operational transceivers. See the chapter titled "Port Status and Basic Configuration" in the *Management and Configuration Guide* for your switch.
- **Scheduled reload**: The scheduled reload feature allows you to reboot the switch at times that are more convenient. The new parameters are "**at**" and "**after**". The **reload at** command allows you to specify a specific time for the reboot. The **reload after** command allows you to reboot the switch after a specified amount of time has passed. See the chapter titled "Switch Memory and Configuration" in the *Management and Configuration Guide* for your switch.
- **Spanning-tree admin-edge-port:** During spanning tree establishment, ports with **admin-edge-port** enabled transition immediately to the forwarding state. If a bridge or switch is detected on the segment, the port automatically operates as non-edge, not enabled. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.

- **Spanning-tree auto-edge-port**: Supports the automatic identification of edge ports. The port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Spanning-tree BPDU Filtering**: The bpdu-filter option forces a port to **always** stay in the forwarding state and be excluded from standard STP operation. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Spanning-tree BPDU Protection**: A security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Spanning-tree root-guard**: When a port is enabled as **root-guard**, it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior STP BPDUs. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Spanning-tree tcn-guard:** Causes the port to stop propagating received topology change notifications and topology changes to other ports. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Loop Protection:** Protects against the formation of loops when an unmanaged device on the network drops spanning tree packets. Transmits loop protocol packets out ports on which loop protection has been enabled. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Show spanning-tree root-history:** Displays the spanning-tree root changes history information. See the chapter titled "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.
- **Added 802.1X Client-based Access Control:** Provides client-level security that allows LAN access to individual 802.1X clients (up to 2 per port), where each client gains access to the LAN by entering valid user credentials. This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated. See the chapter titled "Configuring Port-Based and Client-Based Access Control (802.1X)" in the *Access Security Guide* for your switch.

Version N.11.11 Enhancements

Version N.11.11 includes the following enhancements:

- **Enhancement (PR_1000793342) —** The Auto-10-100 parameter was added as a port configuration option for speed-duplex.

10/100 Auto Negotiation

The 10/100 auto-negotiation feature allows a port to establish a link with a port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting. You can configure one or more of the following port parameters using this command:

Syntax [no] interface < *port-list* >

[< disable | enable >]

Disables or enables the port for network traffic. Does not use the **no** *form of the command. (Default:* **enable**.*)*

[speed-duplex < auto-10 | 10-full | 10-half | 100-full | 100-half |auto| auto-100 | 1000-full |auto-10-100>]

Specifies the port's data transfer speed and mode. Does not use the **no** *form of the command.*
(Default: **auto**.*)*

Note that in the above syntax you can substitute an "**int**" for "**interface**"; that is: **int < port-list >**.

For example, to configure port C5 for auto-10-100, enter this command:

```
Switch(config)# int c5 speed-duplex auto-10-100
```

You can configure and view the port settings by using the menu. Select **Switch Configuration > Port/Trunk Settings**. An example of the Menu display is shown below.

```
============================- TELNET - MANAGER MODE -=============
                    Switch Configuration - Port/Trunk Settings

  Port    Type       Enabled      Mode       Flow Ctrl  Group  Type
  ----  --------- + -------  ------------  ---------  -----  -----
  A1    1000T     | Yes      Auto-10-100   Disable
  A2    1000T     | Yes      Auto-10-100   Disable
  A3    1000T     | Yes      Auto          Disable
  A4    1000T     | Yes      Auto          Disable
  A5    1000T     | Yes      Auto          Disable
  A6    1000T     | Yes      Auto          Disable
  A7    1000T     | Yes      Auto          Disable     Trk1  Trunk
  A8    1000T     | Yes      Auto          Disable     Trk2  Trunk

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute ac-
tion.
```

You can use the **show interface config** command to view the port settings, as shown below.

```
Switch(config)# show interface config

 Port Settings

  Port  Type      | Enabled Mode        Flow Ctrl MDI
  ----- --------- + ------- ----------- --------- ----
  A1    100/1000T | Yes     Auto-10-100 Disable   Auto
  A2    100/1000T | Yes     Auto-10-100 Disable   Auto
  A3    100/1000T | Yes     Auto        Disable   Auto
  A4    100/1000T | Yes     Auto        Disable   Auto
  A5    100/1000T | Yes     Auto        Disable   Auto
  A6    100/1000T | Yes     Auto        Disable   Auto
```

Version N.11.14 Enhancements (Never Released.)

Version N.11.14 includes the following enhancements:

- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the **show tech** command.
- **Enhancement (PR_0000010783) —** Support was added for the following products.

  J9099B - HP 100-BX-D SFP-LC Transceiver
  9100B - HP 100-BX-U SFP-LC Transceiver
  J9142B - HP 1000-BX-D SFP-LC Mini-GBIC
  J9143B – HP 1000-BX-U SFP-LC Mini-GBIC

Version N.11.23 Enhancements

Version N.11.23 (not a public release) includes the following enhancement:

- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting.

Accounting Services

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot.

Accounting Service Types

The switch supports four types of accounting services:

- **Network accounting:** Provides records containing the information listed below on clients directly connected to the switch and operating under Port-Based Access Control (802.1X):
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Input-Packets
  - Acct-Output-Packets
  - Acct-Input-Octets
  - Nas-Port
  - Acct-Output-Octets
  - Acct-Session-Time
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id
- **Exec accounting:** Provides records holding the information listed below about login sessions (console, Telnet, and SSH) on the switch:
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Terminate-Cause
  - Acct-Authentic
  - Acct-Delay-Time
  - Acct-Session-Time
  - User-Name
  - Service-Type
  - NAS-IP-Address
  - NAS-Identifier
  - Calling-Station-Id
- **System accounting:** Provides records containing the information listed below when system events occur on the switch, including system reset, system boot, and enabling or disabling of system accounting.
  - Acct-Session-Id
  - Acct-Status-Type
  - Acct-Delay-Time
  - NAS-IP-Address
  - NAS-Identifier

- **Commands accounting:** Provides records containing information on CLI command execution during user sessions.

  - Acct-Session-Id
  - Acct-Status-Type
  - Service-Type
  - Acct-Authentic
  - User-Name
  - NAS-IP-Address
  - NAS-Identifier
  - NAS-Port-Type
  - Calling-Station-Id
  - HP-Command-String
  - Acct-Delay-Time

The switch forwards the accounting information it collects to the designated RADIUS server, where the information is formatted, stored, and managed by the server. For more information on this aspect of RADIUS accounting, refer to the documentation provided with your RADIUS server.

Operating Rules for RADIUS Accounting

- You can configure up to four types of accounting to run simultaneously: exec, system, network, and command.
- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. Use **show radius** to view the order. As long as the first server is accessible and responding to authentication requests from the switch, a second or third server will not be accessed. (For more on this topic, refer to "Changing RADIUS-Server Access Order" on page 24.)
- If access to a RADIUS server fails during a session, but after the client has been authenticated, the switch continues to assume the server is available to receive accounting data. Thus, if server access fails during a session, it will not receive accounting data transmitted from the switch.

Acct-Session-ID Options in a Management Session

The switch can be configured to support either of the following options for the accounting service types used in a management session. (Refer to "Accounting Service Types" on page 11.)

- unique Acct-Session-ID for each accounting service type used in the same management session (the default)
- same Acct-Session-ID for all accounting service types used in the same management session

Unique Acct-Session-ID Operation. In the Unique mode (the default), the various service types running in a management session operate as parallel, independent processes. Thus, during a specific management session, a given service type has the same Acct-Session-ID for all accounting actions for that service type. However, the Acct-Session-ID for each service type differs from the ID for the other types.

Note

In Unique Acct-Session-ID operation, the Command service type is a special case in which the Acct-Session-ID for each executed CLI command in the session is different from the IDs for other service types used in the session *and also* different for each CLI command executed during the session. That is, the ID for each successive CLI command in the session is sequentially incremented from the ID value assigned to the immediately preceding CLI command in that session.

The figure below shows *Unique mode* accounting operation for a new session in which two commands are executed, and then the session is closed.

User “fred” starts Exec Accounting session “003300000008”.	Acct-Session-Id = "003300000008" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Delay-Time = 0
User “fred” then executes **show ip**, which results in this accounting entry. Notice the session ID (003300000009) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This incrementing of the session ID is normal operation for command accounting in the (default) Unique mode.	Acct-Session-Id = "003300000009" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "show ip" Acct-Delay-Time = 0
User “fred” executes the **logout** command. The session ID (00330000000A) assigned to this accounting entry incrementally follows the preceding Acct-Session-Id. This is another instance of normal Command accounting operation in the Unique mode.	Acct-Session-Id = "00330000000A" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "logout" Acct-Delay-Time = 0
Terminate Exec Accounting Session “003300000008”	Acct-Session-Id = "003300000008" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Terminate-Cause = User-Request Acct-Session-Time = 29 Acct-Delay-Time = 0

Figure 2. Example of Accounting in the (Default) Unique Mode

Common Acct-Session-ID Operation. In this case, all service types running in a given management session operate as subprocesses of the same parent process, and the same Acct-Session-ID is used for accounting of all service types, including successive CLI commands.

