Release Notes:
Version T.12.06 Software
for the ProCurve Series 2900 Switches

The T.12.06 software supports these switches:

- ProCurve Switch 2900-24G (J9049A) and 2900-48G (J9050A)

These release notes include information on the following:

Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at **//www.procurve.com**. Click on **Technical support**, then **Product manuals**.

- Management and Configuration Guide
- Advanced Traffic Management Guide
- Access Security Guide
- Multicast and Routing Guide

Publication Number

5991-4790
April, 2007

Applicable Products

ProCurve Switch 2900-24G (J9049A)
ProCurve Switch 2900-48G (J9050A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

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

www.openssh.com.

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

www.openssl.org.

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

Disclaimer

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

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

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

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

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

Contents

Software Management

Software Updates

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

Downloading Switch Documentation and Software from the Web

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

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

   www.procurve.com.

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

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

1. Go to the ProCurve Networking Web site at **www.procurve.com**.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation. For the ProCurve Series 2900 switches, the link for the manuals pages is: **www.hp.com/rnd/support/manuals/2900.htm**
4. On the resulting web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Switch

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

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

Note

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

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

TFTP Download from a Server

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

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

For example, to download a software file named T_11_1x.swi from a TFTP server with the IP address of 10.28.227.103:

1. Execute the copy command as shown below:

```
ProCurve # copy tftp flash 10.28.227.103 T_11_1x.swi
The primary OS image will be deleted. continue [y/n]? Y
03125K
```

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

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

3. When the CLI prompt re-appears, the switch is ready to reboot to activate the downloaded software:
4. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
5. Reboot the switch from the flash area that holds the new software (primary or secondary).

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

Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

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

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

Syntax: `copy xmodem flash [< primary | secondary >]`

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

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

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

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

2. Execute the following command in the CLI:

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

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

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

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

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

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

Saving Configurations While Using the CLI

The switch operates with two configuration files:

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

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

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

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

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	Secure Router 7000dl Series (7102dl and 7203dl)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G)
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
T	Switch 2900 Series (2900-24G, and 2900-48G)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

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

The following clarifications apply to series 2900 switch documentation as of the T.12.00 release.

- **Enabling Jumbo Frames and Flow Control**
  The 2900 series switches support simultaneous use of Jumbo Frames and Flow Control, and the switch allows flow control and jumbo packet capability to co-exist on a port. (The earlier version of the Management and Configuration Guide incorrectly stated that these features could not be enabled at the same time.)

- **TACACS+ Encryption Key Exclusion from TFTP Copies**
  When using the copy command to transfer a configuration to a TFTP server, any server-specific or global encryption keys in the TACACS+ configuration will not be included in the transferred file. Otherwise, a security breach could occur, allowing access to the TACACS+ username/password information.

Enhancements

Unless otherwise noted, each new release includes the enhancements added in all previous releases. Enhancments are listed in chronological order, oldest to newest software release. For the latest enhancements since the last general release was published, go to "Release T.12.03 Enhancements" on page 10.

Descriptions and instructions for enhancements included in Release T.12.00 or earlier are included in the latest release of manuals for the ProCurve 2900 Series switches (February 2007), available on the web at www.hp.com/rnd/support/manuals

Release T.11.01 was the first production software release for the ProCurve 2900 Series switches. Releases T.11.02 through T.11.09 were never built.

Release T.11.13 is the last release of the T.11.xx software. The switch 2900 series software code was rolled to the T.12.01 code branch with no intervening releases.

Release T.11.10 through T.11.12 Enhancements

No new enhancements, software fixes only.

Release T.11.13 Enhancements

The following enhancements are included in the T.11.13 release.

- Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- Historical information about MAC addresses that have been moved has been added to the "show tech" command output.

Release T.12.01 Enhancements

The following enhancements are included in the T.12.01 release documentation. The enhancements are listed by the title of the switch guide that includes the full description and instructions for that enhancement.

Advanced Traffic Management Guide

- **Loop Protection**—Detects the formation of loops when there is an unmanaged device on the network by transmitting loop protection protocol packets.

- **Qos Queue Config**—Allows you to reduce the number of outbound queues that all switch ports will use to buffer packets for 802.1p user priorities.
- **BPDU Protection**—A security feature designed to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain.
- **BPDU Filtering**—Allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations.

