



# Release Notes:

## Version K.12.25 Software

*for the ProCurve Series 3500yl, 6200yl, and 5400zl Switches*

---

These release notes include information on the following:

- Downloading switch software and documentation from the Web ([page 1](#))
- Support Notes, Known Issues, and Clarifications for certain software features ([page 10](#))
- A listing of software enhancements in recent releases ([page 12](#))
- A listing of software fixes included in releases K.11.11 through K.12.25 ([page 65](#))

---

### Support Notices:

**Security:** Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. If this is not desirable for your network, ProCurve recommends that you disable it after downloading and rebooting with the latest switch software. See "[Support Notes](#)" on [page 10](#) for details.

**ACL numbering restrictions:** This release enforces ACL numbering restrictions. See the Note under Version K.12.01 Software Fixes on [page 80](#) (PR\_1000389442) for details.

**OSPF virtual link:** OSPF virtual links configurations will be lost with the update to K.12.01. See the Note under Version K.12.01 Software Fixes on [page 81](#) (PR\_1000374003) for details.

**MSTP auto-edge-port support and default settings:** With version K.12.04, automatic detection of edge ports is supported, along with revised command options and default settings. See Release K.12.04 Enhancements on [page 19](#) (PR\_1000369492) for details.

---

### Related Publications

See "To Download Product Documentation:" on [page 2](#) to get the latest version of these documents.

- *Management and Configuration Guide*
  - *Advanced Traffic Management Guide*
  - *Access Security Guide*
  - *Multicast and Routing Guide*
  - *Command Line Interface Reference Guide*
  - *Log Message Reference Guide*
-

© Copyright 2006-2007 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

## Publication Number

5991-4720  
August 2007

## Applicable Products

ProCurve Switch 3500yl-24G-PWR Intelligent Edge (J8692A)	
ProCurve Switch 3500yl-48G-PWR Intelligent Edge (J8693A)	
ProCurve Switch 6200yl-24G-mGBIC	(J8992A)
ProCurve Switch 5406zl	(J8697A)
ProCurve Switch 5412zl	(J8698A)
ProCurve Switch 5406zl-48G	(J8699A)
ProCurve Switch 5412zl-96G	(J8700A)

## 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](http://www.openssh.com).

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

[www.openssl.org](http://www.openssl.org).

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

## Disclaimer

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

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

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

## Warranty

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

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

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

# Contents

<b>Software Management</b> .....	<b>1</b>
Premium Edge Switch Software Features .....	1
Software Updates .....	1
Downloading Switch Documentation and Software from the Web .....	2
Downloading Software to the Switch .....	3
TFTP Download from a Server .....	4
Xmodem Download From a PC or Unix Workstation .....	4
Using USB to Download Switch Software .....	6
Saving Configurations While Using the CLI .....	7
ProCurve Switch, Routing Switch, and Router Software Keys .....	8
OS/Web/Java Compatibility Table .....	9
Minimum Software Versions .....	9
<b>Support Notes</b> .....	<b>10</b>
Using SNMP To View and Configure Switch Authentication Features .....	10
Known Issues .....	10
<b>Clarifications</b> .....	<b>11</b>
<b>Enhancements</b> .....	<b>12</b>
Release K.11.12 Enhancements .....	12
Release K.11.13 through K.11.32 Enhancements .....	12
Release K.11.33 Enhancements .....	12
Release K.11.34 Enhancements .....	12
Release K.11.35 Enhancements .....	13
Release K.11.36 through K.11.39 Enhancements .....	13
Release K.11.40 Enhancements .....	13
Release K.11.41 Enhancements .....	13
Release K.11.42 Enhancements .....	14
Release K.11.43 Enhancements .....	14
Release K.11.44 Enhancements .....	14

Release K.11.45 Through K.11.47 Enhancements .....	14
Release K.11.48 Enhancements .....	14
Release K.11.49 Enhancements .....	14
Release K.11.60 through K.11.63 Enhancements .....	15
Release K.11.64 Enhancements .....	15
Release K.11.68 Enhancements .....	15
Release K.11.69 Enhancements .....	15
Release K.12.01 Enhancements .....	16
Release K.12.02 Enhancements .....	18
Release K.12.03 Enhancements .....	18
Release K.12.04 Enhancements .....	19
Configuring MSTP Port Connectivity Parameters .....	19
Release K.12.05 Enhancements .....	22
How RADIUS-Based Authentication Affects VLAN Operation .....	22
Release K.12.06 Enhancements .....	29
Saving Security Credentials in a Configuration File .....	29
Release K.12.07 Enhancements .....	43
Release K.12.08 Enhancements .....	43
Configuring a System Contact and Location for the Switch .....	43
Release K.12.09 Enhancements .....	44
Release K.12.10 Enhancements .....	44
show vlan ports CLI Command Enhancement .....	44
Release K.12.11 Enhancements .....	46
Release K.12.12 Enhancements .....	46
Release K.12.13 Enhancements .....	46
Release K.12.14 Enhancements .....	46
Release K.12.15 Enhancements .....	46
Send SNMP v2c Informs .....	46
Enabling and Configuring SNMP Informs .....	46
Release K.12.16 Enhancements .....	48
Release K.12.17 Enhancements .....	48
Release K.12.18 Enhancements .....	48

RADIUS Server Unavailable .....	49
Overview .....	49
Configuring RADIUS Authentication .....	49
Specifying the MAC Address Format .....	52
ARP Age Timer Increase .....	52
Release K.12.19 Enhancements .....	55
Release K.12.20 Enhancements .....	55
Release K.12.21 Enhancements .....	55
Classifier-Based Rate Limiting .....	55
CLI Command for Rate Limiting .....	56
Viewing the RL-PACL Information .....	57
Troubleshooting .....	60
Concurrent TACACS+ and SFTP” .....	61
Release K.12.22 Enhancements .....	61
“OSPF Passive and Routing Interface Increase” .....	61
Release K.12.23 Enhancements .....	63
Web Auth Secure Protocol .....	63
Release K.12.24 Enhancements .....	64
Release K.12.25 Enhancements .....	64
<b>Software Fixes in Release K.11.12 - K.12.25 .....</b>	<b>65</b>
Release K.11.12 .....	65
Release K.11.13 .....	66
Release K.11.14 .....	66
Release K.11.15 .....	66
Release K.11.16 .....	67
Release K.11.17 .....	67
Release K.11.32 .....	67
Release K.11.33 .....	70
Release K.11.34 .....	71
Release K.11.35 .....	71
Release K.11.36 .....	72

Release K.11.37 .....	72
Release K.11.38 .....	72
Release K.11.39 .....	72
Release K.11.40 .....	73
Release K.11.41 .....	73
Release K.11.43 .....	73
Release K.11.44 .....	74
Release K.11.46 .....	74
Release K.11.47 .....	75
Release K.11.48 .....	75
Release K.11.49 .....	75
Release K.11.61 .....	76
Release K.11.62 .....	76
Release K.11.63 .....	77
Release K.11.64 .....	77
Version K.11.65 .....	78
Version K.11.66 .....	78
Version K.11.67 .....	79
Version K.11.68 .....	79
Version K.11.69 .....	80
Version K.12.01 .....	80
Version K.12.02 .....	81
Version K.12.03 .....	82
Version K.12.04 .....	83
Version K.12.05 .....	84
Version K.12.06 .....	84
Version K.12.07 .....	84
Version K.12.08 .....	85
Version K.12.09 .....	85
Version K.12.10 .....	85
Version K.12.11 .....	86

Version K.12.12 .....	86
Version K.12.13 .....	86
Version K.12.14 .....	86
Version K.12.15 .....	87
Version K.12.16 .....	88
Version K.12.17 .....	88
Version K.12.18 .....	88
Version K.12.19 .....	89
Version K.12.20 .....	90
Version K.12.21 .....	90
Version K.12.22 .....	91
Version K.12.23 .....	91
Version K.12.24 .....	92
Version K.12.25 .....	92

# Software Management

---

## Premium Edge Switch Software Features

The ProCurve 3500yl and 5400zl switches ship with the ProCurve Intelligent Edge software feature set. The additional Premium Edge switch software features for the 3500yl and 5400zl switches can be acquired by purchasing the optional Premium Edge license and installing it on the Intelligent Edge version of these switches. As of February, 2007, the Premium Edge features include the following:

- OSPF
- PIM Dense mode
- PIM Sparse mode
- VRRP

Part numbers for the Premium Edge licenses are:

- 3500yl switches: J8993A
- 5400zl switches: J8994A

The ProCurve 6200yl switch is available only as a Premium Edge switch.

To purchase a Premium Edge license, go to the following web page and click on How To Buy.

[www.hp.com/rnd/accessories/J8994A/accessory.htm](http://www.hp.com/rnd/accessories/J8994A/accessory.htm)

To view or download a listing of Intelligent Edge and Premium Edge features, refer to the "Software Features Index" available for download on the product documentation page for your switch model:

- [ProCurve Switch 3500yl and 6200yl series](#)
- [ProCurve Switch 5400zl series](#)

---

### **Note:**

Switch software Version K.11.33 software or newer is required for proper functioning of Intelligent Edge features on ProCurve Switch 3500yl series, and ProCurve Switch 5400zl series

---

## 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](http://www.procurve.com).
2. Click on **Software updates** (in the sidebar).
3. Under **Latest software**, click on **Switches**.

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

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

## Downloading Software to the Switch

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

- For a TFTP transfer from a server, do either of the following:
  - 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 USB port to download a software file from a USB flash drive (page 6).
- 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 K\_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 K_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:
  - a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
  - b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

**Syntax:** boot system flash [ < primary | 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.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the Software revision field.

## 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.

## Using USB to Download Switch Software

To use the USB port on the switch to download a software version from a USB flash drive:

- The software version must be stored on the USB flash drive, and you must know the file name (such as K\_12\_10.swi).
- The USB flash drive must be properly installed in the USB port on the switch.

---

### Note

Some USB flash drives may not be supported on your switch. For information on USB device compatibility, refer to the HP ProCurve support website: <http://www.hp.com/rnd/support/faqs/index.htm>.

---

**Syntax:** copy usb flash <filename> [ < primary | secondary > ]

For example, to download a software file named K\_12\_10.swi from a USB flash drive:

1. Execute the copy command as shown below:

```
ProCurve # copy usb flash K_12_10.swi secondary
The Ssecondary 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:

- a. Use the **show flash** command to verify that the new software version is in the expected flash area (primary or secondary)
- b. Reboot the switch from the flash area that holds the new software (primary or secondary), using the following command:

**Syntax:** boot system flash [ < primary | 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.

4. Verify the software version by displaying the system information for the switch (for example, through the **show system-information** command), and viewing the Software revision field.

## 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

<b>Software Letter</b>	<b>ProCurve Networking Products</b>
<b>C</b>	1600M, 2400M, 2424M, 4000M, and 8000M
<b>CY</b>	Switch 8100fl Series (8108fl and 8116fl)
<b>E</b>	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
<b>F</b>	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
<b>G</b>	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
<b>H</b>	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
<b>I</b>	Switch 2800 Series (2824 and 2848)
<b>J</b>	Secure Router 7000dl Series (7102dl and 7203dl)
<b>K</b>	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G)
<b>L</b>	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
<b>M</b>	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.
<b>N</b>	Switch 2810 Series (2810-24G and 2810-48G)
<b>PA/PB</b>	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
<b>Q</b>	Switch 2510 Series (2510-24)
<b>T</b>	Switch 2900 Series (2900-24G, and 2900-48G)
<b>VA/VB</b>	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
<b>WA</b>	ProCurve Access Point 530
<b>WS</b>	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
<b>numeric</b>	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	

## Minimum Software Versions

**For ProCurve Series 3500yl, 6200yl, and 5400zl Switches and Hardware Features**

ProCurve Device	Minimum Supported Software Version
100-FX SFP-LC Transceiver (J9054B)	K.12.01
Intelligent Edge Features on Series 3500yl and 5400zl Switches	K.11.33
Switch 5400zl 24p Mini-GBIC Module (J8706A)	K.11.33
Switch 5400zl 4p 10-GbE CX4 Module (J8708A)	K.11.33
Switch 6200yl-24G-mGBIC (J8992A)	K.11.33
Switch 3500yl 2p 10GbE X2 + 2p CX4 Module (J8694A).	K.11.17



# Support Notes

---

## Using SNMP To View and Configure Switch Authentication Features

Beginning with software release K.12.01, manager read/write access is available for a subset of the SNMP MIB objects for switch authentication (hpSwitchAuth) features. That is, in the default state, a device with management access to the switch can view the configuration for several authentication features, and using SNMP sets, can change elements of the authentication configuration.

---

### Security Note

In the default configuration for SNMP MIB object access, SNMP sets can be used to reconfigure password and key MIB objects. This means that a device operating as a management station with access to the switch can be used to change the SNMP MIB settings. This can pose a security risk if the feature is used to incorrectly configure authentication features or to reconfigure authentication features to unauthorized settings.

---

If you want to block the SNMP MIB object access described above, use the following command to disable the feature:

```
ProCurve(config)# snmp-server mib hpswitchauthmib excluded
```

For more information on the above topic, refer to "Using SNMP To View and Configure Switch Authentication Features" in the "RADIUS Authentication and Accounting" chapter of the *Access Security Guide* for your switch. For an overview of the security features available on the switch, refer to chapter 1, "Security Overview", in the *Access Security Guide* for your switch.

---

## Known Issues

The following are Known Issues in release K.12.01 or newer, and are not yet resolved.

- **Resources (PR\_1000388697)** — When the switch is writing large files to flash (for example, a transfer of a very large configuration or a software update), switch resources may be impacted during the write operation, causing some potential loss of hello packets. This may impact VRRP, OSPF or spanning tree protocol. In order to mitigate potentially undesirable affects, updates to the switch software should be made during a scheduled downtime. Increasing the hello interval of time sensitive protocols may also assist with mitigation of this issue.

# Clarifications

---

The following clarification or updates apply to documentation for the ProCurve 3500yl Series, 6200yl Series, and 5400zl Series switches as of February 2007.

■ **Enabling Jumbo Frames and Flow Control:**

The 3500yl, 5400zl, and 6200yl switches support simultaneous use of Jumbo Frames and Flow Control. (The earlier version of the *Management and Configuration Guide* incorrectly stated that these features could not be enabled at the same time.)

■ **Clarification for the Number of IP addresses and maximum VLANs** that can be configured on the switch:

You can configure a maximum of 512 routed VLANs per switch. A VLAN can be configured with up to 32 IP addresses. However, the maximum number of IP addresses configurable on the switch is 2048, so it is not possible to configure up to the maximum number of routed VLANs (512) with 32 IP addresses each. For example, if you wanted to use all available IP addresses for the switch and utilize all 512 possible routed VLANs with as many assigned IP addresses as possible, the configuration is calculated as follows:

512 routed VLANs x 4 IP addresses per VLAN = 2048 total IP addresses.

(refer to the *Advanced Traffic Management Guide* for additional details)

■ **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.

■ **RIP and OSPF Redistribution:**

RIP operation supports static, connected, and OSPF route redistribution. OSPF operation supports static, connected, and RIP route redistribution. (The earlier version of the *Advanced Traffic Management Guide* omitted RIP and OSPF route redistribution.)

■ **Maximum UDP Broadcast Forwarding Entries:**

The number of UDP broadcast entries and IP helper addresses combined can be up to 16 per VLAN, with an overall maximum of 2048 on the switch. The *Multicast and Routing Guide* (page 5-142) incorrectly states that the overall maximum is 256.

# Enhancements

---

Unless otherwise noted, each new release includes the enhancements added in all previous releases. Enhancements are listed in chronological order, oldest to newest software release. To review a summary of enhancements included since the last general release that was published, begin with “[Release K.12.06 Enhancements](#)” on page 29.

Descriptions and detailed instructions for enhancements included in Release K.12.xx or earlier are included in the latest release of manuals for the ProCurve 3500yl, 6200yl, and 5400zl Series switches (February 2007), available on the web at [www.hp.com/rnd/support/manuals](http://www.hp.com/rnd/support/manuals).

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.11.69 is the last release of the K.11.xx software. The 3500yl, 6200yl, and 5400zl switch software code was rolled to the K.12.0x code branch with no intervening releases.

## Release K.11.12 Enhancements

Release K.11.12 includes the following enhancement:

- MSTP Enhancement Implementation of legacy path cost MIB and CLI option for MSTP.

## Release K.11.13 through K.11.32 Enhancements

*No enhancements, software fixes only.*

## Release K.11.33 Enhancements

- With the K.11.33 software release, support for the following ProCurve products was added:
  - J8698A / J8700A(bundle) for the ProCurve switch 5412zl
  - J8706A - ProCurve Switch 5400zl 24p Mini-GBIC Module
  - J8708A - ProCurve Switch 5400zl 4p 10-GbE CX4 Module
  - J8992A - ProCurve Switch 6200yl-24G-mGBIC

## Release K.11.34 Enhancements

Release K.11.34 includes the following enhancements:

- **Increased number of telnet/SSH sessions:** The maximum number of simultaneous telnet/SSH sessions has been increased from three to five. The CLI commands **show telnet** and **show ip ssh** now report on five sessions rather than just three.
- **CLI-configured sFlow with multiple instances:** In earlier software releases, the only method for configuring sFlow on the switch was via SNMP using only a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to

## Enhancements

### Release K.11.35 Enhancements

three distinct sFlow instances. For more information, refer to the section on “CLI-Configured sFlow with Multiple Instances” in the chapter titled “Configuring for Network Management Applications” in the *Management and Configuration Guide* for your switch.

- **Event log display options:** Two new options have been added to provide greater flexibility in viewing event log entries via the CLI. The **show logging** command now includes an option to reverse the standard display, and a **clear logging** command has been added to remove all event log entries from the **show logging** display output. For more information, refer to the section on “Using the Event Log To Identify Problem Sources” in the Appendix titled “Troubleshooting” in the *Management and Configuration Guide* for your switch.
- **Scheduled reload:** Additional parameters have been added to the **reload** command to allow for a scheduled reboot of the switch via the CLI. For more information, refer to the section on “Rebooting your Switch” in the Chapter titled “Switch Memory and Configuration” in the *Management and Configuration Guide* for your switch.
- **Real-time rate display:** The **show interface port-utilization** command provides a real-time rate display for all ports on the switch.

## Release K.11.35 Enhancements

Release K.11.35 includes the following enhancement:

- Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.

## Release K.11.36 through K.11.39 Enhancements

*No new enhancements, software fixes only.*

## Release K.11.40 Enhancements

Release K.11.40 includes the following enhancement:

- **RSTP/MSTP BPDU Protection:** When this feature is enabled on a port, the switch will disable (drop the link) of a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP trap.

## Release K.11.41 Enhancements

Release K.11.43 includes the following enhancement:

- Added support for Unidirectional Fiber Break Detection (UDLD).

## Release K.11.42 Enhancements

*No enhancements, software fixes only.*

## Release K.11.43 Enhancements

Release K.11.43 includes the following enhancement:

- 802.1X Controlled Directions enhancement. With this change, Administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.

## Release K.11.44 Enhancements

Release K.11.44 includes the following enhancement:

- Loop Protection enhancement allows STP to detect and block network topology loops on a single port.

## Release K.11.45 Through K.11.47 Enhancements

*No enhancements, software fixes only.*

## Release K.11.48 Enhancements

Release K.11.48 includes the following enhancement:

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

## Release K.11.49 Enhancements

Release K.11.49 includes the following enhancement:

- DHCP Protection (Snooping) enhancement.

## Enhancements

Release K.11.60 through K.11.63 Enhancements

### Release K.11.60 through K.11.63 Enhancements

*No enhancements, software fixes only.*

- Versions K.11.50 through K.11.59 were never built.
- Version K.11.60 was never released.

### Release K.11.64 Enhancements

Release K.11.64 includes the following enhancement:

- 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 K.11.68 Enhancements

Release K.11.68 includes the following enhancement:

- Improved SFlow function to accommodate bursty traffic.

### Release K.11.69 Enhancements

*No new enhancements, software fixes only.*

Release K.11.69 is the last release of the K.11.xx software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0x code branch with no intervening releases.

## Release K.12.01 Enhancements

Release K.12.01 is a major software update containing many new features and enhancements to existing features. The following updates have been documented in the latest revisions to the manuals (February 2007). Refer to the manuals for additional details.

Software Manual/ Enhancements	Description
<i>Management and Configuration Guide</i>	
<b>Bi-directional Rate Limiting:</b>	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
<b>Loopback Interface:</b>	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.
<b>USB Support</b>	Provides an option for using a USB device as a source or destination for file transfers. Refer to "Using USB To Download Switch Software" in the "File Transfers" appendix of the <i>Management and Configuration Guide</i> for your switch (February 2007 or newer). For information on USB device compatibility on the 3500yl, 5400zl, and 6200yl switches, refer to the HP ProCurve support website: <a href="http://www.hp.com/rnd/support/faqs/index.htm">http://www.hp.com/rnd/support/faqs/index.htm</a> .
<b>Intelligent Mirroring</b>	Enables copying of network traffic from a network interface to a local or remote exit port where a host such as a traffic analyzer or intrusion detection system (IDS) is connected.
<b>DNS Resolver</b>	Used in local network domains to enable the use of a hostname or fully-qualified domain name to perform ping and traceroute operations from the switch.
<b>SNMP-Server Source IP Commands:</b>	Provides added security by allowing you to send SNMP replies from the same IP address as the one on which the corresponding SNMP request was received.
<b>SNMPv3 AES Support:</b>	Authentication and privacy for SNMPv3 users has been enhanced to support AES 128-bit encryption as a privacy protocol in SNMPv3 messages in compliance with RFC 3826.
<i>Multicast and Routing Guide</i>	
<b>OSPF NSAA:</b>	Support for Not-So-Stubby-Areas (NSAA).
<b>DHCP Relay:</b>	Enhancements to the DHCP Relay feature allow you to disable the hop count in DHCP requests, and enable support for up to 2048 IP helper addresses of DHCP servers.

Software Manual/ Enhancements	Description
<i>Advanced Traffic Management Guide</i>	
<b>Qos Queue Config:</b>	Allows you to reduce the number of outbound queues that all switch ports will use to buffer packets for 802.1p user priorities.
<b>Number of Default VLANs:</b>	In the factory default state, support has been increased from 8 VLANs to 256 VLANs. (You can reconfigure the switch to support up to 2048 (vids up to 4094) VLANs.)
<b>Migrating Layer 3 VLANs Using VLAN MAC Configuration:</b>	Allows you to upgrade to ProCurve routing switches without stopping the operation of attached hosts that use existing routers as their default gateway to route traffic between VLANs.
<i>Access Security Guide</i>	
<b>RADIUS AAA:</b>	Provides client-level security that allows LAN access to individual 802.1X clients (up to 32 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.
<b>SNMP Access to Switch Authentication features:</b>	Enables manager read/write access for a subset of the SNMP MIB objects for switch authentication features. <b>Security Note:</b> Downloading and booting software release K.12.01 or greater for the first time automatically enables SNMP access to the hpSwitchAuth MIB objects. For more information, or to disable this feature see <a href="#">"Support Notes" on page 10</a> for details.
<b>Password Set via SNMP:</b>	Allows configuration of username and password via SNMP.
<b>Client-based Access Control:</b>	In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. This enhancement allows you to configure outbound rate-limiting for all traffic on a port, and specify bandwidth usage in terms of bits per second (bps).
<b>Virus Throttling on Bridged Traffic:</b>	This enhancement allows connection-rate filtering on all IP traffic (not just routed traffic as in earlier releases).
<b>ACLs on Port Traffic and Bridged Traffic:</b>	Allows configuration of ACLs to filter traffic entering the switch on a VLAN or port.
<b>Dynamic ARP Protection:</b>	Protects your network from ARP cache poisoning by dropping packets, with an invalid IP-to-MAC address binding, that are received on untrusted ports.
<b>Instrumentation Monitor:</b>	Protects your network from a variety of common attacks by generating alerts for detected anomalies on the switch.



Software Manual/ Enhancements	Description
<p><b>Controlled Directions Web/MAC Auth:</b></p>	<p>Allows you to use the <code>aaa port-access controlled-directions</code> command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state. This feature is available for both 802.1X and Web/MAC authorization.</p>
<p><b>Note on Manual Updates:</b> In addition to the above updates to the manuals, the chapter on ACLs has been moved from the <i>Advanced Traffic Management Guide</i> to the <i>Access Security Guide</i>. The <i>Access Security Guide</i> also provides a new introductory "Security Overview" chapter, plus a new chapter on "Advanced Threat Protection" covering topics such as DHCP Snooping and Dynamic Arp Protection.</p>	

In addition to the updates listed above, K.12.01 also provides the following enhancements:

- **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 the ProCurve 100-FX SFP-LC Transceiver (J9054B).
- **Enhancement (PR\_1000376626)** — Enhance 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 K.12.02 Enhancements

*No enhancements, software fixes only.*

## Release K.12.03 Enhancements

Release K.12.03 includes the following enhancements:

- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the `show tech` command output.
- **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.
- **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.