User "fred" starts Exec Accounting session "00330000000B".	Acct-Session-Id = "00330000000B" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Delay-Time = 0
User "fred" then executes **show ip**, which results in this command accounting entry. Because this example assumes Common Mode configuration, the session ID (00330000000B) assigned to this accounting entry is identical to the session ID assigned when the session was opened. No incrementing of the session ID is done for individual commands.	Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "show ip" Acct-Delay-Time = 0
User "fred" executes the **logout** command. The session ID (00330000000B) used for the earlier Exec and Command accounting entries continues to be the same as was originally assigned to the session.	Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS User-Name = "fred" NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "172.22.17.101" HP-Command-String = "logout" Acct-Delay-Time = 0
Terminate Exec Accounting Session "00330000000B"	Acct-Session-Id = "00330000000B" Acct-Status-Type = Stop Service-Type = NAS-Prompt-User Acct-Authentic = RADIUS NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" User-Name = "fred" Calling-Station-Id = "172.22.17.101" Acct-Terminate-Cause = User-Request Acct-Session-Time = 29 Acct-Delay-Time = 0

Figure 3. Example of Accounting in Common Mode (Same Session ID Throughout)

Configuring RADIUS Accounting

RADIUS Accounting Commands	Page
[no] radius-server host < *ip-address* >	16
[acct-port < *port-number* >]	16
[key < *key-string* >]	16
[no] aaa accounting < exec | network | system > < start-stop | stop-only> radius	19
[no] aaa accounting commands < stop-only | interim-update > radius	
aaa accounting session-id < unique | common >	
[no] aaa accounting update periodic < 1 - 525600 > (*in minutes*)	20
[no] aaa accounting suppress null-username	20
show accounting	24
show accounting sessions	24
show radius accounting	24

Note

This section assumes you have already:

Configured RADIUS authentication on the switch for one or more access methods

Configured one or more RADIUS servers to support the switch

Steps for Configuring RADIUS Accounting

1. Configure the switch for accessing a RADIUS server.

   You can configure a list of up to three RADIUS servers (one primary, two backup). The switch operates on the assumption that a server can operate in both accounting and authentication mode. (Refer to the documentation for your RADIUS server application.)

   - Use the same **radius-server host** command that you would use to configure RADIUS authentication.
   - Provide the following:
     - A RADIUS server IP address.
     - Optional—a UDP destination port for authentication requests. Otherwise the switch assigns the default UDP port (1812; recommended).
     - Optional—if you are also configuring the switch for RADIUS authentication, and need a unique encryption key for use during authentication sessions with the RADIUS server you are designating, configure a server-specific key. This key overrides the global encryption key you can also configure on the switch, and must match the encryption key used on the specified RADIUS server.

2. (Optional) Reconfigure the desired Acct-Session-ID operation.
   - **Unique (the default setting):** Establishes a different Acct-Session-ID value for each service type, and incrementing of this ID per CLI command for the Command service type. (Refer to "Unique Acct-Session-ID Operation" on page 12.)
   - **Common:** Establishes the same Acct-Session-ID value for all service types, including successive CLI commands in the same management session.

3. Configure accounting types and the controls for sending reports to the RADIUS server.
   - **Accounting types:**
     - exec (page 11)
     - network (page 11)
     - system (page 11)
     - commands (page 12)
   - **Trigger for sending accounting reports to a RADIUS server:** At session start and stop or only at session stop
4. (Optional) Configure session blocking and interim updating options
   - **Updating:** Periodically update the accounting data for sessions-in-progress.
   - **Suppress accounting:** Block the accounting session for any unknown user with no username access to the switch.

1. Configure the Switch To Access a RADIUS Server. Before you configure the actual accounting parameters, you should first configure the switch to use a RADIUS server. You need to repeat this step here only if you have not yet configured the switch to use a RADIUS server, your server data has changed, or you need to specify a non-default UDP destination port for accounting requests. Note that switch operation expects a RADIUS server to accommodate both authentication and accounting.

Syntax: [no] radius-server host < *ip-address* >

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration.*

[acct-port < *port-number* >]

Optional. Changes the UDP destination port for accounting requests to the specified RADIUS server. If you do not use this option, the switch automatically assigns the default accounting port number. (Default: 1813)

[key < *key-string* >]

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

Note: *If you save the config file using Xmodem or TFTP, the key information is not saved in the file. This causes RADIUS authentication to fail when the config file is loaded back onto the switch.*

For example, suppose you want the switch to use the RADIUS server described below for both authentication and accounting purposes.

- IP address: 10.33.18.151
- A non-default UDP port number of 1750 for accounting.
- An encryption key of “source0151” for accounting sessions.

For this example, assume that all other RADIUS authentication parameters for accessing this server are acceptable at their default settings, and that RADIUS is already configured as an authentication method for one or more types of access to the switch (Telnet, Console, etc.).

```
Switch(config)# radius-server host 10.33.18.151 acct-port 1750 key source0151

Switch(config)# write mem
Switch(config)# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- --------------------------------
  10.33.18.151    1812  1750  source0151
```

Because the radius-server command includes an **acct-port** keyword with a non-default UDP port number of 1750, the switch assigns this value as the UDP accounting port.

Figure 4. Example of Configuring for a RADIUS Server with a Non-Default Accounting UDP Port Number

The radius-server command as shown in figure figure 4, above, configures the switch to use a RADIUS server at IP address 10.33.18.151, with a (non-default) UDP accounting port of 1750, and a server-specific key of "source0151".

2. (Optional) Reconfigure the Acct-Session-ID Operation.

Syntax: aaa accounting session-id < unique | common >

Optional command to reconfigure the Acct-Session-ID mode to apply to the accounting service type records for a given management session.

unique: *Configures the switch to use a different Acct-Session-ID for each accounting service type. (Default setting)*

common: *Configures the switch to apply the same Acct-Session-ID to all accounting service types in the same management session.*

For more on these options, refer to "Acct-Session-ID Options in a Management Session" on page 12.

```
Switch(config)# aaa accounting session-id common
Switch(config)# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 0
  Suppress Empty User : No
  Sessions Identification : Common

  Type      | Method Mode
  --------- + ------ --------------
  Network   | None
  Exec      | None
  System    | None
  Commands  | None
```

Example of common Session ID Configuration

Figure 5. Accounting Configured for the Common Option

3. Configure Accounting Types and the Controls for Sending Reports to the RADIUS Server. Accounting Service Types. Configure one or more accounting service types to track:

- **Exec:** Use **exec** if you want to collect accounting information on login sessions on the switch via the console, Telnet, or SSH.
- **System:** Use **system** if you want to collect accounting data when:
  - A system boot or reload occurs
  - System accounting is turned on or off

  Note that there is no time span associated with using the **system** option. It simply causes the switch to transmit whatever accounting data it currently has when one of the above events occurs.
- **Network:** Use **network** if you want to collect accounting information on 802.1X port-based-access to the network by users connected to the physical ports on the switch.
- **Commands:** When commands accounting is enabled, an accounting notice record is sent after the execution of each command.

Accounting Controls. These options are enabled separately, and define how the switch will send accounting data to a RADIUS server:

- **Start-Stop:** Applies to the **exec**, **network**, and **system** accounting service types:
  - Send a "start record accounting" notice at the beginning of the accounting session and a "stop record notice" at the end of the session. Both notices include the latest data the switch has collected for the requested accounting type.
  - Do not wait for an acknowledgement.
- **Stop-Only:** Applies to the **network**, **exec**, **system**, and **command** service types, as described below:
  - Send a stop record accounting notice at the end of the accounting session. The notice includes the latest data the switch has collected for the requested accounting type (**network**, **exec**, or **system** service types). For the **commands** service type, sends the "Stop" accounting notice after execution of each CLI command.
  - Do not wait for an acknowledgment.
- **Interim-Update:** Applies only to the **command** service type, and is intended for use when the optional **common** session ID is configured. Enabling **interim-update** in this case results in the command accounting records appearing as enclosed sub-parts of the **exec** service type record for a given management session. (Using interim-update when the **unique** session ID is configured has no effect because in this case, the different service types appear as separate accounting processes with separate Acct-Session-ID values.

Note

Configuring **interim-update** for Command accounting results in all commands being reported as "update" records, regardless of whether common or unique is configured for the accounting session ID (page 17).

Syntax: [no] aaa accounting < exec | network | system > < start-stop | stop-only > radius
[no] aaa accounting command < stop-only | interim-only > radius

Configures RADIUS accounting service type and how data will be sent to the RADIUS server.

< exec | network | system | command >: *Specifies an accounting service type to configure. Refer to "Accounting Service Types" on page 18.*

start-stop: *Applies to exec, network, and system accounting service types. Refer to "Accounting Controls" on page 18.*

stop-only: *Applies to all accounting service types. Refer to "Accounting Controls" on page 18.*

interim-update: *Applies to the commands accounting service type. Refer to "Accounting Controls" on page 18*

Example. To configure RADIUS accounting on the switch with **start-stop** for Exec functions, **stop-only** for system functions, and **interim-update** for **commands** functions. This example continues from figure 5, where the session ID was configured as **common**.

```
Switch(config)# aaa accounting exec start-stop radius
Switch(config)# aaa accounting system stop-only radius
Switch(config)# aaa accounting commands interim-update radius
Switch(config)# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 0
  Suppress Empty User : No
  Sessions Identification : Common

  Type     | Method Mode
  -------- + ------ --------------
  Network  | None
  Exec     | Radius Start-Stop
  System   | Radius Stop-Only
  Commands | Radius Interim-Update
```

Common is configured to apply the same Acct-Session-ID to all accounting records for a given switch management session.