Management and Configuration Guide

- **Unidirectional Link Detection (UDLD)**—Monitors a link between two ProCurve switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks.
- **Loopback Interface**—A virtual interface that is always up and reachable as long as at least one of the IP interfaces on the switch is operational. By default, each switch has an internal loopback interface (**lo0**). You can configure up to seven other loopback interfaces on the switch.
- **sFlow**— can be configured via the CLI for up to three distinct sFlow instances. Once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. (Introduced in Software Release K.11.34)
- **Clear Logging Command**—Causes event log entries to be hidden from display when using the standard **show logging** command.
- **Reload After/At Command**—**after:** Schedules a warm reboot of the switch after a given amount of time has passed.
  at: *S*chedules a warm reboot of the switch at a given time.

Multicast and Routing Guide

- **DHCP Option 82 Enhancement**—Specifies the IP address of the (optional) Management VLAN configured on the routing switch.
- **RIP**—the Routing Exchange Protocol (RIP) is now supported. RIP is an IP route exchange protocol that uses a ***distance vector*** (a number representing distance) to measure the cost of a given route.

Security Guide

- **RADIUS AAA**—Allows you to limit the services for a user by enabling AAA RADIUS authorization. The NAS uses the information set up on the RADIUS server to control the user's access to CLI commands.

- **Client-based Access Control**—provides client-level security that allows LAN access to individual 802.1X clients (up to 8 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.
- **Controlled Directions 802.1X and Web/MAC Auth**— allows you to use the **aaa port-access controlled-directions** command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state. Available for 802.1X and Web/MAC authorization. (Added in T.11.10, now documented)

The following enhancements included in Release T.12.01 are not covered in the February 2007 version of the switch 2900 series documentation.

- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR_1000373226)** — Support was added for a future SFP.
- **Enhancement (PR_1000376626)** — Enhanced CLI **qos dscp-map help** help and **show dscp-map** text to warn the user that inbound classification based on DSCP codepoints only occurs if **qos type-of-service diff-services** is also configured.

Release T.12.02 Enhancements

The following enhancements are included in the T.12.02 release.

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

Release T.12.03 Enhancements

The following enhancements are included in the T.12.03 release (never released).

- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports. The **range** option requires two port numbers that specify the range.

  qos <udp-port | tcp-port> < tcp/udp port number | range <*tcp/udp port number*> <*tcp/udp port number*> > priority < 0 - 7>

For more information, refer to "QoS UDP/TCP Priority" in the *Advanced Traffic Management Guide*.

- **Enhancement (PR_1000398393)** — For the **interface *<port-list>* speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.

Release T.12.04 Enhancements

No new enhancements, software fixes only.

Release T.12.05 Enhancements

The following enhancement is included in the T.12.05 release (never released).

- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs. For more information, see "How RADIUS-Based Authentication Affects VLAN Operation" below.

How RADIUS-Based Authentication Affects VLAN Operation

Using a RADIUS server to authenticate clients, you can provide port-level security protection from unauthorized network access for the following authentication methods:

- 802.1X: Port-based or client-based access control to open a port for client access after authenticating valid user credentials.
- MAC address: Authenticates a device's MAC address to grant access to the network.
- Web-browser interface: Authenticates clients for network access using a web page for user login.

Note

You can use 802.1X (port-based or client-based) authentication and either Web or MAC authentication at the same time on a port, with a maximum of 8 clients allowed on the port. (The default is one client.) Web authentication and MAC authentication are mutually exclusive on the same port. Also, you must disable LACP on ports configured for any of these authentication methods. For more information, refer to the "Configuring Port-Based and Client-Based Access Control (802.1X)" and "Web and MAC Authentication" chapters of the *Access Security Guide*.

VLAN Assignment on a ProCurve Port

Following client authentication, VLAN configurations on a ProCurve port are managed as follows when you use 802.1X, MAC, or Web authentication:

- The port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. Tagged VLAN membership allows a port to be a member of multiple VLANs simultaneously.
- The port is temporarily assigned as a member of an untagged (static or dynamic) VLAN for use during the client session according to the following order of options.
  a. The port joins the VLAN to which it has been assigned by a RADIUS server during client authentication.
  b. If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the authorized-client VLAN configured for the authentication method.
  c. If the port does not have an authorized-client VLAN configured, but is configured for membership in an untagged VLAN, the switch assigns the port to this untagged VLAN.