```
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 TCP/UDP Priority” in the *Advanced Traffic Management Guide*.

## Release K.12.04 Enhancements

Release K.12.04 includes the following enhancement:

- **Enhancement MSTP (PR\_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution. For more information on selected configuration options and updated MSTP port parameters, see “[Configuring MSTP Port Connectivity Parameters](#)” below.

### Configuring MSTP Port Connectivity Parameters

With release K.12.04, all ports are configured as auto-edge-ports by default, and the spanning tree **edge-port** option has been removed. This section describes selected **spanning-tree <port-list>** command parameters for enhanced operation.

Basic port connectivity parameters affect spanning-tree links at the global level. Therefore, in most cases, ProCurve recommends that you use the revised default settings for these parameters and apply changes on a per-port basis only where a non-default setting is clearly indicated by the circumstances of individual links (for example, see the **root-guard** option below).

To display the spanning-tree settings for each port, use the **show spanning-tree config** command.

**Syntax:** [no] spanning-tree < port-list > < auto-edge-port | admin-edge-port | mcheck | root-guard | tcn-guard >

[auto-edge-port ]

*Enables **auto-edge-port** operation for MSTP, and supports the automatic detection of edge ports. (Default: **Yes**, enabled)*

*The port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets. If **admin-edge-port** is enabled for a port, the setting for **auto-edge-port** is ignored whether set to yes or no. If **admin-edge-port** is disabled, and **auto-edge-port** has not been disabled, then the **auto-edge-port** setting controls the behavior of the port.*

*The **no spanning-tree < port-list > auto-edge-port** command disables **auto-edge-port** operation on the specified ports.*

[ admin-edge-port ]

*Enables **admin-edge-port** for RSTP/MSTP. If a bridge or switch is detected on the segment, the port automatically operates as non-edge, not enabled. (Default: **No** - disabled)*

*If **admin-edge-port** is disabled on a port and **auto-edge-port** has not been disabled, the **auto-edge-port** setting controls the behavior of the port.*

*The **no spanning-tree < port-list > admin-edge-port** command disables **admin-edge-port** operation on the specified ports.*

[mcheck ]

*Forces a port to send RSTP/MSTP BPDUs for 3 seconds. This allows for another switch connected to the port and running RSTP to establish its connection quickly and for identifying switches running 802.1D STP. If the whole-switch force-version parameter is set to stp-compatible, the switch ignores the mcheck setting and sends 802.1D STP BPDUs out all ports.*

[root-guard]

*MSTP only. 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. The BPDUs received on a **root-guard** port are ignored. All other BPDUs are accepted and the external devices may belong to the spanning tree as long as they do not claim to be the Root device. (Default: **No** - disabled)*

***Note:** In standard Spanning Tree Protocol operation, the calculation of active network topologies may be an issue when switches outside the core region of a network are under shared or limited administrative control. Such a switch may become a Root Bridge for the entire network and create non-optimal forwarding paths. By enabling the **root-guard** feature on ports that face outside the core network, external boundaries for the core network are created to ensure the Root Bridge is located within the core network.*

[tcn-guard]

*When **tcn-guard** is enabled for a port, it causes the port to stop propagating received topology change notifications and topology changes to other ports. (Default: **No** - disabled)*

**Syntax:** spanning-tree < port-list > < hello-time | path-cost | point-to-point-mac | priority >

[ hello-time < global | 1 - 10 >

*When the switch is the CIST root, this parameter specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports. This interval also applies to all ports in all switches downstream from each port in the < port-list >. A setting of **global** indicates that the ports in < port-list > on the CIST root are using the value set by the global spanning-tree **hello-time** value. When a given switch "X" is not the CIST root, the per-port **hello-time** for all active ports on switch "X" is propagated from the CIST root, and is the same as the **hello-time** in use on the CIST root port in the currently active path from switch "X" to the CIST root. (That is, when switch "X" is not the CIST root, then the upstream CIST root's port **hello-time** setting overrides the **hello-time** setting configured on switch "X". (Default Per-Port setting: **Use Global**. Default Global Hello-Time: **2**.)*

[ path-cost < auto | 1..200000000 > ]

*Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree. In the default configuration (auto) the switch determines a port's path cost by the port's type:*

- 10 Mbps: **2000000**
- 100 Mbps: **200000**
- 1 Gbps: **20000**

point-to-point-mac <true | false | auto >

*This parameter informs the switch of the type of device to which a specific port connects.*

**True (default):** Indicates a point-to-point link to a device such as a switch, bridge, or end-node.

**False:** Indicates a connection to a hub (which is a shared LAN segment).

**Auto:** Causes the switch to set False on the port if it is not running at full duplex. (Connections to hubs are half-duplex.)

priority <0..15 >

*MSTP uses this parameter to determine the port(s) to use for forwarding. The port with the lowest assigned value has the highest priority. While the actual priority range is 0 to 240, this command specifies the priority as a multiplier (0-15) of 16. That is, when you specify a priority multiplier of 0-15, the actual priority assigned to the switch is:*

*(priority-multiplier) x 16 = priority*

*The default priority-multiplier value is 8.*

*For example, if you configure “2” as the priority multiplier for a given port, then the actual priority is 32. Thus, after you specify the port priority multiplier, the switch displays the actual port priority (and not the multiplier) in the **show spanning-tree config** display. You can view the actual multiplier setting for ports by executing **show running** and looking for an entry in this form:*

*spanning-tree <port-list> priority <priority-multiplier>*

*For example, configuring port 2 with a priority multiplier of “3” results in this line in the **show running-config** output:*

*spanning-tree B2 priority 3*

## Release K.12.05 Enhancements

Release K.12.05 includes the following enhancement:

- **Enhancement (PR\_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. 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 32 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 User-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 28](#).
- 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 25](#)), 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 A2 has been authenticated by a RADIUS server for access to VLAN 22. However, port A2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in [Figure 1](#).

```

===== CONSOLE - MANAGER MODE =====
Switch Configuration - VLAN - VLAN Port Assignment

Port  default_vlan  vlan_22  vlan_33  vlan_44
----+-----
A1   | Untagged      Tagged   No       No
A2   | No            No       Untagged No
A3   | Untagged      Forbid  Forbid   Forbid
A4   | Untagged      Tagged  Tagged   Tagged
  :   | :             :       :       :
  :   | :             :       :       :
Actions->  Cancel  Edit    Save    Help
Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute
  
```

**Scenario:** An authorized 802.1X client requires access to VLAN 22 from port A2. However, access to VLAN 22 is blocked (not untagged or tagged) on port A2 and VLAN 33 is untagged on port A2.

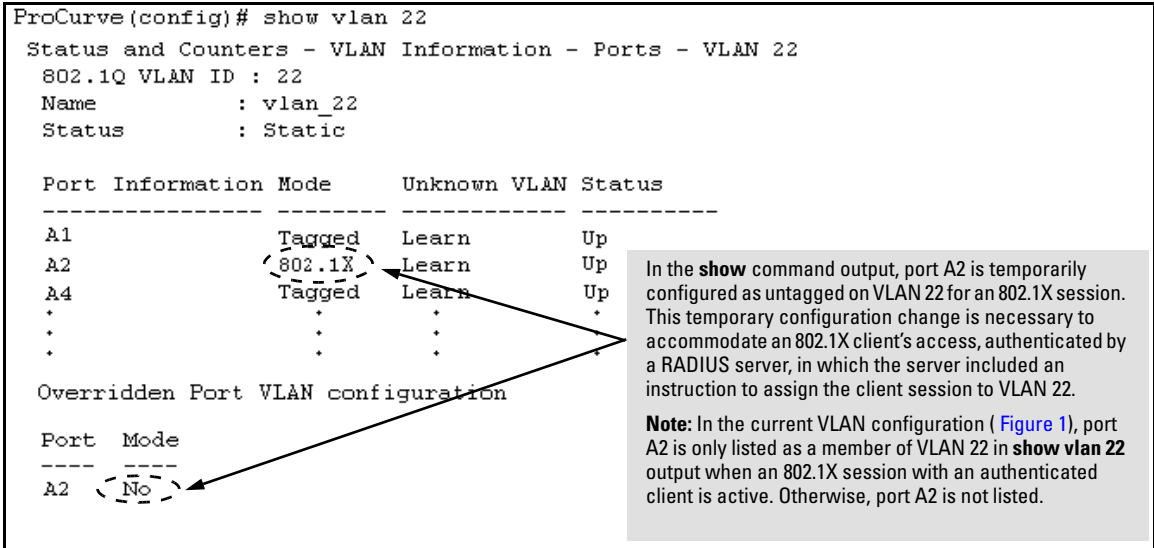
**Figure 1. Example of an Active VLAN Configuration in the Menu Interface View**

In [Figure 1](#), if RADIUS authenticates an 802.1X client on port A2 with the requirement that the client use VLAN 22, then:

- VLAN 22 becomes available as Untagged on port A2 for the duration of the session.
- VLAN 33 becomes unavailable to port A2 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.

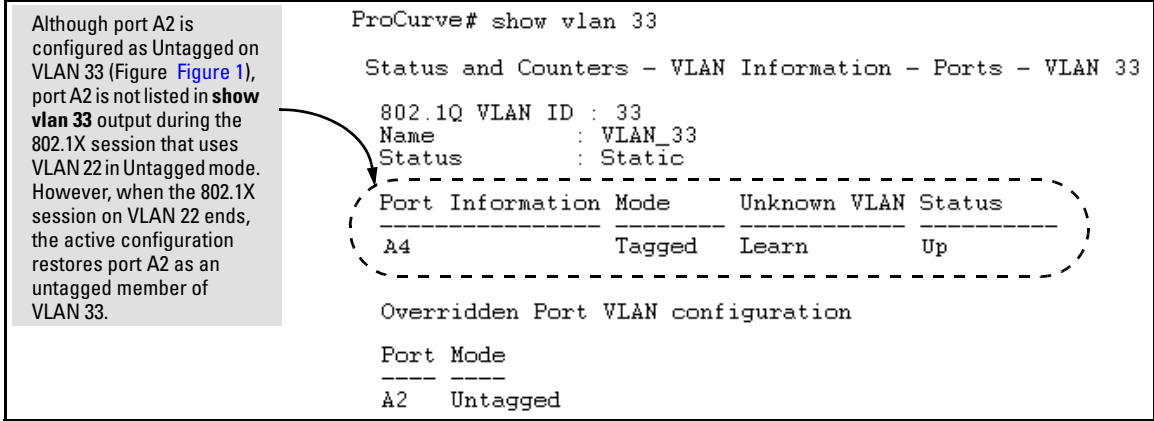




**Figure 2. Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session**

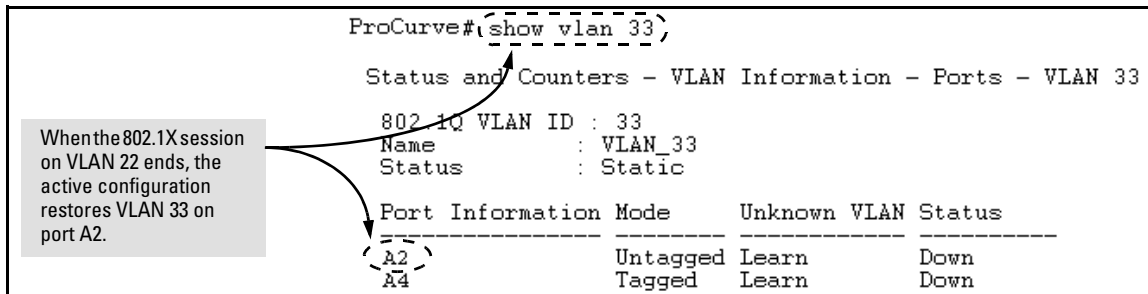
However, as shown in [Figure 1](#), because VLAN 33 is configured as untagged on port A2 and because a port can be untagged on only one VLAN, port A2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of 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 22 for the 802.1X Session**

When the 802.1X client session on port A2 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 A2 ends, VLAN 22 access on port A2 also ends, and the untagged VLAN 33 access on port A2 is restored as shown in [Figure 4](#).