Exec, System, and Commands accounting are active. (Assumes the switch is configured to access a reachable RADIUS server.)

Figure 6. Example of Configuring Accounting Types and Controls

Example. If the switch is configured with RADIUS accounting on the switch to use **start-stop** for Exec, System, and Command functions, as shown in figure figure 7, there will be an "Accounting-On" record when the switch boots up and an "Accounting-Off" record when the switch reboots or reloads. (Assume that Acct-Session-Id is configured for **common**.)

Record of Switch Bootup	Acct-Session-Id = "003600000001" Acct-Status-Type = Accounting-On NAS-IP-Address = 1.1.1.15 NAS-Identifier = "gsf_dosx_15" Acct-Delay-Time = 5
Record of User Session Start	Acct-Session-Id = "003600000002" Acct-Status-Type = Start Service-Type = NAS-Prompt-User Acct-Authentic = Local NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" Calling-Station-Id = "0.0.0.0" Acct-Delay-Time = 0
Record of **reload** Command Issued	Acct-Session-Id = "003600000002" Acct-Status-Type = Interim-Update Service-Type = NAS-Prompt-User Acct-Authentic = Local NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" NAS-Port-Type = Virtual Calling-Station-Id = "0.0.0.0" HP-Command-String = "reload" Acct-Delay-Time = 0
Record of System Accounting Off When Switch Reboots	Acct-Session-Id = "003600000001" Acct-Status-Type = Accounting-Off NAS-IP-Address = 10.1.242.15 NAS-Identifier = "gsf_dosx_15" Acct-Delay-Time = 0

Figure 7. Example of Accounting Session Operation with "start-stop" Enabled

4. (Optional) Configure Session Blocking and Interim Updating Options. These optional parameters give you additional control over accounting data.

- **Updates:** In addition to using a Start-Stop or Stop-Only trigger, you can optionally configure the switch to send periodic accounting record updates to a RADIUS server.
- **Suppress:** The switch can suppress accounting for an unknown user having no user name.

Syntax: [no] aaa accounting update periodic < 1 - 525600 >

Sets the accounting update period for all accounting sessions on the switch. (The **no** *form disables the update function and resets the value to zero.) (Default: zero; disabled)*

Syntax: [no] aaa accounting suppress null-username

Disables accounting for unknown users having no username. (Default: suppression disabled)

To continue the example in figurefigure 6, suppose that you wanted the switch to:

- Send updates every 10 minutes on in-progress accounting sessions.
- Block accounting for unknown users (no username).

```
Switch(config)# aaa accounting update periodic 10
Switch(config)# aaa accounting suppress null-username
Switch(config)# show accounting
 Status and Counters - Accounting Information

  Interval(min) : 10
  Suppress Empty User : Yes
  Sessions Identification : Common

  Type     | Method Mode
  -------- + ------ --------------
  Network  | None
  Exec     | Radius Start-Stop
  System   | Radius Stop-Only
  Commands | Radius Interim-Update
```

Update Period

Suppress Unknown User

Figure 8. Example of Optional Accounting Update Period and Accounting Suppression on Unknown User

Viewing RADIUS Statistics

General RADIUS Statistics

Syntax: show radius [host < *ip-addr* >]

Shows general RADIUS configuration, including the server IP addresses. Optional form shows data for a specific RADIUS host. To use **show radius**, *the server's IP address must be configured in the switch, which. requires prior use of the* **radius-server host** *command. (See "Configuring RADIUS Accounting" on page 15.)*

```
Switch(config)# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 5
  Timeout(secs) : 10
  Retransmit Attempts : 2
  Global Encryption Key : myg10balkey

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- ------------------------------
  192.33.12.65    1812  1813  my65key
```

Figure 9. Example of General RADIUS Information from Show Radius Command

```
Switch(config)# show radius host 192.33.12.65
 Status and Counters - RADIUS Server Information
  Server IP Addr : 192.33.12.65
  Authentication UDP Port : 1812         Accounting UDP Port  : 1813
  Round Trip Time         : 2            Round Trip Time      : 7
  Pending Requests        : 0            Pending Requests     : 0
  Retransmissions         : 0            Retransmissions      : 0
  Timeouts                : 0            Timeouts             : 0
  Malformed Responses     : 0            Malformed Responses  : 0
  Bad Authenticators      : 0            Bad Authenticators   : 0
  Unknown Types           : 0            Unknown Types        : 0
  Packets Dropped         : 0            Packets Dropped      : 0
  Access Requests         : 2            Accounting Requests  : 2
  Access Challenges       : 0            Accounting Responses : 2
  Access Accepts          : 0
  Access Rejects          : 0
```

Figure 10. RADIUS Server Information From the Show Radius Host Command

Table 1. Values for Show Radius Host Output (Figure figure 10)

Term	Definition
Round Trip Time	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets which contained invalid authenticators received from this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets which were received from this server on the accounting port and dropped for some other reason.
Access Requests	The number of RADIUS Access-Requests the switch has sent since it was last rebooted. (Does not include retransmissions.)
Accounting Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Responses	The number of RADIUS packets received on the accounting port from this server.

RADIUS Authentication Statistics

Syntax: show authentication

Displays the primary and secondary authentication methods configured for the Console, Telnet, Port-Access (802.1X), and SSH methods of accessing the switch. Also displays the number of access attempts currently allowed in a session.

show radius authentication

Displays NAS identifier and data on the configured RADIUS server and the switch's interactions with this server. (Requires prior use of the **radius-server host** *command to configure a RADIUS server IP address in the switch. See "Configuring RADIUS Accounting" on page 15.)*

```
Switch(config)# show authentication
 Status and Counters - Authentication Information
  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Radius     None
  Port-Access | Local      None
  Webui       | Local      None       Local      None
  SSH         | Radius     None       Radius     None
  Web-Auth    | ChapRadius None
  MAC-Auth    | ChapRadius None
```

Figure 11. Example of Login Attempt and Primary/Secondary Authentication Information from the Show Authentication Command

```
Switch(config)# show radius authentication
 Status and Counters - RADIUS Authentication Information
  NAS Identifier : Switch
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port  Timeouts   Requests   Challenges Accepts    Rejects
  --------------- ----- ---------- ---------- ---------- ---------- ----------
  192.33.12.65    1812  0          2          0          2          0
```

Figure 12. Example of RADIUS Authentication Information from a Specific Server

RADIUS Accounting Statistics

Syntax: show accounting

Lists configured accounting interval, "Empty User" suppression status, session ID, accounting types, methods, and modes.

show radius accounting

Lists accounting statistics for the RADIUS server(s) configured in the switch (using the **radius-server host** *command).*

show accounting sessions

Lists the accounting sessions currently active on the switch.

```
Switch(config)# show accounting

 Status and Counters - Accounting Information

  Interval(min) : 5
  Suppress Empty User : No
  Sessions Identification : Common

  Type      | Method Mode
  --------- + ------ --------------
  Network   | None
  Exec      | Radius Start-Stop
  System    | Radius Stop-Only
  Commands  | Radius Interim-Update
```

Figure 13. Listing the Accounting Configuration in the Switch

```
Switch(config)# show radius accounting

 Status and Counters - RADIUS Accounting Information

  NAS Identifier : Switch
  Invalid Server Addresses : 0

                  UDP
  Server IP Addr  Port  Timeouts   Requests   Responses
  --------------- ----- ---------- ---------- ----------
  192.33.12.65    1813  0          1          1
```

Figure 14. Example of RADIUS Accounting Information for a Specific Server

```
Switch(config)# show accounting sessions

Active Accounted actions on SWITCH, User (n/a) Priv (n/a),
 Acct-Session-Id 0x013E00000006, System Accounting record, 1:45:34 Elapsed
 system event 'Accounting On
```

Figure 15. Example Listing of Active RADIUS Accounting Sessions on the Switch

Changing RADIUS-Server Access Order

The switch tries to access RADIUS servers according to the order in which their IP addresses are listed by the **show radius** command. Also, *when you add a new server IP address, it is placed in the highest empty position in the list.*

Adding or deleting a RADIUS server IP address leaves an empty position, but does not change the position of any other server addresses in the list. For example if you initially configure three server addresses, they are listed in the order in which you entered them. However, if you subsequently remove the second server address in the list and add a new server address, the new address will be placed second in the list.

Thus, to move a server address up in the list, you must delete it from the list, ensure that the position to which you want to move it is vacant, and then re-enter it. For example, suppose you have already configured the following three RADIUS server IP addresses in the switch:

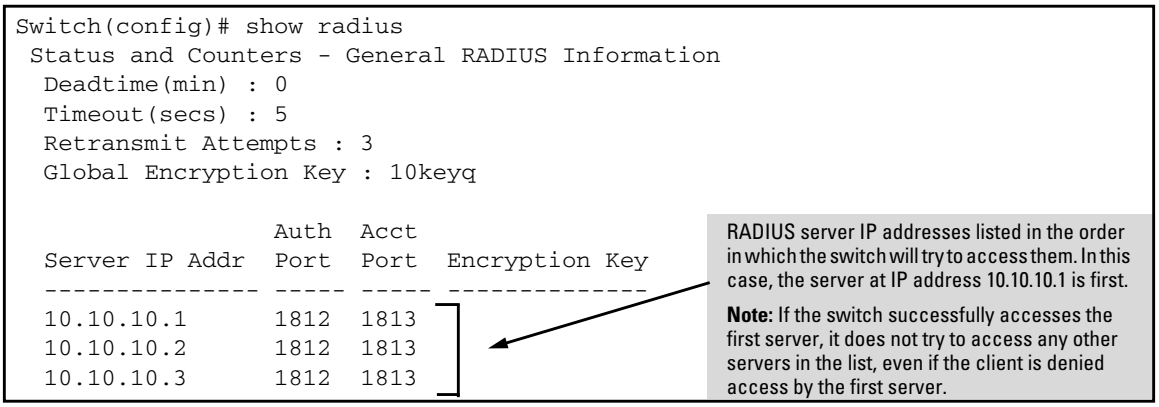

Figure 16. Search Order for Accessing a RADIUS Server

Version N.11.42

- **Enhancement (PR_0000068837)** - Adds the ability to manually add permanent static ARP entries to the ARP table.