Operating Notes

- During client authentication, a port assigned to a VLAN by a RADIUS server or an authorized-client VLAN configuration is an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN. The following restrictions apply:
  - If the port is assigned as a member of an untagged *static* VLAN, the VLAN must already be configured on the switch. If the static VLAN configuration does not exist, the authentication fails.
  - If the port is assigned as a member of an untagged *dynamic* VLAN that was learned through GVRP, the dynamic VLAN configuration must exist on the switch at the time of authentication and GVRP-learned dynamic VLANs for port-access authentication must be enabled

    If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.
- To enable the use of a GVRP-learned (dynamic) VLAN as the untagged VLAN used in an authentication session, enter the **aaa port-access gvrp-vlans** command, as described in "Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions" on page 16.
- Enabling the use of dynamic VLANs in an authentication session offers the following benefits:
  - You avoid the need of having static VLANs pre-configured on the switch.
  - You can centralize the administration of user accounts (including user VLAN IDs) on a RADIUS server.

For information on how to enable the switch to dynamically create 802.1Q-compliant VLANs on links to other devices using the GARP VLAN Registration Protocol (GVRP), refer to the "GVRP" chapter in the *Advanced Traffic Management Guide*.

- For an authentication session to proceed, a ProCurve port must be an untagged member of the (static or dynamic) VLAN assigned by the RADIUS server (or an authorized-client VLAN configuration). The port temporarily drops any current untagged VLAN membership.

  If the port is not already a member of the RADIUS-assigned (static or dynamic) untagged VLAN, the switch temporarily reassigns the port as an untagged member of the required VLAN (for the duration of the session). *At the same time, if the ProCurve port is already configured as an untagged member of a different VLAN, the port loses access to the other VLAN for the duration of the session.* (A port can be an untagged member of only one VLAN at a time.)

  When the authentication session ends, the switch removes the temporary untagged VLAN assignment and re-activates the temporarily disabled, untagged VLAN assignment.

- If GVRP is already enabled on the switch, the temporary untagged (static or dynamic) VLAN created on the port for the authentication session is advertised as an existing VLAN.

  If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in "Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session" on page 14), the disabled VLAN assignment is not advertised. When the authentication session ends, the switch:

  - Removes the temporary untagged VLAN assignment and stops advertising it.
  - Re-activates and resumes advertising the temporarily disabled, untagged VLAN assignment.

- If you modify a VLAN ID configuration on a port during an 802.1X, MAC, or Web authentication session, the changes do not take effect until the session ends.

- When a switch port is configured with RADIUS-based authentication to accept multiple 802.1X and/or MAC or Web authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session.

  Therefore, on a port where one or more authenticated client sessions are already running, all such clients are on the same untagged VLAN. If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail. For more on this topic, refer to "802.1X Open VLAN Mode" in the "Configuring Port-Based and Client-Based Access Control (802.1X)" chapter in the *Access Security Guide*.

Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session

The following example shows how an untagged static VLAN is temporarily assigned to a port for use during an 802.1X authentication session. In the example, an 802.1X-aware client on port 2 has been authenticated by a RADIUS server for access to VLAN 22. However, port 2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in Figure 1.