**Figure 4. The Active Configuration for VLAN 33 Restores Port A2 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.*

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 from 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-Based Authentication Affects VLAN Operation” section in the “RADIUS Authentication and Accounting” chapter of the Access Security Guide.*

## Release K.12.06 Enhancements

Release K.12.06 includes the following enhancement:

- **Enhancement (PR\_1000308332)**— Passwords (hashed) can be saved to the configuration file.

### Saving Security Credentials in a Configuration File

In software release K.12.06 and greater, you can store and view the following security settings in the running-config file associated with the current software image by entering the **include-credentials** command. Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.

- Local manager and operator passwords and (optional) user names that control access to a management session on the switch through the CLI, menu interface, or web browser interface
- SNMP security credentials used by network management stations to access a switch, including authentication and privacy passwords
- Port-access passwords and usernames used as 802.1X authentication credentials for access to the switch
- TACACS+ encryption keys used to encrypt packets and secure authentication sessions with TACACS+ servers
- RADIUS shared secret (encryption) keys used to encrypt packets and secure authentication sessions with RADIUS servers
- Secure Shell (SSH) public keys used to authenticate SSH clients that try to connect to the switch.

### Benefits of Saving Security Credentials

The benefits of including and saving security credentials in a configuration file are as follows:

- After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.
- By permanently saving a switch's security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the ProCurve switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.

- By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files by changing the configuration file used when you reboot the switch.

For more information about how to experiment with, upload, download, and use configuration files with different software versions, refer to the following chapters:

- “Switch Memory and Configuration” and “File Transfers” in the *Management and Configuration Guide*
- “Configuring Username and Password Security” in the *Access Security Guide*

### **Security Settings that Can Be Saved**

This section describes the security settings that can be saved to a configuration file in software release K.12.06 and greater:

- Local manager and operator passwords and user names
- SNMP security credentials, including SNMPv1 community names and SNMPv3 usernames, authentication, and privacy settings
- 802.1X port-access passwords and usernames
- TACACS+ encryption keys
- RADIUS shared secret (encryption) keys
- Public keys of SSH-enabled management stations that are used by the switch to authenticate SSH clients that try to connect to the switch

### **Local Manager and Operator Passwords**

In software releases earlier than K.12.06, the manager and operator passwords and user names used to start a management session on the switch are treated as follows:

- You set the passwords and (optional) user names using the CLI or menu interface as described in “Configuring Local Password Security” in the *Access Security Guide*.
- Only the following information is saved to the running configuration:

```
password manager [user-name <name>]
password operator [user-name <name>]
```

In software release K.12.06 and greater, you cannot view the configured local password settings in plain text. However, by entering the **include-credentials** command described later, you can view a hash of the local password settings in the running-config file, in the format:

```
password manager [user-name <name>] <hash-type> <pass-hash>
password operator [user-name <name>] <hash-type> <pass-hash>
```

Where:

<name> is an alphanumeric string for the user name assigned to the manager or operator.

<hash-type> indicates the type of hash algorithm used: SHA-1.

<pass-hash> is the SHA-1 authentication protocol's hash of the password.

For example, a manager username and password may be stored in a running-config file as follows:

```
password manager user-name Spock SHA1
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

If you permanently save password configurations in the startup-config file by entering the **write memory** command, the passwords take effect when a switch boots with the software version associated with the configuration file.

---

## Caution

If a startup configuration file does not contain a manager or operator password, the switch will not have password protection and can be accessed through Telnet, the serial port, or web interface with full manager privileges.

---

## Password Command

In software release K.12.06 and greater, the **password** command in the CLI is enhanced to support the following syntax:

**Syntax:** [no] password <manager | operator | port-access> [user-name <name>] <hash-type> <password>

Where:

- **manager** configures access to the switch with manager-level privileges.
- **operator** configures access to the switch with operator-level privileges.
- **port-access** configures access to the switch through 802.1X authentication with operator-level privileges.
- **user-name <name>** is the (optional) text string of the user name associated with the password.

- The **<hash-type>** parameter specifies the type of algorithm (if any) used to hash the password. Valid values are **plaintext** or **sha-1**.
- The **<password>** parameter is the clear ASCII text string or SHA-1 hash of the password.  
You can enter a manager/operator password in clear ASCII text or hashed format, while the port-access password must be clear ASCII text only. Manager and operator passwords are displayed and saved in a configuration file only in hashed format; port-access passwords are displayed and saved only as plain ASCII text.

After you enter the complete command syntax that includes the password, the password is set and you are not prompted to enter the password a second time.

This command enhancement allows you to configure manager, operator, and 802.1X port-access passwords using the CLI in only one step (instead of entering the **password** command and then being prompted twice to enter the actual password, as in software releases earlier than K.12.06).

- For more information about configuring local manager and operator passwords, refer to the “Configuring Username and Password Security” chapter in the *Access Security Guide*.
- For more information about configuring a port-access password for 802.1X client authentication, see “[802.1X Port-Access Credentials](#)” on page 33.

## SNMP Security Credentials

In software releases earlier than K.12.06, SNMP security credentials are saved in a configuration file as follows:

- SNMPv1 community names and write-access settings are saved as shown in the following example:

```
snmp-server community "vulcan" Unrestricted
```

- SNMPv3 authorization and privacy protocols and passwords used with each SNMPv3 user are not saved. However, SNMPv3 user names are saved; for example:

```
snmpv3 user "initial"
```

In software release K.12.06 and greater, SNMPv1 community names and write-access settings, and SNMPv3 usernames are still saved in the running configuration when you enter the **include-credentials** command.

In addition, the following SNMPv3 security parameters are also saved:

```
snmpv3 user "<name>" [auth <md5|sha> "<auth-pass>"] [priv "<priv-pass>"]
```

Where:

**<name>** is the name of an SNMPv3 management station.

**auth <md5 | sha>** is the (optional) authentication method used for the management station.

**<auth-pass>** is the hashed authentication password used with the configured authentication method. **priv** "**<priv-pass>**" is the (optional) hashed privacy password used by a privacy protocol to encrypt SNMPv3 messages between the switch and the station.

The following example shows the additional security credentials for SNMPv3 users that can be saved in a running-config file:

```
snmpv3 user boris \  
auth md5 "9e4cfef901f21cf9d21079debeca453" \  
priv "82ca4dc99e782db1a1e914f5d8f16824"  
  
snmpv3 user alan \  
auth sha "8db06202b8f293e9bc0c00ac98cf91099708ecdf" \  
priv "5bc4313e9fd7c2953aaa9406764fe8bb629a538"
```

**Figure 5. Security Credentials for SNMPv3**

Although you can enter an SNMPv3 authentication or privacy password in either clear ASCII text or the SHA-1 hash of the password, the password is displayed and saved in a configuration file only in hashed format, as shown in the preceding example.

For more information about the configuration of SNMP security parameters, refer to the “Configuring for Network Management Applications” chapter in the *Management and Configuration Guide*.

### 802.1X Port-Access Credentials

In software release K.12.06 and greater, 802.1X authenticator (port-access) credentials can be stored in a configuration file.

802.1X *authenticator* credentials are used by a port to authenticate supplicants requesting a point-to-point connection to the switch. 802.1X *supplicant* credentials are used by the switch to establish a point-to-point connection to a port on another 802.1X-aware switch. Only 802.1X authenticator credentials are stored in a configuration file. For information about how to use 802.1X on the switch both as an authenticator and a supplicant, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

In software release K.12.06 and greater, the local password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access**) is introduced to configure the local operator username and password used as 802.1X authentication credentials for access to the switch.

The **password port-access** values are now configured separately from the manager and operator passwords configured with the **password manager** and **password operator** commands and used for management access to the switch. For information on the new **password** command syntax, see “Password Command” on page 31.



After you enter the complete **password port-access** command syntax, the password is set. You are not prompted to enter the password a second time.

### **TACACS+ Encryption Key Authentication**

You can use TACACS+ servers to authenticate users who request access to a switch through Telnet (remote) or console (local) sessions. TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local manager and operator passwords configured on the switch.

When you configure TACACS+, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so.

For improved security, you can configure a global or server-specific encryption key that encrypts data in TACACS+ packets transmitted between a switch and a RADIUS server during authentication sessions. The key configured on the switch must match the encryption key configured in each TACACS+ server application. (The encryption key is sometimes referred to as “shared secret” or “secret” key.) For more information, refer to the “TACACS+ Authentication” chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, the global and server-specific TACACS+ encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show tacacs** command.

In software release K.12.06 and greater, TACACS+ shared secret (encryption) keys can be saved in a configuration file with the following syntax:

```
tacacs-server key <keystring>
```

Where:

**<keystring>** is the encryption key (in clear text) used for secure communication with all or a specific TACACS+ server.

### **RADIUS Shared-Secret Key Authentication**

You can use RADIUS servers as the primary authentication method for users who request access to a switch through Telnet, SSH, Web interface, console, or port-access (802.1X). The shared secret key is a text string used to encrypt data in RADIUS packets transmitted between a switch and a RADIUS server during authentication sessions. Both the switch and the server have a copy of the key; the key is never transmitted across the network. For more information, refer to the “RADIUS Authentication and Accounting” chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, the global and server-specific RADIUS encryption keys cannot be saved in a configuration file that can be copied from the switch. These keys are stored only in flash memory and can be viewed by using the **show radius** command.

In software release K.12.06 and greater, RADIUS shared secret (encryption) keys can be saved in a configuration file with the following syntax:

```
radius-server key <keystring>
```

Where:

**<keystring>** is the encryption key (in clear text) used for secure communication with all or a specific RADIUS server.

## SSH Client Public-Key Authentication

Secure Shell version 2 (SSHv2) is used by ProCurve switches to provide remote access to SSH-enabled management stations. Although SSH provides Telnet-like functions, unlike Telnet, SSH provides encrypted, two-way authenticated transactions. SSH client public-key authentication is one of the types of authentication used.

Client public-key authentication uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a public key stored on the switch can gain access at the manager or operator level. For more information about how to configure and use SSH public keys to authenticate SSH clients that try to connect to the switch, refer to the “Configuring Secure Shell” chapter in the *Access Security Guide*.

In software releases earlier than K.12.06, client public-keys that are used to authenticate SSH clients are only stored in flash memory, not in the running-config file. You can view the SSH public keys stored on a switch by entering the **show crypto client-public-key** command. The only SSH security credential that is stored in the running configuration are the following commands:

```
aaa authentication ssh login public-key  
aaa authentication ssh enable public-key
```

- The **aaa authentication ssh login public-key** command allows operator access using SSH public-key authentication.
- The **aaa authentication ssh enable public-key** command allows manager access using SSH public-key authentication.

In software release K.12.06 and greater, the SSH security credential that is stored in the running configuration is the syntax of the **ip ssh public-key** command used to authenticate SSH clients for manager or operator access, along with the hashed content of each SSH client public-key. The syntax of the **ip ssh public-key** command is as follows:

```
ip ssh public-key <manager/operator> <keystring>
```

Where:

**manager** allows manager-level access using SSH public-key authentication.

**operator** allows operator-level access using SSH public-key authentication.

**<keystring>** is a legal SSHv2 (RSA or DSA) public key. The text string for the public key must be a single quoted token.

If the keystring contains double-quotes, it can be quoted with single quotes ('*keystring*'). The following restrictions for a keystring apply:

- A keystring cannot contain both single and double quotes.
- A keystring cannot have extra characters, such as a blank space or a new line. However, to improve readability, you can add a backslash at the end of each line.

---

## Note

In software release K.12.01 and earlier, you can add up to ten SSH client public-keys to the switch only by using the **copy** command; for example:

```
$ copy tftp public-key ip-addr filename <managerloperator> [append]
```

If you enter the optional **append** keyword, the transmitted public-keys are added to existing SSH public-key configurations. If you omit the **append** keyword, the transmitted keys overwrite existing SSH public-key configurations.

In software release K.12.06 and greater, the **ip ssh public-key** command allows you to configure only one SSH client public-key at a time. (This command behavior differs from the **copy** command, which in earlier software releases allows you to load up to ten SSH client public-key configurations at once if they are stored in a single file on a TFTP server.) Therefore, the **ip ssh public-key** command behavior includes an implicit append that never overwrites existing public-key configurations on a running switch.

In all software releases, if you download a software configuration file that contains SSH client public-key configurations, the downloaded public-keys overwrite any existing keys, as happens with any other configured values.

---

To display the SSH public-key configurations (72 characters per line) stored in a configuration file, enter the **show config** or **show running-config** command. The following example shows the SSH public keys configured for manager access, along with the hashed content of each SSH client public-key, that are stored in a configuration file:

```
...
include-credentials
ip ssh public-key manager "ssh-dss \
AAAAB3NzaC1kc3MAAACBApWJHSJmTRtpZ9BUNC+ZrsxhMuZEXQhaDME1vc/ \
EvYnTKxQ31bWvr/bT7W58NX/YJ1ZKTV2GZ2QJJCicUUZVWjNFJCSa0v03XS4 \
BhkXjtHhz6gD701otgizU0O6/Xzf4/J9XkJKHkOCnbHIqtB1sbRYBTxj3Nza \
K1ymvIaU09X5TDAAAAFQCpWkxnbwFfTPasXnxfvDuLSxaC7wAAAIASBwxUP \
pv2scqPPXQghgaTkdPwGGtdFW/+K4xRskAnIaxuG0qLbnekohi+ND4TkKZd \
EeidgDh7qHusBhOFXM2g73RpE2rNqQnSf/QV95kdNwWIbxuusBAzvfaJptd \
gca6cYR4xS4TuBcaKiorYj60kk144E1fkDWieQx8zABQAAAIEAu7/1kV0dS \
G0vE0eJD23TLXvu94plXhRKCUCAvyv2UyK+piG+Q1e1w9zSMaxPA1XJzSY/ \
imEp4p6WXEMc10lpXMRnkhnuMMpAPMaQUT8NJTNu6hqf/LdQ2kqZjUuIyV9 \
LWyLg5ybs1kFLeOt0oo2Jbpy+U2e4jh2Bb77sX3G5C0= spock@sfc.gov" \
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAADAQABAAQgQDyO9RDD52JZP8k2F2YZXubgwRAN0R \
JRslEov6y1RK3XkmgVatz1+mspiEmPS4wNK7bX/IoXNdGrGkoE8tPklZOZ \
oqGCf5Zs50PlnkxXvAidFs55AWqOf4MhfCqvtQCelnt6LFh4ZMig+YewgQG \
M6H1geCSLUBXXScipdPHysakw== "TectiaClientKey [1024-bit rsa, \
nobody@testmachine, Mon Aug 15 2005 14:47:34]"
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAAABIwAAAIEA1Kk9sVQ9LJOR6XO/hCMPxbiMNOK8C/ay \
+SQ10qGw+K9m3w3TmCfjh0ud9hivgbFT4F99AgnQkvm2eVsGoTtLRnff7uw \
NmpzqOqpHjD9YzItUgSK1uPuFwXMCHKUGKa+G46A+EWxDAlYpwVIZ697QmM \
qPFj1zdI4sIo5bDett2d0= joe@hp.com"
...
```

**Figure 6. Example of Hashed Content of an SSH Client Public Key**

If a switch configuration contains multiple SSH client public keys, each public key is saved as a separate entry in the configuration file. You can configure up to ten SSH client public-keys on a switch.

## Enabling the Storage and Display of Security Credentials

To enable the security settings described in [“Security Settings that Can Be Saved” on page 30](#) to be included and viewed in the running configuration on the switch, enter the **include-credentials** command.

**Syntax:** [no] include-credentials

*Enables the inclusion and display of the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys in the running configuration. (Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.)*

*To view the currently configured security settings in the running configuration, enter one of the following commands:*

- **show running-config:** *Displays the configuration settings in the current running-config file.*
- **write terminal:** *Displays the configuration settings in the current running-config file. For more information, refer to the “Switch Memory and Configuration” chapter in the Management and Configuration Guide.*

*To copy the contents of the running-config file from the switch to a USB flash memory device, enter the **copy running-config usb** command. For more information, refer to the “File Transfers” appendix in the Management and Configuration Guide.*

*The “no” form of the command disables only the display and copying of these security parameters from the running configuration, while the security settings remain active in the running configuration.*

**Default:** *The security credentials described in [“Security Settings that Can Be Saved” on page 30](#) are not stored in the running configuration.*

## Operating Notes

---

### Caution

- When you first enter the **include-credentials** command to save the additional security credentials to the running configuration, these settings are moved from internal storage on the switch to the running-config file.

You are prompted by a warning message to perform a **write memory** operation to save the security credentials to the startup configuration. The message reminds you that if you do not save the current values of these security settings from the running configuration, they will be lost the next time you boot the switch and will revert to the values stored in the startup configuration.

- When you boot a switch with a startup configuration file that contains the **include-credentials** command, any security credentials that are stored in internal flash memory are ignored and erased. The switch will load only the security settings in the startup configuration file, if any.
- In software releases earlier than K.12.06, configuration changes to some security credentials (described in [“Security Settings that Can Be Saved” on page 30](#)) are applied immediately and saved in internal storage (flash memory) on the switch. They do not require you to enter the **write memory** command to permanently save them in the startup configuration.

However, in software release K.12.06 and greater, this switch behavior changes. Security settings are no longer automatically saved internally in flash memory and loaded with the startup configuration when a switch boots up. The configuration of all security credentials requires that you use the **write memory** command to save them in the startup configuration in order for them to not be lost when you log off or reboot the switch. A warning message reminds you to permanently save a security setting, which was formerly automatically saved in internal flash, after you configure it.

---

- After you enter the **include-credentials** command, the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys are saved in the running configuration.

Use the **no include-credentials** command to disable the display and copying of these security parameters from the running configuration (using the **show running-config** and **copy running-config** commands), without disabling the configured security settings on the switch.

After you enter the **include-credentials** command, you can toggle between the non-display and display of security credentials in **show** and **copy** command output by alternately entering the **no include-credentials** and **include-credentials** commands.

- After you permanently save security configurations to the current startup-config file using the **write memory** command, you can view and manage security settings with the following commands:
  - **show config**: Displays the configuration settings in the current startup-config file.
  - **copy config <source-filename> config <target-filename>**: Makes a local copy of an existing startup-config file by copying the contents of the startup-config file in one memory slot to a new startup-config file in another, empty memory slot.
  - **copy config tftp**: Uploads a configuration file from the switch to a TFTP server.
  - **copy tftp config**: Downloads a configuration file from a TFTP server to the switch.
  - **copy config xmodem**: Uploads a configuration file from the switch to an Xmodem host.
  - **copy xmodem config**: Downloads a configuration file from an Xmodem host to the switch.

For more information, refer to the “Switch Memory and Configuration” chapter in the *Management and Configuration Guide*.

- The switch supports the storage of up to three configuration files. Each configuration file contains its own security credentials and these security configurations may differ. It is the responsibility of the system administrator to ensure that the appropriate security credentials are contained in the configuration file that is loaded with each software image.
  - When you load a configuration file associated with a software release earlier than K.12.06 on a switch running software release K.12.06 or greater, all security credentials in the configuration file are supported.
  - When you load a configuration file associated with a software release K.12.06 or greater on a switch running a software release earlier than K.12.06, all security credentials saved with the **include-credentials** command are rejected as invalid configurations by the earlier software.
- If you have already enabled the storage of security credentials (including local manager and operator passwords) by entering the **include-credentials** command, the **Reset-on-clear** option is disabled. When you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the running configuration. However, the switch does not reboot after the local passwords are erased. (The **reset-on-clear** option normally reboots the switch when you press the Clear button.)

For more information about the **Reset-on-clear** option and other front-panel security features, refer to the “Configuring Username and Password Security” chapter in the *Access Security Guide*.

- If you upgrade ProCurve software on a switch from an earlier software release to software release K.12.06 or greater and then enter the **include-credentials** command, security passwords are managed as follows:
  - The manager password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have a manager password configured.
  - The operator password (if any) in the earlier software version is copied into the running configuration. The other two configuration files, if configured, will not have an operator password configured.
  - No port-access password for 802.1X authentication is configured. The operator password in the earlier software version is not automatically copied as the new port-access password. To configure password access to the switch through 802.1X authentication, use the **password port-access** command as described in [“Password Command” on page 31](#). (It is not recommended that you use the same password for operator console access and for 802.1X port-access authentication.)
  - The SSH client public-keys for manager and operator access are copied from flash memory into the running configuration.
  - The RADIUS shared secret and TACACS+ encryption keys for access to authentication servers are already included in the running configuration.
  - SNMPv3 user credentials are already included in the running configuration.
- If you downgrade ProCurve software on a switch and use a software release earlier than K.12.06, security passwords are managed as follows:
  - Because SNMPv3 user credentials, RADIUS shared secret keys, and TACACS+ encryption keys are already included in the startup configuration, these security credentials are not lost. They continue to be used in the earlier software version.
  - The local manager and operator passwords are not recognized by an earlier software version and are not saved in the running configuration. However, passwords in inactive configuration files remain stored there. Although they are not displayed in **show config** command output, they are not automatically erased.
  - Although the hashed SSH client public-keys (for manager and operator access) are not recognized by an earlier software version, they remain stored so that they are immediately reloaded if you upgrade back to software release K.12.06 or greater.
  - As in a software upgrade, no port-access (operator) password for 802.1X authentication is saved from software release K.12.06 or greater.



## Restrictions

The following restrictions apply when you enable security credentials to be stored in the running configuration with the **include-credentials** command:

- The private keys of an SSH host cannot be stored in the running configuration. Only the public keys used to authenticate SSH clients can be stored. An SSH host's private key is only stored internally; for example, on the switch or on an SSH client device.
- SNMPv3 security credentials saved to a configuration file on a switch cannot be used after downloading the file on a different switch. The SNMPv3 security parameters in the file are only supported when loaded on the same switch for which they were configured.

The reason is that when SNMPv3 security credentials are saved to a configuration file, they are saved with the engine ID of the switch as shown here:

```
snmpv3 engine-id 00:00:00:0b:00:00:08:00:09:01:10:01
```

If you download a configuration file with saved SNMPv3 security credentials on a switch, when the switch loads the file with the current software version, the SNMPv3 engine ID value in the downloaded file must match the engine ID of the switch in order for the SNMPv3 users to be configured with the authentication and privacy passwords in the file. (To display the engine ID of a switch, enter the **show snmpv3 engine-id** command. To configure authentication and privacy passwords for SNMPv3 users, enter the **snmpv3 user** command.)

If the engine ID in the saved SNMPv3 security settings in a downloaded configuration file does not match the engine ID of the switch:

- The SNMPv3 users are configured, but without the authentication and privacy passwords. You must manually configure these passwords on the switch before the users can have SNMPv3 access with the privileges you want.
- Only the **snmpv3 user <user\_name>** credentials from the SNMPv3 settings in a downloaded configuration file are loaded on the switch; for example:

```
snmpv3 user boris  
snmpv3 user alan
```

- In software release K.12.06 and greater, you can store 802.1X authenticator (port-access) credentials in a configuration file. However, 802.1X supplicant credentials cannot be stored.
- In software release K.12.06 and greater, the local operator password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access**) is introduced to configure the username and password used as 802.1X authentication credentials for access to the switch. You can store the **password port-access** values in the running configuration by using the **include-credentials** command.

## Enhancements

### Release K.12.07 Enhancements

Note that the **password port-access** values are configured separately from local operator username and passwords that are configured with the **password operator** command and used for management access to the switch. For more information about how to use the **password port-access** command to configure operator passwords and usernames for 802.1X authentication, refer to the “Configuring Port-Based and Client-Based Access Control (802.1X)” chapter in the *Access Security Guide*.

## Release K.12.07 Enhancements

*No enhancements, software fixes only.*

## Release K.12.08 Enhancements

Release K.12.08 includes the following enhancement:

- **Enhancement (PR\_1000413764)** — Increase the size of the sysLocation and sysContact entries from 48 to 255 characters.

### Configuring a System Contact and Location for the Switch

Both the **system-contact** and the **system-location** fields allow up to 255 characters when configured through the CLI or the Web browser interface.

#### CLI Command

**Syntax:** snmp-server [contact <system-contact>] [location <system-location>]

where < system-contact > and <system-location > are ASCII strings up to 255 characters each.

#### Web Browser Interface

Using the Web browser interface for the switch, click the **Configuration** tab, and select **System Info** to access the **System Location** and **System Contact** fields. In each field, you can enter ASCII strings up to 255 characters each. You can view all the characters by using the cursor to scroll through the field.

#### Menu Interface

Unlike the CLI command and the Web browser interface, the Menu interface will only allow configuration of System Contact and System Location strings of up to 48 characters. However, if a System Contact or System Location string length configured through the CLI command or Web browser interface exceeds 48 characters, the Menu fields will display “+” followed by the last 47 characters of the string. Use the CLI **show running**, **show config**, or **show system-information** commands to see the complete text string.

## Release K.12.09 Enhancements

*No enhancements, software fixes only.*

## Release K.12.10 Enhancements

Release K.12.10 includes the following enhancement:

- **Enhancement (PR\_1000419653)** — The **show vlan ports** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged) for each port. See [“show vlan ports CLI Command Enhancement”](#) below.

### show vlan ports CLI Command Enhancement

The **show vlan ports** command has been enhanced with an option (**detail**) to display VLAN memberships on a per-port basis when a range of ports is specified in the command. In addition, user-specified port names will be displayed (if assigned), along with tagged or untagged membership modes.

### Displaying the VLAN Membership of One or More Ports

This command shows VLAN memberships associated with a port or a group of ports.

**Syntax** show vlan ports < port-list > [detail]

*Displays VLAN information for an individual port or a group of ports, either cumulatively or on a detailed per-port basis.*

**port-list:** *Specify a single port number, a range of ports (for example, a1-a16), or all.*

**detail:** *Displays detailed VLAN membership information on a per-port basis.*

*Descriptions of items displayed by the command are provided below.*

**Port name:** *The user-specified port name, if one has been assigned.*

**VLAN ID:** *The VLAN identification number, or VID.*

**Name:** *The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of **VLAN-x** where “x” matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of **GVRP\_x** where “x” matches the applicable VID.*

**Status:**

**Port-Based:** *Port-Based, static VLAN*

**Protocol:** *Protocol-Based, static VLAN*

**Dynamic:** *Port-Based, temporary VLAN learned through GVRP.*

**Voice:** Indicates whether a (port-based) VLAN is configured as a voice VLAN.

**Jumbo:** Indicates whether a VLAN is configured for Jumbo packets. For more on jumbos, refer to the chapter titled “Port Traffic Controls” in the Management and Configuration Guide for your switch.

**Mode:** Indicates whether a VLAN is tagged or untagged.

The following examples illustrate the displayed output depending on whether the **detail** option is used.

```
ProCurve# show vlan ports a1-a33

Status and Counters - VLAN Information - for ports A1-A33

VLAN ID  Name                | Status      Voice Jumbo
-----  -
1         DEFAULT_VLAN          | Port-based  No   No
10        VLAN_10               | Port-based  Yes  No
20        VLAN_20               | Protocol    No   No
33        GVRP_33              | Dynamic     No   No

ProCurve#
```

**Figure 7. Example of “Show VLAN Ports” Cumulative Listing**

```
ProCurve# show vlan ports a1-a4 detail

Status and Counters - VLAN Information - for ports A1

Port name: Voice_Port
VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1         DEFAULT_VLAN          | Port-based  No   No   Untagged
10        VLAN_10               | Port-based  Yes  No   Tagged

Status and Counters - VLAN Information - for ports A2

Port name: Uplink_Port
VLAN ID  Name                | Status      Voice Jumbo Mode
-----  -
1         DEFAULT_VLAN          | Port-based  No   No   Untagged
20        VLAN_20               | Protocol    No   No   Tagged
33        GVRP_33              | Dynamic     No   No   Tagged

Status and Counters - VLAN Information - for ports A3

VLAN ID  Name                | Status      Voice Jumbo Mode
```

**Figure 8. Example of “Show VLAN Ports” Detail Listing**

## Release K.12.11 Enhancements

*No enhancements, software never released.*

## Release K.12.12 Enhancements

*No enhancements, software fixes only.*

## Release K.12.13 Enhancements

*No enhancements, software never released.*

## Release K.12.14 Enhancements

*No enhancements, software fixes only.*

## Release K.12.15 Enhancements

Release K.12.15 includes the following enhancement:

- **Enhancement (PR\_1000427592)** — This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.

The IP address of the client is included in the RADIUS accounting packet sent by the switch to the RADIUS server. The client obtains the IP address through DHCP, so DHCP snooping must be enabled for the VLAN of which the client is a member.

- **Enhancement (PR\_1000428642)** — The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.

## Send SNMP v2c Informs

### Enabling and Configuring SNMP Informs

You can use the **snmp-server informs** command (SNMPv2c and SNMPv3 versions) to send notifications when certain events occur. When an SNMP Manager receives an informs request, it can send an SNMP response back to the sending agent. This lets the agent know that the informs request reached its destination and that traps can be sent successfully to that destination.

## Enhancements

### Send SNMP v2c Informs

Informs requests can be sent several times until a response is received from the SNMP manager or the configured retry limits are reached. The request may also timeout.

To enable SNMP informs, enter this command:

**Syntax:** [no] snmp-server enable informs

Enables or disables the informs option for SNMP.

Default: Disabled

To configure SNMP informs request options, use the following commands.

**Syntax:** [no] snmp-server informs [retries<retries>] [timeout<seconds>] [pending <pending>]

Allows you to configure options for SNMP informs requests.

**retries:** Maximum number of times to resend an informs request. Default: 3

**timeout:** Number of seconds to wait for an acknowledgement before resending the informs request. Default: 30 seconds

**pending:** *Maximum number of informs waiting for acknowledgement at any one time. When the maximum configured number is reached, older pending informs are discarded. Default: 25*

To specify the manager that receives the informs request, use the **snmp-server host** command.

**Syntax:** snmp-server host < ip-address >[<traps | informs>] [version <1 | 2c | 3>]< community-string >

Using community name and destination IP address, this command designates a destination network-management station for receiving SNMP event log messages from the switch. If you do not specify the event level, then the switch does not send event log messages as traps. You can specify up to 10 trap receivers (network management stations).

**Note:** *In all cases, the switch sends any threshold trap(s) or informs to the network management station(s) that explicitly set the threshold(s).*

[traps | informs>]

Select whether SNMP traps or informs are sent to this management station.

[version <1 | 2c | 3>]

Select the version of SNMP being used.

**Note:** SNMP informs are supported on version 2c or 3 only.

[<none | all | non-info | critical | debug>]

---

Options for sending switch Event Log messages to a trap receiver. The levels specified with these options apply only to Event Log messages, and not to threshold traps.

You can see if informs are enabled or disabled with the **show snmp-server** command as shown in Figure 9.

```
ProCurve(config)# show snmp-server
SNMP Communities
  Community Name   MIB View Write Access
  -----
  public           Manager  Unrestricted
Trap Receivers
  Link-Change Traps Enabled on Ports [All] : All
  Send Authentication Traps [No] : No
  [ Informs [Yes] : Yes ]
  Address          | Community      Events Sent in Trap
  -----
--
Excluded MIBs

Snmpp Response Pdu Source-IP Information
  Selection Policy : Default rfc1517
Trap Pdu Source-IP Information
  Selection Policy : Default rfc1517
```

**Figure 9. Example Showing SNMP Informs Option Enabled**

## Release K.12.16 Enhancements

*No enhancements, software fixes only.*

## Release K.12.17 Enhancements

*No enhancements, software fixes only.*

## Release K.12.18 Enhancements

Release K.12.18 includes the following enhancement:

- **Enhancement (PR\_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method.

## RADIUS Server Unavailable

### Overview

In certain situations, RADIUS servers can become isolated from the network. Users are not able to access the network resources configured with RADIUS access protection and are rejected. To address this situation, configuring the “**authorized**” secondary authentication method allows users unconditional access to the network when the primary authentication method fails because the RADIUS servers are unreachable.

### Configuring RADIUS Authentication

You can configure the switch for RADIUS authentication through the following access methods:

- **Console:** Either direct serial-port connection or modem connection.
- **Telnet:** Inbound Telnet must be enabled (the default).
- **SSH:** To use RADIUS for SSH access, first configure the switch for SSH operation.
- **Web:** Enables RADIUS authentication for web browser interface access to the switch.

You can configure **radius** as the primary password authentication method for the above access methods. You also need to select either **local**, **none**, or **authorized** as a secondary, or backup, method..

**Syntax:** `aaa authentication < console | telnet | ssh | web > < enable | login > radius`

*Configures RADIUS as the primary password authentication method for console, Telnet, SSH, and the web browser interface. (The default primary < enable | login > authentication is local.)*

`[< local | none | authorized >]`

*Provides options for secondary authentication (default: none).*

---

### Caution

Configuring **authorized** as the secondary authentication method used when there is a failure accessing the RADIUS servers allows clients to access the network unconditionally. Use this method with care.

---



You can configure **local**, **chap-radius** or **eap-radius** as the primary password authentication method for the port-access method. You also need to select **none** or **authorized** as a secondary, or backup, method.

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

*Configures **local**, **chap-radius**, or **eap-radius** as the primary password authentication method for port-access. The default primary authentication is **local**.*

[<none | authorized >]

*Provides options for secondary authentication. The **none** option specifies that a backup authentication method is not used. The **authorized** option allows access without authentication. (default: **none**).*

You can configure **chap-radius** as the primary password authentication method for web-based or mac-based port-access methods. You also need to select **none** or **authorized** as a secondary, or backup, method.

**Syntax:** aaa authentication <mac-based | web-based> chap-radius

*Configures **chap-radius** as the primary password authentication method for mac-based or web-based port access.*

[<none | authorized >]

*Provides options for secondary authentication. The **none** option specifies that a backup authentication method is not used. The **authorized** option allows access without authentication. (default: **none**).*

Figure 1 shows an example of the **show authentication** command displaying **authorized** as the secondary authentication method for port-access, Web-auth access, and Mac-auth access. Since the configuration of **authorized** means no authentication will be performed and the client has unconditional access to the network, the “Enable Primary” and “Enable Secondary” fields are not applicable (N/A).

**Enhancements**  
RADIUS Server Unavailable