Version N.11.52

Disable Eavesdrop Prevention

- **Enhancement (PR_0000071339, CR_0000100801)** - Traffic with an unknown destination address is blocked when port security is configured and Eavesdrop Prevention is enabled. Eavesdrop Prevention was enabled by default and could not be disabled in previous software versions. This enhancement provides the ability to disable Eavesdrop Prevention on ports where it may cause problems, such as on ports that are configured to use "limited-continuous" learning mode.

SCP and SFTP Use TACACS+ Credentials

- **Enhancement (PR_0000071457, CR_0000076445)** - The new parameter "privilege-mode" is added to the **aaa authentication login** command. This allows the user to access either Operator or Manager mode on the switch with a single login. This feature also allows SCP and SFTP to use TACACS+ credentials for file transfers.

Event Log Severity Change

- **Enhancement (PR_0000071660, CR_0000076630)** - This enhancement allows customers to use SNMP to change the severity of event log entries from their default values.

Software Fixes

Software fixes are listed in chronological order, from the oldest to the newest software release.

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

Version N.10.02 is the first software release for the HP 2810 Series switches.

Version N.10.03

The following problems were resolved in version N.10.03 (never released).

- **Auto-TFTP (PR_1000353270)** — The "auto-tftp" feature does not consistently download the configured file upon reboot.
- **CLI/Web UI (PR_1000281397)** — Passwords longer than 16 characters are truncated without user notification.
- **Crash/Software (PR_1000344998)** — The switch may crash with a message similar to:

  ```
  Software exception at sme.c:103 -- in 'mSess1', task ID = 0x8e05520 -> ASSERT: failed
  ```

- **Crash (PR_1000345064)** — Attempting to use TFTP to transfer a pub-key-file with the following command:

  ```
  copy tftp pub-key-file <ip-addr> <file-name>
  ```

  causes the switch to crash with a message similar to:

  ```
  TLB Miss: Virtual Addr=0x00000000 IP=0x805bf714 Task='mftTask' Task ID=0x81dc2000
  ```

- **Crash (PR_1000355366)** — A TLB Miss crash occurs when an LACP protocol packet is received out of order. The crash message may be similar to:

  ```
  TLB Miss: Virtual Addr=0x00000000 IP=0x80254498 Task='mLACPCtrl' Task ID=0x8347bb40
  fp:0x00000000 sp:0x8347ba98 ra:0x80254478 sr:0x1000fc01
  ```

- **Login (PR_1000347300)** — Login failures do not result in an "`Invalid Password`" response.
- **RADIUS EAP (PR_1000334731)** — PEAP/TLS EAP types fail to authenticate with Microsoft IAS Radius Server. The switch event log will report:

  ```
  can't reach RADIUS server
  ```

- **SSH (PR_1000350999)** — The SSH login prompts user to **press any key to continue** twice before providing a prompt.

Version N.10.04

The following problems were resolved in version N.10.04 (never released).

- **802.1x (PR_1000353479)** — Changing the supplicant start period (e.g., "`aaa port-access supplicant A1 start-period 15`") corrupts the supplicant password on a switch that is configured as a supplicant.

Version N.10.05

The following problems were resolved in version N.10.05 (not a public release).

- **802.1x (PR_1000366179)** — Open VLAN supplicants that fail 802.1X authentication can access the authorized VLAN.

- **802.1x (PR_1000366395)** — Enabling port-access authentication on gig ports causes the switch to crash.
- **Authorization (PR_1000365285)** — IP Authorized Managers behaves incorrectly with regard to telnet access.
- **Auto-TFTP (PR_1000362661)** — When auto-TFTP is enabled, after a **reload** command is issued from the CLI, the switch crashes after displaying the message **Rebooting the System**.
- **CLI (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.
- **Crash (PR_1000360267)** — Removing a VLAN that is assigned as the unauthorized VID may cause the switch to crash with a message similar to:

  ```
  Software exception at vls_dyn_reconfig.c:2640 -- in 'mSnmpCtrl', task ID = 0x170 ->
  ASSERT: failed.
  ```

- **Enhancement (PR_1000351445)** — The **show tech transceiver** CLI command output now contains the HP part number and revision information for all transceivers on the switch.
- **Hang (PR_1000365567)** — Switch may hang and ports not link up.
- **Hang (PR_1000346328)** — RMON alarms/events configuration files may become corrupt and prevent initialization, resulting in failure to boot.
- **RADIUS (PR_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.
- **Source Port Filtering (PR_1000352851)** — Source Port Filtering on trunks does not work, even though the switch accepts the configuration.

Version N.10.06

The following problems were resolved in version N.10.06 (not a public release).

- **802.1X (PR_1000378481)** — 802.1X authentication needs to be limited to two users per port.
- **CLI (PR_1000364628)** — The command output from **show ip rip peer** yields an incorrectly formatted peer IP address.
- **CLI/Config (PR_1000342824)** — Configuring a port for MDI will cause the port to act as MDI-X, and vice versa.
- **CLI/Config (PR_1000375830)** — When using the **no vlan** command, the user is asked if they want to remove the VLAN. Answering no will result in the VLAN being removed anyway.
- **Crash (PR_1000368540)** — The switch may crash with a message similar to:

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

- **Crash (PR_1000382962)** — Executing the CLI command, **sho int** on a miniGBIC that is not linked, may cause the switch to crash with a message similar to:

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

- **Crash (PR_1000386489)** — The switch may crash with a message similar to:

  ```
  Unalligned Access: Virtual Addr=0xa3e2dad7 IP=0x801f8234 Task='eDrvPoll' Task
  ID=0x81b02650 fp:0x81ecce90 sp:0x81b02538 ra:0x801f8208
  ```

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

- **Syslog (PR_1000379802)** — Forwarding of event log message to a configured syslog server is not disabled when a specific event log message has been disabled via MIB.
- **Web/RADIUS (PR_1000368520)** — Web Authentication does not authenticate clients due to a failure to send RADIUS requests to the configured server.
- **Web-UI (PR_1000373711)** — Attempting to access the Web UI of a stack member without being logged on as Manager returns a 404 Page Not Found error.

Version N.10.07

The following problems were resolved in version N.10.07.

- **Auto MDIX (PR_1000355099)** — Forced mode auto-MDIX on 10/100 ports does not function.
- **CLI (PR_1000380660)** — The **show tech transceivers** CLI command displays the wrong message when inserting an "A" version transceiver into a switch that only supports "B" version transceivers. Also, "B" version CX4 transceivers show up as "A" and "A" version SR, LR, and ER transceivers show up as "B" versions.
- **CLI/config (PR_1000391119)** — Copying a configuration file to a switch with a BPDU protection timeout value set may produce an error similar to:

  ```
  CCCCCline: 10007. 1200: Error setting configuration
  ```

- **CLI/LLDP (PR_1000377191)** — Output from the CLI command, **show lldp info remote-device <port>** shows a blank field for the chassis ID.
- **CLI (PR_1000390385)** — The CLI help text for **span bpdu-protection-timeout** is incorrect; it erroneously displays the help text for **span hello-time**.
- **CLI/Config (PR_1000377413)** — CLI does not prevent invalid configuration from being loaded. With this fix, configurations with excess IP Address QoS entries will result in an error message and the config file will not load.
- **Crash (PR_1000357252)** — When authenticating with Web UI using a Radius server, the switch may crash with a message similar to:

  ```
  TLB Miss: Virtual Addr=0x00211dc4 IP=0x00211dc4 Task='tHttpd' Task ID=0x83413db0
  fp:0x00000000 sp:0x83413c68
  ```

- **Daylight savings (PR_1000364740)** — Due to the passage of the Energy Policy Act of 2005, Pub. L. no. 109-58, 119 Stat 594 (2005), starting in March 2007 daylight time in the United States will begin on the second Sunday in March and end on the first Sunday in November.
- **Enhancement (PR_1000365862)** — This portion of the enhancement added the option of configuring ports that had been previously disabled by BPDU Protection to be automatically re-enabled.
- **Enhancement (PR_1000373226)** — Support was added for the J9054B 100-FX SFP-LC transceiver.
- **GVRP (PR_1000385623)** — The switch does not process GVRP frames when the receiving port is tagged, so no VLANs are learned from that source.
- **Trunking (PR_1000238829)** — Trunks numbered **trk10** and greater cause the output from the CLI command **show span** output to be misaligned.
- **Web UI (PR_1000326265)** — Attempting to access the Web UI of a stack member hangs the browser.

Version N.10.08

The following problems were resolved in version N.10.08 (never released).