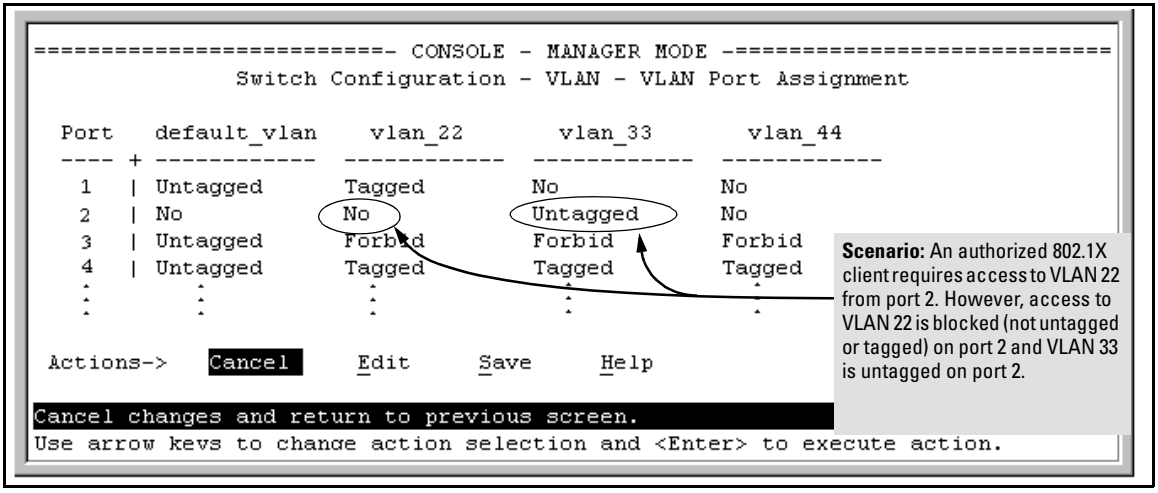

Figure 1. Example of an Active VLAN Configuration in the Menu Interface View

In Figure 1, if RADIUS authorizes an 802.1X client on port 2 with the requirement that the client use VLAN 22, then:

- VLAN 22 becomes available as Untagged on port 2 for the duration of the session.
- VLAN 33 becomes unavailable to port 2 for the duration of the session (because there can be only one untagged VLAN on any port).

To view the temporary VLAN assignment as a change in the active configuration, use the **show vlan *<vlan-id>*** command as shown in Figure 2, where ***<vlan-id>*** is the (static or dynamic) VLAN used in the authenticated client session.

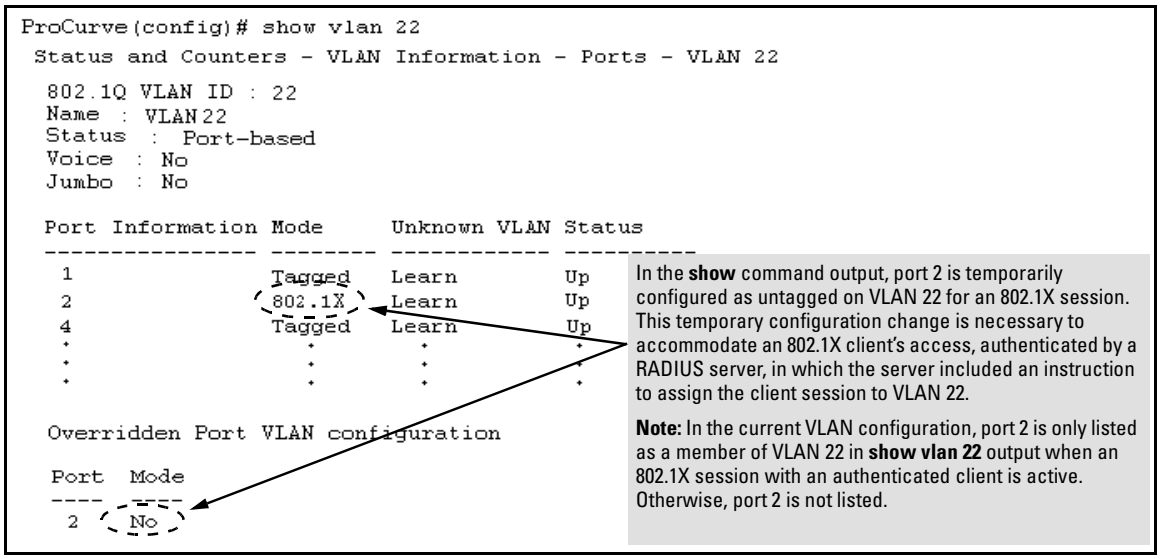

Figure 2. Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session

However, as shown in Figure 1, VLAN 33 is configured as untagged on port 2 and because a port can be untagged on only one VLAN, port 2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of port 2 access to VLAN 33 by entering the **show vlan 33** command as shown in Figure 3.

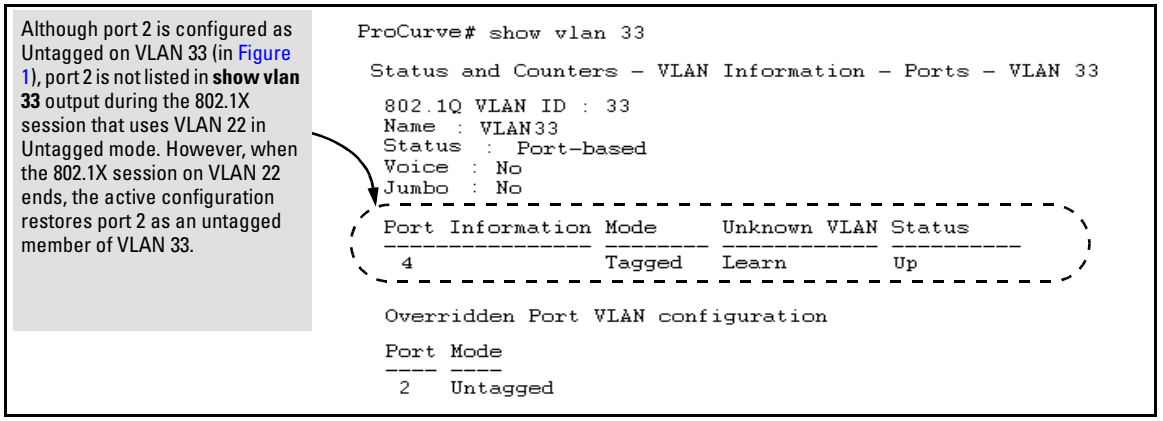

Figure 3. Active Configuration for VLAN 33 Temporarily Drops Port 2 for the 802.1X Session

When the 802.1X client session on port 2 ends, the port removes the temporary untagged VLAN membership. The static VLAN (VLAN 33) that is "permanently" configured as untagged on the port becomes available again. Therefore, when the RADIUS-authenticated 802.1X session on port 2 ends, VLAN 22 access on port 2 also ends, and the untagged VLAN 33 access on port 2 is restored as shown in Figure 4.

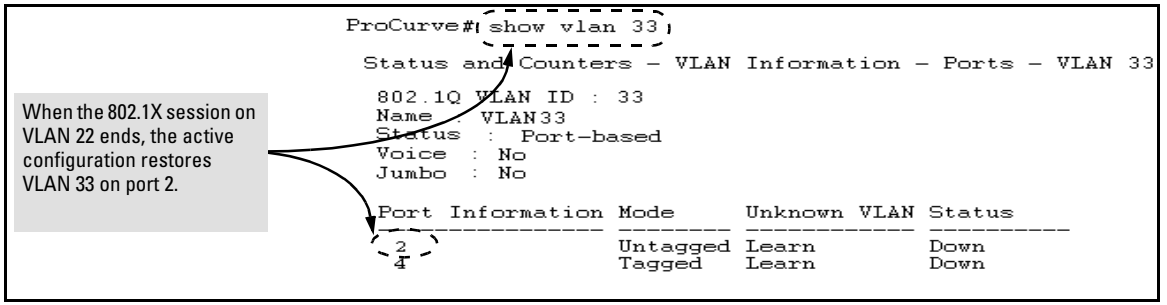

Figure 4. The Active Configuration for VLAN 33 Restores Port 2 After the 802.1X Session Ends

Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions

Syntax: aaa port-access gvrp-vlans

Enables the use of dynamic VLANs (learned through GVRP) in the temporary untagged VLAN assigned by a RADIUS server on an authenticated port in an 802.1X, MAC, or Web authentication session.

Enter the **no** *form of this command to disable the use of GVRP-learned VLANs in an authentication session.*

For information on how to enable a switch to dynamically create 802.1Q-compliant VLANs, refer to the "GVRP" chapter in the Access Security Guide.

Notes:

1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic VLAN configuration must exist at the time of authentication and GVRP for port-access authentication must be enabled on the switch.

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

(Continued)

Syntax: aaa port-access gvrp-vlans *(Continued)*

2. After you enable dynamic VLAN assignment in an authentication session, it is recommended that you use the **interface unknown-vlans** *command on a per-port basis to prevent denial-of-service attacks. The* **interface unknown-vlans** *command allows you to:*

- *Disable the port from sending advertisements of existing GVRP-created VLANs on the switch.*
- *Drop all GVRP advertisements received on the port.*

For more information, refer to the "GVRP" chapter in the Advanced Traffic Management Guide.