- **CLI (PR_1000240838)** — If an invalid time is entered using **clock set** command, the switch responds with an "invalid date" error.
- **CLI (PR_1000199785)** — Tab help (command-completion) for "IP RIP authentication" is inaccurate.
- **CLI (PR_1000373443)** — The CLI **update** command help and confirmation message is misleading and confusing.
- **Traceroute (PR_1000379199)** — Reported **traceroute** time is inaccurate. It appears to be one decimal place off.
- **sFlow (PR_1000396889)** — If sflow skip count is set greater than the maximum skip count or less than minimum skip count, the switch returns an error, preventing PCM from collecting sampling data.
- **Menu (PR_1000392862)** — The menu will allow values greater than 720 seconds to be entered for the SNTP poll interval without error.
- **BPDU Protection (PR_1000395569)** — BPDU-protection fails after a module is hot-swapped.

Version N.10.09

The following problems were resolved in version N.10.09.

- **IP Connectivity (PR_1000418378)** — The switch (incorrectly) updates its ARP table when a client, which is configured with a valid IP address for a valid VLAN, is connected to a port in another VLAN on the switch. This will result in loss of connectivity for the valid client in the appropriate VLAN.
- **Trunking (PR_1000395062)** — When one port of a trunk fails or is disconnected, the trunk does not correctly failover.
- **Trunking (PR_1000410057)** — When a trunk port becomes inactive or a cable is unplugged, it affects communication through other trunks.
- **Crash (PR_1000413907)** — The switch crashes when stacking.
- **CLI (PR_1000413734)** — MDI/MDIX information now reports N/A when doing a **show int brief.** It should report either MDI or MDIX.
- **Crash (PR_1000410959)** — If the SNMP v3 user is deleted on the switch without deleting associated parameters and then rebooted, the switch may reboot continuously. It reports a software exception error similar to:

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

Version N.11.01

The following problems were resolved in version N.11.01 (never released).

- **System (PR_1000412897)** — Configuring a port speed to 10 mbps does not work.
- **CLI (PR_1000410952)** — When stacking, accessing a member switch through the commander's CLI may crash switch.
- **Crash (PR_1000412287)** — The switch may crash when receiving a BPDU on a port configured with 802.1x authentication.
- **CLI (PR_1000380660)** — The **show tech transceivers** command may display incorrect information when inserting certain transceivers into switch.
- **System (PR_1000403054)** — The switch does not process CDP packets.

- **STP (PR_1000382901)** — An auto-edge port link down state change may cause an STP topology change.
- **Logging (PR_1000420713)** — The switch does not properly report excessive oversized or undersized packets.
- **Web UI (PR_1000424035)** — Password sent in URL when using web interface
- **Web UI (PR_1000416167)** — CA-signed certificate cannot be installed via the Web interface with the message:

  ```
  error too large
  ```

- **Crash (PR_1000418699)** — When using Web authentication, authenticating multiple clients on a port may cause a crash.
- **Crash (PR_1000413907)** - The switch may crash when using the stacking menu.
- **CLI (PR_1000416350)** — The **show span root-history msti <x>** does not show the correct priority.
- **Crash (PR_1000420712)** — Enabling both Spanning Tree and MAC authentication may cause the switch to crash.
- **Web UI (PR_1000429039)** — Changing the IP address via the Web interface incorrectly displays the subnet mask as IP address.
- **Crash (PR_1000420722)** — The switch may crash when downloading a configuration report from the Web interface.
- **Web UI (PR_1000405976)** — The Web UI allows deleting the startup-config file without reboot creating an inconsistent state.
- **Web UI (PR_1000427213)** — The Upload/Download screen in Web interface has no scroll bars.
- **Trunk (PR_1000395062)** — Trunking may not fail over properly from one link to the other.
- **Trunk (PR_1000410057)** — Trunk failure may affect communication through other configured trunks.
- **Port Security (PR_1000402594)** — The Switch may allow unauthorized MACs to be learned when using port security.
- **TIMEP (PR_1000427372)** — "`Timesync ?`" incorrectly refers to the network time protocol. It should be “TIME” protocol.
- **MSTP** — Various MSTP compliance fixes.

Version N.11.02

The following problems were resolved in version N.11.02.

- **Web Auth (PR_1000334982)** — A software exception might occur when Web authentication and an open VLAN is configured.

Version N.11.03

The following problems were resolved in version N.11.03 (not a public release).

- **Port Counters (PR_1000440553)** — Port counters may erroneously report traffic on port 26.
- **Web-Auth (PR_1000425595)** — Web-Auth is not responding to DNS queries.
- **Network Connectivity (PR_1000436184)** — Using multiple LACP trunks with MSTP may cause a loss of network connectivity.
- **Crash (PR_1000448326)** — MAC-Auth/Web-Auth crashes the switch.

Version N.11.04

The following problems were resolved in version N.11.04.

- **Port Security (PR_1000449644)** — Port Security that is used in conjunction with 10-mbps port speed may cause the switch to crash.
- **Port Counters (PR_1000373805)** — Menu port counters "total frames" does not include all transmitted traffic.
- **OID (PR_1000450982)** — The PortSlotOID definitions are incorrect.
- **Auto_MDIX (PR_1000452011)** — Auto-MDIX does not function correctly with fixed-speed ports. Each time that he switch is reloaded, it will give random MDI/MDIX values for each port.
- **Crash (PR_1000453410)** — Stack member crashes repeatedly with a message similar to:

```
TLB Miss: Virtual Addr=0x00000000 IP=0x800a84d4 Task='mSnmpEvt' Task ID=0x833edbf0
fp:0x00000000 sp:0x833eda38 ra:0x800a84cc sr:0x1000fc01
```

Version N.11.05

The following problems were resolved in version N.11.05 (not a public release).

- **Hang/Reset (PR_1000450986)** — The switch may experience a reset while booting, making the boot time longer. The switch may boot only from the primary flash image.

Version N.11.06

The following problems were resolved in version N.11.06.

- **SNMP (PR_1000406398)** — URL-embedded SNMP traps are not sent as SSL (https) when SSL is enabled, but they are instead sent as plain text (http). This may result in the trap receiver (PCM) unable to display the URL when SSL is enabled.
- **CLI (PR_1000451000)** — Cancelling **boot system flash (prilsec)** command sets the default boot image. Issuing a **reload** after canceling causes the switch to boot into the canceled flash image.

Version N.11.07

The following problems were resolved in version N.11.07 (not a public release).

- **RX Counters (PR_1000458490) —** The "Drops RX" counters increment on spanning tree-blocked ports.

Version N.11.08

The following problems were resolved in version N.11.08.

- **IGMP (PR_1000466842) —** IGMP (PR_1000466842) - IGMP drops multicast streams at random intervals, if there are two or more streams. The first stream is not affected.

Version N.11.09

The following problems were resolved in version N.11.09.

- **Mirroring (PR_1000460844) —** Packets to other VLANs are mirrored when the **vlan x monitor** command is used.

- **SNMP (PR_1000715545) —** The switch sends unconfigured traps upon boot.
- **DST (PR_1000467724) —** The DST change-over dates are incorrect for the Western-European time zone.
- **xSTP (PR_1000330684) —** The spanning-tree command help text has been updated.
- **Sflow (PR_1000749192) —** When ports are configured as a trunk, traffic may not be sampled or may be sampled incorrectly.
- **Counters (PR_1000756649) —** The switch is incorrectly incrementing the IfInDiscard error counter.

Version N.11.10

The following problems were resolved in version N.11.10 (not a public release).

- **Web/MAC Auth (PR_1000761024) —** The Web and MAC Authentication client limit is limited to 2. This fix restores the original client limit of 32.
- **Config (PR_1000400244) —** The switch prompts the user to save config, even though no apparent changes have been made. However, if SNMP sets have occurred in the background, then the user will still see the save config prompt due to the configuration changes caused by the SNMP sets.
- **CLI (PR_1000745696) —** The scheduled reload commands **reload at** and **reload after** are not available in the CLI even though the feature is supported.
- **IGMP (PR_1000772303) —** When IP IGMP is enabled on a VLAN, and a trunk is a member of that VLAN, multicast traffic may not properly pass through.

Version N.11.11

The following problems were resolved in version N.11.11 (not a public release).

- **Authentication (PR_1000454714)** — Concurrent 802.1X and MAC-authentication does not give the 802.1X value precedence. This fix gives 802.1X VLAN assignment precedence over MAC auth RADIUS VLAN assignment.
- **Web GUI (PR_1000760153)** — A Java Error occurs when viewing the Stack Closeup page, causing a blank page to be displayed.
- **CLI (PR_1000430534)** — CLI output from the **show port-access mac-based** command does not show the correct clients connected; some are omitted.
- **Management Hang (PR_1000779084) —** The management interface may become unresponsive when all of its packet buffers are depleted.
- **System Up-time (1000772402) —** The system up-time rolls back to zero after 49 days.
- **RADIUS/Jumbo (PR_ 1000779048)** — When an 802.1X-enabled port belongs to a VLAN that is jumbo enabled, the Access-Request will specify a value of Framed-MTU of 9182 bytes. When the RADIUS server replies with a large frame, the switch does not respond, causing the authentication process to halt.
- **Web Auth (PR_1000380278)** — After running for a period, the switch will get into a state in which it must be rebooted in order for the Web authentication page to load.
- **Enhancement (PR_1000793342) —** The Auto-10-100 parameter was added as a port configuration option for speed-duplex. For more information, see "Version N.11.11 Enhancements" on page 9.
- **Crash (1000790482) —** When MAC-based or Web-based port access is configured for dual-personality ports, the switch may crash with a message similar to the following.

```
Software exception at hp53xx_port.c:2781 -- in 'mAdMgrCtrl',         task ID =
0x8347f560 -> internal error
```

- **Crash (PR_0000001756)** — Configuration of VLANs and VLAN port assignment using SNMP may cause the switch may crash with a message similar to the following.

```
Software exception at bcmHwVlans.c:149 -- in 'mAdMgrCtrl',                    task
ID = 0x18636e8 -> ASIC call failed: Entry not found.
```

- **Crash (PR_1000795039)** — The switch may crash while uploading the configuration file, if there are extra space(s) in the configuration file header. The message is similar to:

```
TLB Miss: Virtual Addr=0x00000000 IP=0x804cfd80 Task='mftTask' Task
ID=0x83357880 fp:0x83357678 sp:0x83357608 ra:0x804cfe10 sr:0x1000fc01
```

Version N.11.12

The following problems were resolved in version N.11.12 (not a public release).