3. If you disable the use of dynamic VLANs in an authentication session using the **no aaa port-access gvrp-vlans** *command, client sessions that were authenticated with a dynamic VLAN continue and are not deauthenticated.*

(This behavior differs form how static VLAN assignment is handled in an authentication session. If you remove the configuration of the static VLAN used to create a temporary client session, the 802.1X, MAC, or Web authenticated client is deauthenticated.)

However, if a RADIUS-configured dynamic VLAN used for an authentication session is deleted from the switch through normal GVRP operation (for example, if no GVRP advertisements for the VLAN are received on any switch port), authenticated clients using this VLAN are deauthenticated.

For information on how static and dynamic VLANs are assigned in a RADIUS-based 802.1X, MAC, or Web authentication session, refer to the "How RADIUS/802.1X Authentication Affects VLAN Operation" section in the "Configuring Port-Based and Client-Based Access Control (802.1X)" chapter of the Access Security Guide.

Release T.12.06 Enhancements

No new enhancements, software fixes only.

Software Fixes in Release T.11.10 - T.12.06

Software fixes are listed in chronological order, oldest to newest. To review the list of fixes included since the last general release that was published, go to "Release T.12.03" on page 23.

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

Release T.11.01 was the first production software release for the ProCurve 2900 Series switches.

Releases T.11.02 through T.11.09 were never built.

Release T.11.13 is the last release of the T.11.xx software. The switch 2900 series software code was rolled to the T.12.01 code branch with no intervening releases.

Release T.11.10

The following problems were resolved in release T.11.10 (never released)

- **802.1X (PR_1000359976)** — Changed the maximum number of 802.1X users to 8.
- **802.1x (PR_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports.
- **CLI (PR_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **Crash (PR_1000346971)** — When stacking is disabled, the switch may crash with a message similar to:

  ```
  PPC Data Storage (Bus Error) exception vector 0x300: Stack Frame=0x08895e48
  HW Addr=0x39200000 IP=0x007132f8 Task='mSnmpCtrl'
  ```

- **Crash (PR_1000357083)** — The switch may crash with a message similar to:

  ```
  Software exception at ngDmaTx.c:722 -- in 'tDevPollTx', task ID = 0x4305c504
  -> HW DMA DRIVER unable.
  ```

- **Enhancement (PR_1000358903)** — 802.1X Controlled Directions enhancement. With this enhancment, administrators can use "Wake-on-LAN" with computers that are connected to ports configured for 802.1X authentication. No further information on using this feature is available at this time.
- **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_1000359640)** — Switch hangs on initialization and becomes unresponsive.

- **Management VLAN (PR_1000299387)** — The management VLAN does not allow connectivity from valid IP addresses.
- **SNMP (PR_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.
- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.

Release T.11.11

The following problems were resolved in release T.11.11

- **802.1X (PR_1000367404)** — CLI allows configuration of more 802.1X users per port than the eight per port supported by the switch.

Release T.11.12

The following problems were resolved in release T.11.12

- **802.1p QoS (PR_1000368188)** — 802.1p prioritization may not work once a trunk is enabled on a module, unless the user issues the commands "qos type-of service ip-precedence" or "qos type-of service diff-services".
- **ACL (PR_1000368901)** — Outbound access control lists (ACLs) do not function after a reboot.
- **Authorization (PR_1000365285)** — IP Authorized Managers behaves incorrectly with regard to telnet access.
- **CLI (PR_1000313916)** — The CLI output for the "show ip" command is misaligned; the proxy-arp column is shifted over to the left by one.
- **CLI (PR_1000368900)** — VLAN names over 12 characters in length cause "show ip route" to be displayed incorrectly.
- **Crash (PR_1000356446)** — When traffic monitoring is in use, the switch may crash with a message similar to this.

  ```
  Data Bus Error: Addr=0x704a6114 Data=0x00000011 flags=0x10000751,
  IP=0x4012eaac Task='mEaseUpdt' TaskID=0x42fef338
  ```

- **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_1000372604)** — When multiple of instances of sFlow have been configured via the CLI, the switch may crash with an error similar to:

  ```
  Software exception at sflow.c:1170 -- in 'mEaseCtrl', task ID =
  0x80e5fe0-> ASSERT:  failed.
  ```

- **Menu/Event Log (PR_1000319407)** — Disabling of event log numbers, via the "no log-numbers" CLI command, doesn't work properly when viewing the event log via the Menu. Using the 'next' and 'prev' buttons causes the log numbers to reappear.
- **Routing (PR_1000350144)** — Adding a VLAN and assigning an IP address to that VLAN through the menu interface takes routing information protocol (RIP) offline in all VLANs.
- **RADIUS (PR_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.
- **sFlow (PR_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.
- **Traffic Monitoring/Performance Degradation (PR_1000370061)** — The switch is affected by ProCurve Manager (PCM) traffic monitoring, causing throughput degradation.
- **VLAN (PR_1000356062)** — When configuring from the menu interface, the 3500yl series switches will not allow the following name format for a new VLAN: "VLANx" (where "x" is a VLAN number).

Release T.11.13

The following problems were resolved in release T.11.13 (not a general release)

- **CLI (PR_1000377318)** — The output from the CLI command, 'show dhcp-relay' is truncated.
- **CLI (PR_1000379455)** — The output from some CLI "show" commands produces incorrectly formatted output on the screen.
- **Enhancement (PR_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **Event Log (PR_1000373796)** — Selecting "Save", within the IP Configuration screen of the Menu causes unnecessary Event Log messages.
- **Menu/Counters (PR_1000370619)** — The Menu Interface does not reflect changes to SNMP OIDs for "IP Mgmt - Tx/Rx" counters; the counter always reads "0."

- **sFlow/Flow-Control (PR_1000375851)** — To protect performance, egress sFlow sampling will be disabled on all ports if Flow-Control is enabled on any one or more ports, and a CLI/Event Log message will be generated.
- **Syslog (PR_1000379802)** — Forwarding of event log messages 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.

Release T.12.01

The following problems were resolved in release T.12.01

- **CLI (PR_1000332352)** — The output of a "show int brief" command should show the negotiated flow control status rather than the flow control configuration setting.
- **Crash (PR_1000378804)** — The switch may crash when the maximum number of QoS rules is exceeded.
- **Crash (PR_1000392105)** — Specific actions in the port status screen of the menu interface may trigger a crash. Scrolling down to the ports on a module in slot L and pressing [enter] may cause the switch to crash with a message similar to:

```
Software exception at exception.c:424 -- in 'mSess1', task ID =
0x8dd1ab0 -> Memory system error at 0x881a480 - memPartFree
```

- **Enhancement (PR_1000373226)** — Support was added for a future SFP.
- **Enhancement (PR_1000298920)** — A ping request issued to a VLAN which is down will now return a more specific message; instead of "request timed out," the message "The destination address is unreachable" will be displayed.
- **Enhancement (PR_1000376626)** — Enhance CLI "qos dscp-map he" help and "show dscp-map" text to warn the user that inbound classification based on DSCP codepoints only occurs if "qos type-of-service diff-services" is also configured.
- **Routing (PR_1000359162)** — When the user configures a static route that overlaps with a local subnet configured on the switch, the router will not respond to packets destined for its own IP address. The packets for its own IP address will be routed using the configured static route.

Release T.12.02

The following problems were resolved in release T.12.02

- **CLI (PR_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.
- **Crash (PR_1000398746)** — The switch may crash with the task "swInitTask". This could result in repeated crashes until the switch configuration is cleared.
- **Crash /Traffic Monitoring (PR_1000396662)** — When Traffic Monitoring is enabled on the switch by a network management station (such as PCM) the switch may crash with a message similar to:

```
Data Bus Error: Addr=0x704a613c Data=0xffffffff flags=0x10000750,
IP=0x4012fa80 Task='tSvcWorkQ' TaskID=0x44b42ad0 cpsr=0x80000013
```

- **Crash (PR_1000392863)** — Switch may crash when "setmib tcpConnState" is used, with a message similar to:

```
NMI event SW:IP=0x0079f4a0 MSR:0x00029210 LR:0x006dca60
Task='eTelnetd' Task ID=0x8a7cbb0 cr: 0x20000042 sp:0x08a7c871
```