- **UDLD (PR_0000002473)** — UDLD protocol packets received on a (non-UDLD) trunk port are incorrectly forwarded out of the same port from which they are received, resulting in high CPU usage on the switch.
- **Crash (PR_0000005374) —** Enabling snmpv3 on the switch may result in a crash with a message similar to the following:

```
TLB Miss:  Virtual Addr=0x00000009 IP=0x800a861c Task='mSnmpEvt'Task ID=0x833d51a0
fp:0x8334bec0  sp:0x833d4fe8 ra:0x800a858  csr:0x1000fc01
```

- **TACACS (PR_0000003010) —** The switch does not allow single manager sign-on using TACACs.

Version N.11.13

The following problems were resolved in version N.11.13 (never released).

No problems were fixed, nor enhancements introduced.

Version N.11.14

The following problems were resolved in version N.11.14 (never released).

- **TACACS+ (PR_0000003839)** — The TACACS server configuration parameter accepts an address from an invalid/ reserved IP range, 0.0.0.1 to 0.255.255.255.
- **Enhancement (PR_1000406763)** — New commands were added to the CLI response to the **show tech** command. For more information, see "Version N.11.14 Enhancements (Never Released.)" on page 11.
- **Enhancement (PR_0000010783) —** Support was added for the following products.

  J9099B - HP 100-BX-D SFP-LC Transceiver
  J9100B - HP 100-BX-U SFP-LC Transceiver
  J9142B - HP 1000-BX-D SFP-LC Mini-GBIC
  J9143B – HP 1000-BX-U SFP-LC Mini-GBIC

For more information, see "Version N.11.14 Enhancements (Never Released.)" on page 11.

Version N.11.15

The following problems were resolved in version N.11.15.

- **Web (PR_0000011479) —** The HP HP 1000 BX and 1000 LH mini-GBICs were neither visible nor configurable in the Web Management Interface config screen.
- **Transceivers (PR_0000010525) —** Intermittent self test failure may occur if transceivers are hot-swapped in and out of the switch in too short a time frame. Note that even with this fix, transceivers should always be allowed to initialize fully prior to removal and subsequent re-insertion.

  Best Practice Tip: Upon hot insertion of a transceiver, the mode LED will come on for two seconds. Once this LED has extinguished, it is once again safe to remove the transceiver.

Version N.11.16

The following problems were resolved in version N.11.16 (not a public release).

- **BPDU Protection (PR_0000012541)** — The presence of a trunk group in a switch with STP BPDU protection configured may trigger the switch to block the wrong port when a BPDU is received.
- **CDP/LLDP (PR_0000005741)** — The switch is not consistently detecting neighboring Cisco Catalyst switches via CDP.
- **Config (PR_0000002077)** — Presence of the valid CLI/configuration parameter **spanning-tree trap errant-bpdu** will trigger failure to upload a configuration, with the switch reporting an error similar to the following (in this example, the problem parameter was on line 16 of the configuration).

  ```
  line: 16. trap: Error setting configuration.
  Corrupted download file.
  ```

- **Loop Protect(PR_0000010897)** — The loop detection feature may not function properly on ports configured with any combination of MAC-Authentication, spanning-tree, and bpdu-protection.
- **Management (PR_0000005902)** — The switch management may become unresponsive, resulting in loss of Telnet, Web Management, and console access functionality of the switch.

Version N.11.17

The following problems were resolved in version N.11.17 (never released).

- **802.1X (PR_0000008780)** — 802.1X does not receive expiration notifications from port security if 802.1X is running alone (without Web or MAC Authentication).
- **802.1X (PR_0000012568)** — There may be a problem with a login error message.
- **802.1X (PR_0000015662)** — When AAA Authentication with 802.1X using PEAP is configured, the port status does not change appropriately to 802.1X, leading to client 802.1X authentication failure.
- **Authentication (PR_0000013472)** — Port-access authentication may not occur when there is a combination of tagged and untagged port membership in the same VLAN (as the auth-vid, unauth-vid, or a RADIUS-assigned VLAN). This fix prevents untagged VLAN assignment to be applied to a port if that port is a tagged member of the same VLAN. Best Practice Tip: Configure different VLANs for the **auth-vid** and **unauth-vid** roles.
- **CLI (PR_0000008217)** — The **copy flash** CLI command does not allow the user to specify a source OS location (primary/secondary).

- **CLI (PR_0000010942)** — The CLI command output for **show run** does not display **aaa port-access <port#>** when MAC-based authentication with mixed port access mode is configured. Other show commands may also be affected.
- **Config (PR_0000005002)** — If a friendly port name uses the characters TRUNK=, then after a reload, all the trunking configuration will have been removed from the configuration.
- **Config (PR_0000010713)** — The configuration line **aaa port-access web-based dhcp-addr <IP address> <subnet mask>** cannot be removed via the CLI.
- **Config (PR_0000017930)** — Preconfiguration of an SFP port followed by a save of the configuration, power down of the switch, insertion of a mini-GBIC, and then power up the switch causes the port configuration to return to default values.
- **Controlled Directions (PR_0000009818)** — The switch does not properly enable or edit the controlled direction parameter (in the config line **aaa port-access controlled-direction <in|out|both>**) in the configuration.
- **Crash (PR_0000038448)** — Switches configured for Web Authentication may reboot unexpectedly in response to DHCP activity, displaying a message similar to the following.

```
Software exception at exception.c:621 -- in 'mAcctCtrl', task ID =
0x842d140 -> Memory system error at 0x7ed5950 - memPartFree
```

- **GVRP (PR_0000012224)** — Changing the GVRP unknown-vlan state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **MAC Authentication (PR_0000015520)** — Traffic from unauthenticated clients may be allowed during the process of authenticating clients under heavy loads.
- **RADIUS Accounting (PR_0000012487)** — The switch doesn't send an accounting-stop when a switch reload closes the session.
- **SNMP (PR_0000002409)** — Several supported OIDs return 'No such variable' in response to the CLI command **walkmib <OID>**. Affected OIDs include the following.

```
1.3.6.1.4.1.11.2.14.11.5.1.32 (hpSwitchAutzServicePrimaryMethod)
1.3.6.1.4.1.11.2.14.5.1.35 (hpicfInstMonTrapEnable)
```

- **SNMP (PR_0000002764), (PR_1000310843)** — The SNMP MIB object that allows authenticator functionality on a port to be enabled or disabled (hpicfDot1xPaePortAuth) can be set to an invalid value.
- **SNMP (PR_0000037800)** — The following OIDs are in violation of RFC 4133, which specifies, "If no specific hardware revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string."

```
entPhysicalHardwareRev
entPhysicalFirmwareRev
entPhysicalSerialNum
entPhysicalModelName
```

- **VLAN (PR_0000013388)** — A switch with trunks not configured for VLAN <x> still accepts tagged frames for VLAN <x> and forwards them to other ports configured for VLAN <x>.

Version N.11.18

The following problems were resolved in version N.11.18 (not a public release).

- **802.1X (PR_0000005372)** — Some combinations of source and destination MAC addresses may cause 802.1X to stop functioning on a port; only a reboot will recover functionality.

- **802.1X (PR_0000010850)** — If an unauth-vid is configured, and the client limit is reached on a switch port, a properly credentialed re-authentication following an improperly credentialed authentication attempt (for example, incorrect password) will leave the 802.1X client in the unauthorized VLAN instead of applying the appropriate authorized VLAN.
- **802.1X (PR_0000041041)** — The switch may reach a point at which it will no longer be able to authenticate 802.1X clients until it is reloaded. The speed at which this occurs is dependent on the rate of 802.1X connection attempts.
- **Crash (PR_0000015095)** — The switch may reboot unexpectedly when it receives a certain type of traffic. A message similar to the following may be present in the switch event and crash logs.

  ```
  Unaligned Access: Virtual Addr=0xa7fb7aa3 IP=0x803628ac
  Task='eDrvPoll'
  ```

- **Crash (PR_0000039959)** — When a port is configured for limited-continuous learn mode (**port-security <port number> learn-mode limited-continuous**), MAC-address timeouts followed by port-access activity may cause the switch to reboot unexpectedly with a message similar to one of the following.

  ```
  Software exception at exception.c:373 -- in 'm8021xCtrl', task ID =
  0x17ff538
  -> Memory system error at 0x16c9370 - memPartFree
  ```

  ```
  NMI event SW:IP=0x005906a8 MSR:0x0000b032 LR:0x00350144
  Task='m8021xCtrl' Task D=0x17fb968
  cr: 0x48000042 sp:0x017fb270 xer:0x20000000
  ```

  ```
  PPC Bus Error exception vector 0x300:
  Stack-frame=0x017f6350 HW Addr=0x6d6d3434 IP=0x0059069c
  Task='m8021xCtrl' Task ID=0x17f6698
  fp: 0x017f6410 sp:0x017f6410 l
  ```

- **LLDP (PR_0000038230)** — The length of a CDP packet may prevent the switch from accepting the packet.
- **Loop Protection (PR_0000006192)** — When Loop Protection is enabled, sometimes the switch will forward broadcasts instead of disabling the port.
- **MAC Authentication (PR_0000011949)** — MAC authentication may fail to occur unless the switch port status is toggled.

Version N.11.19

The following problems were resolved in version N.11.19 (not a public release).

- **Crash (PR_0000015979)** — When Secure Shell (SSH) is configured, the switch may reboot unexpectedly with a crash message similar to the following.

  ```
  NMI event SW:IP=0x803f4fc0 SR:0x1000fc01 Task='tSsh0' Task ID=0x81d68220 sp:0x81d67830
  ```

- **Crash (PR_0000041599)** — When a configuration file is uploaded to the switch via TFTP or SCP/SFTP, the switch crashes during attempted reload into the configuration if one or more of the following configuration lines are present in the configuration.

  snmp-server response-source <IP address>
  snmp-server response-source dst-ip-of-request
  snmp-server trap-source <IP address>

  The switch will log a crash message similar to the following.

  ```
  PPC Bus Error exception vector 0x300: Stack-frame=0x0124cc40
  HW Addr=0x025aa1cc IP=0x00538808 Task='mftTask' Task ID=0 x124dcb0
  fp: 0x012d5c30 sp:0x0124cd00 lr:0
  ```

- **SNMP (PR_1000469020)** — Warm start and cold start traps are not sent to all configured trap receivers.
- **STP (PR_0000041155)** — When spanning tree is disabled, the switch floods spanning tree BPDUs received on a port that is tagged for VLAN 1.
- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (**unauth-vid**) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an **unauth-vid** for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

  Best Practice Tip: 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if the first packet sent was not 802.1X, Web- or MAC-auth could be initiated before 802.1X places the user in the unauthenticated VLAN and when Web- or MAC-auth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

  If a MAC- or Web-based configuration on a port is associated with an unauth-VID, and an attempt is made to configure an unauth-VID for 802.1X (**port-access authenticator**), the switch with this fix will reject the configuration change with a message similar to one of the following.

  Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):

  ```
  Configuration change denied for port <number>. Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please disable Web and MAC authentication on this port using the following commands:
  ```

  no aaa port-access web-based <PORT-LIST> or

  no aaa port-access mac-based <PORT-LIST>

  ```
  Then you can enable 802.1X authentication with unauthenticated VLAN. You can re-enable
  Web and/or MAC authentication after you remove the unauthenticated VLAN from 802.1X.
  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.
  ```

  Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):

  ```
  Configuration change denied for port <number>.Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please remove the unauthenticated VLAN from 802.1X authentication on this port using
  the following command:
  ```

  no aaa port-access authenticator <PORT-LIST> unauth-vid

  ```
  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.
  ```

  Message 3:

  ```
  Configuration change denied for port <number>. Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please use unauthenticated VLAN for Web or MAC authentication instead.
  ```

  Event log message when the configuration is changed:

  ```
  mgr: Disabled unauthenticated VLAN on port <number> for the 802.1X.
  Unauthenticated VLAN cannot be simultaneously enabled on both 802.1X and Web or MAC
  authentication.
  ```

Version N.11.20

The following problems were resolved in version N.11.20 (never released).

- **Crash (PR_0000042767)** — After configuring an "unrestricted" SNMP community name that is exactly 32 characters (the maximum allowed), when the switch is rebooted or power-cycled it will unexpectedly reboot repeatedly. A factory reset is required to recover. The crash message is similar to the following.

```
TLB Miss:  Virtual Addr=0x00a21270 IP=0x800b2d1c Task='swInitTask'
Task ID=0x85f72860 fp:0x00000000 sp:0x85f72648 ra:0x800b2cd0 sr:0x1000fc01
```

- **Crash (PR_0000043167)** — When using TFTP with "octet" mode to upload the switch's configuration file, the switch may reboot unexpectedly with a message similar to the following.

```
Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabeb240
-> MemWatch Trigger: Offending task 'tTftpDmn'.
Offending IP=0x1cb174
```

- **Crash (PR_0000043999)** — When the switch is configured with SNMPv3, it may reboot unexpectedly when a network management server communicates with it using SNMPv3. The crash message will be similar to the following.

```
TLB Miss: Virtual Addr=0x00000000 IP=0x800ab0f8 Task='mSnmpCtrl'
Task ID=0x85d26d00 fp:0x00000000 sp:0x85d26a60 ra:0x800aadc8
sr:0x1000fc01
```

- **MSTP (PR_0000043241)** — This enhancement to MSTP operation causes all VLANs to automatically be placed in the IST by default, when MSTP is configured.

Version N.11.21

The following problems were resolved in version N.11.21 (not a public release).

- **Config (PR_0000045067)** — After configuring MSTP instances using some VLANs that are explicitly defined and some VLANs that are not yet defined, uploading of the resulting config file onto a switch will remove the not-yet-defined VLANs from the configuration.

Version N.11.22

The following problems were resolved in version N.11.22 (not a public release).

- **CLI (PR_0000010378)** — Session time (sec.) remains at zero in response to the CLI command **show port-access authenticator <port> session-counters**; it should increment.
- **Command Authorization (PR_0000043525)** — HP-Command-String authorization does not work as expected.
- **Controlled Directions (PR_0000038263)** — Some frames are allowed on the switch port despite the default aaa parameter **controlled-directions both**.
- **GVRP (PR_0000040238)** — After a dynamically-learned VLAN is converted to a static port-based VLAN, and an interface is made a static member of that VLAN, disabling GVRP causes the port to lose the VLAN membership. The running-config, startup-config and the SNMP egress static member list for the VLAN show the port as member of the VLAN. All other data shows the port is no longer a member of the VLAN. VLAN communication over the affected interface is no longer possible until the one of the two following workarounds is executed. Workarounds: Either re-issue the tag and untag commands for VLAN port assignment, or reload the system.
- **Web Management (PR_0000043877)** — On a 2810-48 switch, port 48 is incorrectly labeled as port 49M in the Web management screen.

Version N.11.23

The following problems were resolved in version N.11.23 (not a public release).

- **Authentication (PR_0000044893)** — When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch may change the Class of Service (COS) settings.
- **CLI (PR_0000046278)** — When a user issues the command, **copy flash flash <pri | sec>**, the system does not process packets scheduled for CPU processing in a timely manner for the duration of the write to flash task. This can cause issues such as Spanning Tree topology changes due to BPDU starvation.
- **Crash (PR_0000046987)** — When a switch port configured for Web authentication receives certain packets, the switch may reboot unexpectedly and log a message similar to the following.

```
Unalligned Access:  Virtual Addr=0xa3fb08cb IP=0x8032bbbc Task='eDrvPoll'
Task ID=0x834d9970 fp:0x834d98c8 sp:0x834d97b8 ra:0x8032b29c sr:0x1000fc01
```

- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see "Accounting Services" on page 11.
- **GVRP (PR_0000040758)** — Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each 'spanning-tree' (the IST and each of the MSTIs).
- **MAC Authentication (PR_0000039884)** — The configured MAC authentication timeout period does not function properly.

Version N.11.24

The following problems were resolved in version N.11.24 (not a public release).

- **802.1X (PR_0000047025)**
- **Web Authentication (PR_0000047284**) — A Web Authentication client that is also running Skype will not be authenticated by the switch.

Version N.11.25

- **Authentication (PR_0000052226)** — When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch may change the Class of Service (COS) settings. This PR_0000052226 improves the Authentication fix in N.11.23 software (PR_0000044893).
- **Config (PR_0000037570)** — After using the CLI to assign a port in a VLAN number higher than 32, the configuration cannot be saved via the Menu interface.
- **Crash (PR_0000038008)** — The switch may reboot unexpectedly during Telnet access, with a message similar to the following.

```
NMI event SW:IP=0x0049cba8 MSR:0x0000b032 LR:0x00489a8c Task='tTelnetOut2' Task
ID=0x3210d30
cr: 0x22000080 sp:0x03210860 xer:0x20000000
```

- **Management (PR_0000044146)** — Ping and telnet to the switch fail at exactly 1243 days of uptime.
- **RADIUS Accounting (PR_0000042522)** — The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.

- **SSH (PR_0000014531)** — Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.

Version N.11.26

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.26.

- **Authentication (PR_0000053003) -** After a client is authenticated by 802.1X, if the switch receives a subsequent successful Web or MAC Authentication for that same client, the switch overwrites the 802.1X client RADIUS attributes.
- **Console (PR_0000001136) -** Rarely, the switch console may hang after a software image transfer to the switch. Workaround: **<Ctrl-C>** will restore the command prompt.
- **GVRP (PR_0000046133) -** This improves the GVRP fix in N.11.23 (PR_0000040758).
- **LLDP-MED (PR_0000050798)** - In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.
- **SNMP/Config (PR_0000043775)** - The switch allows invalid configuration parameters to be set via SNMP.
- **Stacking (PR_0000052110)** - When a commander accesses a member switch and the user issues the **show tech all** command, in some situations the session from commander to member can become unresponsive. Workaround: from the commander switch, **kill** the unresponsive session.
- **Web Management (PR_0000050589)** - The Web user interface **Apply Changes** button saves the switch's IP address but not the default gateway. This fix adds a separate **Apply** button to save the default gateway address. This fix was improved upon with PR_0000058137 in N.11.28 software.