- **Crash (PR_1000399448)** — Changes to traffic monitoring settings may trigger the switch to crash with a message similar to:

```
Software exception at ease_ctrl.c:575 -- in 'mEaseCtrl', task ID =
0x8347160
```

- **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.
- **DHCP (PR_1000397753)** — A unicast DHCP request that has already been relayed by another router is sometimes dropped.
- **Hang (PR_1000397964)** — The switch appears to hang where all routing stops, the switch cannot ping anything, even addresses configured locally.
- **Enhancement (PR_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.
- **Proxy-ARP (PR_1000393571)** — Proxy-ARP sends responses to gratuitous ARPs.
- **RIP (PR_1000393366)** — The switch does not process RIP (v2) responses containing subnets with a classful subnet mask, when the receiving RIP switch has a connected VLSM network defined that would fall within that classful range.

Release T.12.03

The following problems were resolved in release T.12.03 (never released).

- **Enhancement (PR_1000404544)** — Provides TCP/UDP port range prioritization in the **qos** command; the **range** option assigns an 802.1p priority to (IPv4) TCP or UDP packets associated with a range of TCP/UDP ports. For more information, see "Release T.12.03 Enhancements" on page 10.
- **Enhancement (PR_1000398393)** — For the **interface <*port-list*> speed-duplex** command, added the **auto-10-100** configuration option to constrain a link to 10/100 Mbps speed and allow a more rapid linkup process when 1000 Mbps operation is not possible.

Release T.12.04

The following problems were resolved in release T.12.04 (never released).

- **ACL (PR_1000395595)** — Removing a VLAN via SNMP does not remove the related ACL relationship to that VLAN.
- **ACL (PR_1000402901)** — The ACL resequencing feature may discard some ACEs in a random fashion.
- **BootROM (PR_1000402707)** — BootROM does not upgrade to latest version when upgrading code to primary flash.
- **CLI (PR_1000403104)** — Executing the **erase startup-configuration** command and rebooting does not clean up the RMON 'alarm' table.
- **Crash (PR_1000405465)** — Use of dynamically assigned ACLs may cause the switch to reboot with the following error:

```
Software exception at aclBttfMUtils.c:1208 -- in 'midmCtrl',
task ID = 0x85f6a60 -> internal error
```

- **MSTP (PR_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specifications to stay in sync with the protocol evolution.
- **sFlow (PR_1000408145)** — sFlow samples for routed packets do not occur bidirectionally; inbound packets are dropped and only outbound packets are sampled.
- **Traceroute (PR_1000379199)** — The reported **traceroute** time is inaccurate; it is one decimal place off.

Release T.12.05

The following problems were resolved in release T.12.05 (never released).

- **Enhancement (PR_1000408960)** — RADIUS-Assigned GVRP VLANs. For more information, see "Release T.12.05 Enhancements" on page 11.
- **Menu (PR_1000392862)** — The menu will allow invalid values (greater than 720 sec) to be entered for the SNTP poll interval.

Release T.12.06

The following problems were resolved in release T.12.06.

- **Config (PR_1000410790)** — Errors are returned when applying the **interface *<port-list>* speed-duplex auto-10-100** command to interfaces 45-48.
- **Config (PR_1000405639)** — Various characters in configuration file names (including dash, ampersand, plus, and spaces within quotes) result in truncated names after reboot. This is not just a display issue; the command **erase configs *<filename>*** does not remove a file containing the problem characters.
- **Crash (PR_1000410758)** — When the **interface *<port-list>* speed-duplex auto-10-100** command is issued on a range of ports, the switch may crash with a message similar to:

```
NMI event HW:IP=0x0083f224 MSR:0x00029210 LR:0x0033c3c4
Task='tDevPollRx' Task ID=0x9137e50 cr: 0x20000022
sp:0x09137d78 xer:0x20000000
```

- **RIP (PR_1000377789)** — RIP restrict filters are not working upon reboot.
- **RMON (PR_1000410885)** — RMON alarms/thresholds set via SNMP are cleared after a reboot.

July 2007
Manual Part Number
5991-4790 Edition 2