Version N.11.27

Status: Released and fully supported, but not posted on the Web.
No problems were resolved in software version N.11.27.

Version N.11.28

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.28.

- **File Transfer (PR_0000054790)** - Switch software cannot be updated via HTTPS.
- **SFTP (PR_0000057598)** - Using PuTTY PSFTP to copy SSH authorized keys from the switch fails with a `permission denied` message.
- **Web Management (PR_0000055834)** - From the Web interface, the user cannot create an SSL certificate with an end date beyond the year 2020.
- **Web Management (PR_0000058137)** - The Web user interface **Apply Changes** button saves the switch's IP address but not the default gateway. With this fix, the **Apply Changes** button saves both values simultaneously.

Version N.11.29

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.29.

- **Spanning Tree (PR_0000057003)** - The switch might experience Spanning Tree instability upon changing the system time via CLI, TimeP, or SNTP, if the time change occurs while the switch is receiving high volumes of broadcast traffic (on the order of 1 Mbps) on its Spanning Tree root port. This issue might also affect switch management traffic, causing unresponsive SNMP, TELNET, and SSH sessions.

Version N.11.30

Status: Never released.
The following problems were resolved in software version N.11.30.

- **CLI (PR_0000058067)** - When the switch is configured with a default gateway, the output of **show ip route** gives incorrect values for Metric and Distance. However, communication with the default gateway works properly.
- **Port Security (PR_0000055625)** - With port security enabled, the switch drops the first packet it receives even if the packet passes the security check.

Version N.11.31

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.31.

- **Port Security (PR_0000061391)** - With port security enabled and after the first ARP request is received on a port, for every subsequent ARP request received on that port the switch forwards two ARP requests.
- **Rate Limiting (PR_0000058451)** - The switch implements broadcast rate limiting when it senses a broadcast storm, but does not remove the rate limiting after five seconds as it should.

Version N.11.32

Status: Never released.
The following problems were resolved in software version N.11.32.

- **MSTP (PR_0000061650)** - An MSTP "pending" configuration does not allow the user to move a VLAN from one instance to another.
- **SSL (PR_0000060309)** - The Web User Interface and CLI do not allow the user to configure the same date ranges for SSL certificates. With this fix, both interfaces allow SSL certificate date ranges of 1990 through 2037.
- **Web Management (PR_0000060813)** - Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access.

Version N.11.33

Status: Released and fully supported, but not posted on the Web.
No problems were resolved in software version N.11.33.

Version N.11.34

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.34.

- **Management (PR_0000062888)** - In some situations, moderate levels of broadcast traffic cause the switch to be unresponsive to ping, telnet, or SSH connections.

Version N.11.35

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.35.

- **Management (PR_0000053533)** - The ProCurve Manager (PCM) "test communication parameters" test might fail on the second attempt.

Version N.11.36

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.36.

- **Loop Protection (PR_0000063965)** - The switch might experience a broadcast storm even though loop protection is configured.

Version N.11.37

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.37.

- **CLI (PR_0000051188)** - If the switch uses DHCP to obtain an IP address, the output of **show ip** does not display the correct default gateway. This is a display issue only; the correct gateway address is used by the switch.
- **Web Management (PR_0000060662)** - The Web user interface displays the word `Status` at top of screen even though there is no status information provided.

Version N.11.38

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.38.

- **MAC Authentication (PR_0000066384)** - If a switch port is tagged for a specific VLAN and RADIUS assigns that same VLAN as untagged for a MAC authentication client, authentication fails.

Version N.11.39

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.39.

- **Authentication (PR_0000058441)** - User authentication fails if the user's RADIUS configuration includes a non-HP VSA before any HP VSAs. Workaround: Configure the user in RADIUS with at least one HP VSA before any non-HP VSAs.

- **FFI/Config (PR_0000039989)** - FFI - If an FFI event is triggered, and then the link is brought down and back up again, the same FFI event will be triggered again in about 20 seconds even if the trigger condition isn't met. Config - This fix makes the downgrade of the port to auto-10/100 visible in the running configuration. Note that this may trigger the switch to ask `Do you want to save current configuration?` upon logout or switch reload.

Version N.11.40

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.40.

- **802.1X (PR_0000067682)** - When using 802.1X in client mode, the command **aaa port-access authenticator 1 client-limit 2** should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.
- **Mirroring (PR_0000069115)** - On a 48-port switch, traffic sent out ports 1-24 might not be monitored by a mirror port if the mirror port is on ports 25-48, and vice versa.
- **SNMP (PR_0000069036)** - In response to an SNMP query, the switch reports an MTU size of 9212 even though jumbo frames are not enabled.

Version N.11.41

Status: Released and fully supported, but not posted on the Web.
No problems were resolved in software version N.11.41.

Version N.11.42

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.42.

- **Enhancement (PR_0000068837)** - Adds the ability to manually add permanent static ARP entries to the ARP table.

Version N.11.43

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.43.

- **CLI (PR_0000069348)** - The switch allows configuration of a "voice" VLAN even though the switch does not support LLDP-MED.
- **SSL (PR_0000070330)** - After copying the CA certificate to the switch this error message is received: `Error setting CA Signed Request Configuration - No certificate is installed`.

Version N.11.44

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.44.

- **CLI (PR_0000041836)** - The switch asks users if they want to save the configuration even though no changes were made. Note that configuration changes made via SNMP will still trigger this behavior even after this fix.
- **CLI (PR_0000068813)** - The commands **page** and **no page** are not available at the Operator privilege level.

- **IGMP (PR_0000070385)** - After receiving a frame with destination address 231.0.0.2, the switch floods all multicast streams that have no clients.

Version N.11.45

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.45.

- **SSH (PR_0000062389)** - After connecting to the switch with Operator privileges, a subsequent SSH connection will only receive Operator privileges instead of Manager privileges.

Version N.11.46

Status: Never released.
No problems were resolved in software version N.11.46.

Version N.11.47

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.47.

- **Latency (PR_0000070153)** - On the 48-port switch, traffic from a port in the first bank of ports (ports 1-24) to a port in the second bank of ports (25-48) and vice versa might experience latency and packet drops when the outbound port is oversubscribed (asked to send more traffic than it can handle).
- **Web Management (PR_0000070264)** - The config file saved via the Web user interface is corrupted and cannot be loaded onto a switch.

Version N.11.48

Status: Released and fully supported, but removed from the Web due to CR_0000103000.
The following problems were resolved in software version N.11.48.

- **CLI (PR_0000071004)** - The output of the command **show port-access authenticator config** displays the direction as `both`, even if the direction was configured to be **in** or **out**.
- **File Transfer (PR_0000072686)** - A config file with the entry **spanning-tree trap errant-bpdu** cannot be loaded onto a switch. This issue was fixed with PR_0000002077 in N.11.16, but re-introduced in N.11.20.

Version N.11.49

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.49.

- **Authentication (PR_0000070500, CR_0000075626)** - When the 802.1X authenticator times out waiting for a supplicant response, instead of transitioning to the connecting state and restarting the attempt to acquire a supplicant by transmitting Identity-Requests, it falls silent.
- **Spanning Tree (PR_0000070920, CR_0000075970**) - With Spanning Tree disabled, tagged Spanning Tree BPDUs are not always forwarded out a trunked port.

Version N.11.50

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version N.11.50.

- **IGMP (PR_0000071591, CR_0000076574)** - Forced Fast-Leave IGMP does not work correctly for ports with MACs learned on multiple VLANs, unless each of those VLANs is configured for Forced Fast-Leave.
- **Loop Protection (PR_0000072139, CR_0000077073)** - Loop-protect stops working on the ports connected to an unmanaged switch.
- **Secure Copy (PR_0000072803, CR_0000077639)** - After disabling SCP (Secure Copy Protocol) and enabling TFTP, the switch's config file retains the "no tftp client" entry that was automatically added when SCP was enabled.

Version N.11.51

Status: Released and fully supported, but not posted on the Web.
The following problem was resolved in software version N.11.51.

- **Spanning Tree (CR_0000103000)** - The switch does not process Spanning Tree BPDUs that are received on a port with all VLANs tagged.

Version N.11.52

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version N.11.52.

- **Enhancement (PR_0000071339, CR_0000100801)** - Traffic with an unknown destination address is blocked when port security is configured and Eavesdrop Prevention is enabled. Eavesdrop Prevention was enabled by default and could not be disabled in previous software versions. This enhancement provides the ability to disable Eavesdrop Prevention on ports where it may cause problems, such as on ports that are configured to use "limited-continuous" learning mode.
- **Enhancement (PR_0000071457, CR_0000076445)** - The new parameter "privilege-mode" is added to the **aaa authentication login** command. This allows the user to access either Operator or Manager mode on the switch with a single login. This feature also allows SCP and SFTP to use TACACS+ credentials for file transfers.
- **Enhancement (PR_0000071660, CR_0000076630)** - This enhancement allows customers to use SNMP to change the severity of event log entries from their default values.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/

November2011

Manual Part Number
5991-6273