```
ProCurve(config)# show authentication
```

Status and Counters - Authentication Information

Login Attempts : 3  
Respect Privilege : Disabled

Access Task	Login Primary	Login Secondary	Enable Primary	Enable Secondary
Console	Local	None	Local	None
Telnet	Local	None	Local	None
Port-Access	Local	Authorized	N/A	N/A
Webui	Local	None	Local	None
SSH	Local	None	Local	None
Web-Auth	ChapRadius	Authorized	N/A	N/A
MAC-Auth	ChapRadius	Authorized	N/A	N/A

The access methods with secondary authentication configured as **authorized** allows the client access to the network even if the RADIUS server is unreachable.

**Figure 10. Example of AAA Authentication Using Authorized for the Secondary Authentication Method**

## Specifying the MAC Address Format

The MAC address format command has been enhanced to allow upper-case letters to be used for the hexadecimal numbers when indicating the MAC address in RADIUS packets for MAC-based authentication.

**Syntax:** aaa port-access mac-based addr-format <no-delimiter | single-dash | multi-dash | multi-colon | no-delimiter-uppercase | single-dash-uppercase | multi-dash-uppercase | multi-colon-uppercase>

*Specifies the MAC address format to be used in the RADIUS request message. This format must match the format used to store the MAC addresses in the RADIUS server. (Default: no-delimiter)*

**no-delimiter** — *specifies an aabbccddeeff format.*

**single-dash** — *specifies an aabbcc-ddeeff format.*

**multi-dash** — *specifies an aa-bb-cc-dd-ee-ff format.*

**multi-colon** — *specifies an aa:bb:cc:dd:ee:ff format.*

**no-delimiter-uppercase** — *specifies an AABBCCDDEEFF format.*

**single-dash-uppercase** — *specifies an AABBCD-DDEEFF format*

**multi-dash-uppercase** — *specifies an AA-BB-CC-DD-EE-FF format*

**multi-colon-uppercase** — *specifies an AA:BB:CC:DD:EE:FF format.*

For example, using the multi-colon-uppercase option, the MAC address would appear as follows:

AA:BB:CC:DD:EE:FF

- **Enhancement (PR\_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 32 years).

## ARP Age Timer Increase

The ARP age is the amount of time the switch keeps a MAC address learned through ARP in the ARP cache. The switch resets the timer to zero each time the ARP entry is refreshed and removes the entry if the timer reaches the ARP age.

You can increase the ARP age timeout maximum to 24 hours or more with this command:

**Enhancements**  
ARP Age Timer Increase

**Syntax:** [no] ip arp-age <[1...1440] | infinite>

*Allows the ARP age to be set from 1 to 1440 minutes (24 hours). If the option “infinite” is configured, the internal ARP age timeout is set to 99,999,999 seconds (approximately 3.2 years). An arp-age value of 0 (zero) is stored in the configuration file to indicate that “infinite” has been configured. This value also displays with the show commands and in the menu display (Menu > Switch Configuration > IP Config).*

**Default:** 20 minutes.

```
ProCurve(config)# ip arp-age 1000
```

**Figure 11. Example of Setting the ARP Age Timeout to 1000 Minutes**

To view the value of Arp Age timer, enter the **show ip** command as shown in [Figure 12](#).

```
ProCurve(config)# show ip

Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 15.255.120.1
  Default TTL    : 64
  Arp Age       : 1000
  Domain Suffix :
  DNS server    :

VLAN          | IP Config | IP Address | Subnet Mask | Proxy ARP
-----+-----+-----+-----+-----
DEFAULT_VLAN | Manual    | 15.255.111.13 | 255.255.248.0 | No
```

**Figure 12. Example of show ip Command Displaying Arp Age**

You can also view the value of the Arp Age timer in the configuration file.

```
ProCurve(config)# show running-config

Running configuration:

; J9091A Configuration Editor; Created on release #K.12.XX

hostname "8200LP"
module 2 type J8702A
module 3 type J8702A
module 4 type J8702A
ip default-gateway 15.255.120.1
[ip_arp_age_1000_]
snmp-server community "public" Unrestricted
snmp-server host 16.180.1.240 "public"
vlan 1
    name "DEFAULT_VLAN"
    untagged B1-B24,C1-C24,D1-D24
    ip address 15.255.120.85 255.255.248.0
    exit
gvrp
spanning-tree
```

**Figure 13. Example Showing ip arp-age Value in the Running Config File**

You can set or display the **arp-age** value using the menu interface (**Menu > Switch Configuration > IP Config**).

```
ProCurve                                     12-June-2007  14:45:31
=====-- TELNET - MANAGER MODE =====
                Switch Configuration - Internet (IP) Service

IP Routing : Disabled

Default Gateway : 15.255.120.1
Default TTL    : 64
Arp Age       : 1000

IP Config [Manual] : Manual

IP Address    : 15.255.111.11
Subnet Mask   : 255.255.248.0

Actions->   Cancel      Edit      Save      Help
```

**Figure 14. Example of the Menu Interface Displaying the Arp Age Value**

If the ARP cache should become full because entries are not cleared (due to increased timeout limits) you can use the **clear arp** command to remove all non-permanent entries in the ARP cache.

To remove a specific entry in the ARP cache, enter this command:

**Syntax:** [no] arp IP-ADDRESS

*Allows removal of any dynamic entry in the ARP cache.*

- **Enhancement (PR\_1000438015)**— The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

The size of the login banner page increased from 320 to 3070 characters. The default banner displays product registration information; the copyright splash is no longer displayed.

If a banner is configured, the banner page is displayed when the user accesses the Web user interface. The default product registration information is not displayed as there is already a product registration prompt displayed in the Web user interface.

## Release K.12.19 Enhancements

*No enhancements, software fixes only.*

## Release K.12.20 Enhancements

*No enhancements, software fixes only.*

## Release K.12.21 Enhancements

Release K.12.21 includes the following enhancement:

- **Enhancement (PR\_1000440049)**— Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic.

## Classifier-Based Rate Limiting

Classifier-Based Rate Limiting (also known as Rate-Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic. When packets entering the port match a PERMIT statement in the ACL, they are rate-limited at the rate you have configured. If the packet matches a DENY statement, it is not rate-limited. There is an implicit DENY ALL at the end of the ACL, which means packets with no match are not rate-limited.

RL-PACLs use one meter per port and that meter is shared among all PERMIT statements for the RL-PACL on that port. The meter is not shared with other ports. For a 24-port interface module, 24 meters potentially can be used. (There are up to 256 meters available per module.)

Operating features include:

- Each port individually enforces the rate limit specified for that port.
- Only one rate-limiting ACL is allowed per port. Rate limits can be applied to a range of ports.
- Rate limits set on one port do not affect the traffic on any other port
- If you want to rate-limit some classes of traffic and drop others, the RL-PACL must be used in combination with another CLI-configured PACL; this feature does not provide that functionality.
- The rate-limiting configuration information is stored in the config file
- Rate-limiting ACLs cannot be configured on a port that is part of a trunk.

---

### Caution

All rate-limit values are in Kbps (1000 bits per second); some other rate-limiting features use Bps (bits per second). Be careful to enter the rates correctly.

## CLI Command for Rate Limiting

The **interface <port-list> rate-limit** command is enhanced to support the RL-PACL, as shown below:

**Syntax:** [no] interface <port-list> rate-limit ip access-group <name> in kbps <rate>

*Applies the access-group name specified to the ports selected in <port-list>. All packets that match a permit statement in access-group <name> are rate-limited and all packets that match a deny statement in access-group <name> are not rate-limited.*

**in Kbps <rate>:** *The range is 1-10,000,000 kilobits per second.*

```
ProCurve(config)# interface 4-8 rate-limit ip access-group Group_A in kbps 10000
```

**Figure 1. Example of Rate-Limiting RL-PACL on a Range of Ports**

In the example in [Figure 1](#) the ACL named Group\_A is applied to port 4 through 8 with a limit of 10000 kbps (10 Mbps). When the packets enter the configured ports, all packets that match a PERMIT statement in Group\_A are rate-limited and all packets that match a DENY statement in Group\_A are not rate-limited. The ACL does not have to be defined before being applied as an RL-PACL.

---

## Note

RL-PACLs and other ACL types (normal PACLs, VACLs, RACLs, etc.) operate on packets at the same time. If any ACL indicates the packet should be dropped, the packet is dropped. However, the packet will still count towards RL-PACL meter usage.

To turn off the rate limiting enter this command:

```
ProCurve(config)# no interface 4-8 rate-limit ip access-group
```

**Figure 2. Turning off Rate-Limiting for the Configured Ports**

## Viewing the RL-PACL Information

An enhanced rate-limit CLI command displays information about the rate-limiting configured on each port for each group.

**Syntax:** show rate-limit ip access-group <[ethernet] port-list>

```
ProCurve(config)# show rate-limit ip access-group
```

```
Inbound access-group rate-limits:
```

Port	kbps	Access-group name
----	-----	-----
4	10000	Group_A
5	10000	Group_A
6	10000	Group_A
7	10000	Group_A
8	10000	Group_A

Ports with no RL-PACL applied are not displayed in the output.

**Figure 3. Example of show rate-limit Command for RL-PACLs**

## Show Access Lists by Port

Figure 4 shows the ACL information for a specific port.



```
ProCurve(config)# show access-list ports 4-6

Access Lists for Port 4

  RateLimit : Group_A
  Type      : None

Access Lists for Port 5

  RateLimit : Group_A
  Type      : None

Access Lists for Port 6

  RateLimit : Group_A
  Type      : None
```

**Figure 4. Access-List Information for Selected Ports**

## Displaying the Resources Used

To display the resources used, including ACL resources, enter this command:

```
ProCurve(config)# show qos resources
```

**Enhancements**  
Viewing the RL-PACL Information

```
ProCurve(config)# show qos resources

Resource usage in Policy Enforcement Engine
```

Ports	Rules		Rules Used				
	Available	ACL	QoS	IDM	VT	ICMP	Other
1-24	3019	5	20	0	0	0	0
25-48	3044	0	0	0	0	0	0
A	3044	0	0	0	0	0	0

Ports	Application		Application		
	Port Ranges Available*	ACL	IDM	QoS	Other
1-24	14	0	0	0	0
25-48	14	0	0	0	0
A	14	0	0	0	0

\* If insufficient port ranges are available, additional rules will be used.

Ports	Meters		Meters Used			
	Available	ACL	QoS	IDM	ICMP	Other
1-24	230	0	5	0	0	0
25-48	255	0	0	0	0	0
A	255	0	0	0	0	0

1 of 8 Policy Engine management resources used.

Key:  
 ACL = Access Control Lists; QoS = Host or application port QoS policies;  
 IDM = Identity Driven Management; VT = Virus Throttling;  
 ICMP = network ICMP rate limiting;  
 Other = Management VLAN, Remote Intelligent Mirror endpoints, DHCP Snooping, ARP Protection.

Resource usage includes resources actually in use, or reserved for future use by the listed feature. Internal dedicated-purpose resources, such as port bandwidth limits or VLAN QoS policies, are not included.

In this exmple, five RL-PACLs are configured on ports 1-24.

Policy Engine management resources exclude resources reserved for RL-PACLs.

**Figure 5. Example of show qos resources Command**

# Troubleshooting

The following situations may occur when using RL-PACLs.

Problem	Resolution
You try to apply an RL-PACL to a port, but are informed that there are insufficient resources.	Hardware resources have been consumed by some combination of RL-PACLs, other ACLs, other QoS or rate-limiting features or other features on the switch. Enter the commands <b>show access-list resources</b> or <b>show qos resources</b> to see what features are using resources.
The switch is unexpectedly dropping traffic entering a port and you suspect the RL-PACL is the issue.	The command <b>show access-list ports &lt;port-list&gt;</b> shows which ACLs are applied to a port, including regular ACLs and RL-PACLs. If these are not causing the problem, enter the command <b>show access-list vlan &lt;vlan-id&gt;</b> to check VLANs. Additionally, check the configured rate-limit using the <b>show rate-limit</b> command.
The switch is not rate-limiting traffic even though an RL-PACL is configured.	Verify that the RL-PACL is configured correctly by entering the <b>show rate-limit ip access-group &lt;portnum&gt;</b> command. Check that the ACL name and rate (in kbps) are correctly configured for the port.  Traffic is only dropped when the rate limit for packets matching permit statements is exceeded. For example, if an RL-PACL is configured with a rate-limit of 100 kbps and 100 kbps of traffic matches permit statements and 100 kbps of traffic matches deny statements, all 200 kbps of traffic is allowed to pass through the port.

- **Enhancement (PR\_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Enhancement (PR\_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections.

## Concurrent TACACS+ and SFTP”

It is now possible to have SFTP/SCP sessions run concurrently with TACACS+ authentication. Because the initial login must be with a username/password that has manager level privileges, you must configure TACACS+ single sign-on in order for TACACS+ and SFTP/SCP to coexist.

To configure TACACS+ single sign-on, user the **aaa authentication login privilege-mode** command.

**Syntax:** aaa authentication

<login [privilege-mode] >

*Selects the Operator access level. If the **privilege-mode** option is entered, TACACS+ is enabled for a single login. The authorized privilege level (Operator or Manager) is granted by the TACACS+ server.*

*Default: Single login disabled.*

## Release K.12.22 Enhancements

Release K.12.22 includes the following enhancement:

- **Enhancement (PR\_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR\_1000444415)** — OSPF Passive Interface support was added.

## “OSPF Passive and Routing Interface Increase”

OSPF sends link-state advertisements (LSAs) to all other routers in the same Autonomous System (AS). To limit the flooding of LSAs throughout the AS you can configure OSPF to be passive. OSPF does not run in the AS, but it does advertise the interface as a stub link into OSPF. Routing updates are accepted by a passive interface, but not sent out.

There is a limit of 512 total active and passive interfaces, but only a total of 128 can be active interfaces.

To configure a passive OSPF interface, enter this command in vlan context:

```
ProCurve(vlan-1)# ip ospf passive
```

**Syntax:** [no] ip ospf <ip-addr> passive

*Configures passive OSPF for an Autonomous System.*

*The no option disables the passive option; the interface becomes an active interface.*

**Default:** Active

**<ip-addr>:** *Optionally you can configure an IP address on the VLAN*

To display the OSPF information, enter the command shown in [Figure 6](#):

```
ProCurve(vlan-1)# show ip ospf interface

OSPF Interface Status

IP Address   Status   Area ID   State   Auth-type   Cost   Priority   Passive
-----
10.10.10.1   enabled 0.0.0.2   down    none        1      1          Yes
10.12.13.1   enabled 0.0.0.2   wait    none        1      1          No
```

**Figure 6. Example of the show ip ospf interface Command with Passive Configured on an Interface**

You can display the OSPF information for a particular VLAN, as shown in [Figure 7](#).

```
ProCurve(config) show ip ospf interface vlan 4

OSPF configuration and statistics for VLAN 4

OSPF Interface Status for 10.10.10.1

IP Address:      : 10.10.10.1   Status : enabled
AreaID          : 0.0.0.2     Passive : Yes

State   : DOWN                Auth-type : none
Cost    : 1                   Chain     :
Type    : BCAST               Priority  : 1

Transit Delay   : 1           Retrans Interval : 5
Hello Interval  : 10          Rtr Dead Interval : 40
Designated Router:           Events             : 0
Backup Desig. Rtr:           Passive             : yes
```

**Figure 7. Example of the show ip ospf interface Command for a specific VLAN with Passive Configured on an Interface**

## Release K.12.23 Enhancements

Release K.12.23 includes the following enhancement:

- **Enhancement (PR\_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP.

### Web Auth Secure Protocol

It is desirable to have an additional method for Web authentication that allows the storage of passwords in a secure manner rather than as plain text. The MS-CHAPv2 authentication method allows password verification without requiring access to a plain text password. This method also will be provided for MAC authentication.

The **aaa authentication** command is modified to provide the **web-based** and **mac-based** options. After selecting one of these options, you can choose the authentication method, either **chapradius** (the default) or the more secure **peap-mschapv2** authentication method.

**Syntax:** aaa authentication <console | login | num-attempts | port-access | ssh | telnet | web | web-based | mac-based>

**web-based or mac-based<chapradius | peap-mschapv2>:** *After selecting either web-based or mac-based options, you can choose the authentication method.*

**Default:** *chapradius*

```
ProCurve(config)# aaa authentication web-based peap-mschapv2
```

**Figure 15. Example Command with peap-mschapv2 Option Selected**

The show authentication command will display which authentication method has been configured.

```
ProCurve(config)# show authentication

Status and Counters - Authentication Information

Login Attempts : 3
Respect Privilege : Disabled

Access Task | Login          Login          Enable          Enable
            | Primary        Secondary      Primary         Secondary
-----+-----+-----+-----+-----
Console     | Local          None           Local           None
Telnet      | Local          None           Local           None
Port-Access | Local          None           Local           None
Webui       | Local          None           Local           None
SSH         | Local          None           Local           None
Web-Auth    | PEAP-MSCHAPv2
MAC-Auth    | ChapRadius
```

**Figure 16. Example of show authentication Command with Web-Auth Configured for PEAP-MSCHAPv2 Authentication**

## Release K.12.24 Enhancements

*No enhancements, software fixes only.*

## Release K.12.25 Enhancements

*No enhancements, software fixes only.*

## Software Fixes in Release K.11.12 - K.12.25

---

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

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

Release K.11.11 was the first production software release for the ProCurve 3500yl, 6200yl, and 5400zl Series switches. Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.00 code branch with no intervening releases.

---

### Release K.11.12

The following problems were resolved in release K.11.12 (never released)

- **ACL/QoS (PR\_1000317233)** — Under some circumstances, the Switch may apply an ACL or QoS configuration setting incorrectly.
- **Configuration/Security (PR\_1000316441)** — Operator level can save Manager privilege level changes to the configuration.
- **Crash Log (PR\_1000309533)** — Incorrect crash message displayed in the log, "Too many HSL interrupts".
- **Crash (PR\_1000317489)** — Changing the QoS/ACL portion of the running configuration may cause a switch module to crash with a message similar to:  

```
CL Int status=0x10000000
```
- **Gig-T SFP Modules (PR\_1000316433)** — The switch accepts a Gig-T SFP dual personality module when it should not accept these modules.w
- **Help file enhancement (PR\_1000300491)** — Added support for Help files. Switch can provide a navigation pane on the left side of the screen containing 'Contents' and 'Search' capability.
- **10 Gig Transceiver (PR\_1000317965)** — Switch reports incorrect Link status when a defective fiber cable is connected to the Switch.
- **LED (PR\_1000316434)** — If a mini-GBIC is installed during switch bootup, that port's link LED will not turn on.
- **MSTP Enhancement (PR\_1000310463)** — Implementation of legacy path cost MIB and CLI option for MSTP.
- **RSTP (PR\_1000307278)** — Replacing an 802.1D bridge device with an end node (non-STP device) on the same Switch port, can result in the RSTP Switch sending TCNs.



- **Web UI (PR\_1000303371)** — In the Web User Interface, the QOS Device Priority window scroll bar does not allow sufficient scrolling to view all entries.
- **Web UI (PR\_1000311917)** — When the last port on the last card is configured in a trunk or mesh, and a user browses to a specific location in the Web user interface, the HTTP web server degrades the switch, causing the Web user interface to hang.

## Release K.11.13

The following problems were resolved in release K.11.13 (never released)

- **Routing (PR\_1000306239)** — In some cases, the command '**show ip route**' may display incorrect information.
- **Self-test (PR\_1000315509)** — The self-test LED does not turn off after bootup of an empty chassis.
- **sFlow (PR\_1000317785)** — Using Inmon Traffic Server, traffic will be reported on ports with no traffic present. Other ports may or may not have faulty counter reports.

## Release K.11.14

The following problems were resolved in release K.11.14 (never released)

- **SNMP (PR\_1000315054)** — SNMP security violations are entering the switch syslog when a valid SNMPv3 'get' operation is initiated.
- **Web (PR\_1000302713)** — When using the web interface and a large amount of stacking interactions occur, portions of the information from the stack commander may no longer appear.

## Release K.11.15

The following problems were resolved in release K.11.15 (never released)

- **CLI (PR\_1000298299)** — After a reboot, the Switch does not provide warning that the running configuration and startup configuration differ, and does not offer an option to save the running configuration.
- **CLI (PR\_1000315256)** — Inconsistent error message, "Resource unavailable," when configuring more than the maximum number of allowed static IP routes.
- **Crash (PR\_1000322009)**— The Switch may crash with a message similar to:  
Software exception in ISR at queues.c:123.

- **Menu (PR\_1000318531)** — When using the Menu interface, the Switch hostname may be displayed incorrectly.

## Release K.11.16

The following problems were resolved in release K.11.16 (not a general release)

- **10 GbE module (PR\_1000321201)** — At a high temperature and with long cables, the Switch 3500y1 X2/CX4 10-GbE module (J8694A) may not work properly.

## Release K.11.17

The following problems were resolved in release K.11.17

- **Stacking (PR\_1000298299)** - The Stack Commander setting is not written to the configuration file, so Web/Stacking does not work.

## Release K.11.32

The following problems were resolved in release K.11.32

- **Authentication (PR\_1000334731)** — PEAP/TLS EAP types with IAS Radius Server fail to authenticate.
- **CLI (PR\_1000298038)** — The command "**show arp**" displays incomplete information.
- **CLI (PR\_1000308346)** — The command "**show tech**" failed to execute.
- **CLI (PR\_1000308601)** — The Stack Close Up device view does not display all stack members.
- **CLI (PR\_1000329325)** — Unrecognizable characters printed to console on User Authentication timeout when logging in via TACAS server.
- **CLI (PR\_1000329977)** — User is unable to edit any SNMPv3 target address entries.
- **Config (PR\_1000326255)** — The stacking interval setting does not appear in the startup or running configuration files.
- **Crash (PR\_1000228633)** — The Switch may crash with a message similar to:  

```
Software exception at ldbal_cost.c:1577 -- in 'eDrvPoll', task ID = 0x1760650-> ASSERT: failed.
```
- **Crash (PR\_1000314305)** — The switch may crash with a message similar to:  

```
Software exception at ipamMApi.c:1592/1594 -- in 'eRouteCtrl'
```

- **Crash (PR\_1000323759)** — The Switch may crash with a message similar to:  
TLB Miss: Virtual Addr=0x00000185 IP=0x8027ae04 Task='mLACPCtrl'  
Task ID=0x81597410 fp:0x00000000 sp:0x815972d0 ra:0x8027aa90  
sr:0x1000fc01.
- **Crash (PR\_1000324041)** — A module may crash due to ACL Parity Interrupt with a message similar to  
'ACL Int stats=0x1000000 28=0x80000b2'.
- **Crash (PR\_1000325030)** — The Switch may crash with a message similar to:  
'Software exception at vls\_dyn\_reconfig.c:1939 -- in 'mLpmgrCtrl', task  
ID = 0xa139a80'.
- **Crash (PR\_1000325540)** — The Switch may crash with a message similar to:  
Software exception at sw\_sem.c:712 -- in 'mSnmpCtrl'.
- **Crash (PR\_1000327132)** — The Switch may crash with a message similar to:  
Software exception in ISR at btmDmaApi.c:304.
- **Crash (PR\_1000329818)** — The Switch may crash with a message similar to:  
assert in btmDmaApi.c:289 - out of msgs, need to throttle rmon & syslog  
msgs.
- **Crash (PR\_1000330009)** — The Switch may crash with a message similar to:  
slave assert at btftSlaveLearn.c:1426 - extended bcast loop condition.
- **Crash (PR\_1000332703)** — The Switch may crash with a message similar to:  
slave assert at ngDmaRx.c:495 - ease sample outbound received a fragment.
- **Crash (PR\_1000329485)** — Broadcast loop creates additional packets causing throughput  
traffic to decrease.
- **Crash/ACL (PR\_1000332850)** — When authenticating using Radius ACLS, configuring and  
un-configuring multiple ACLs may cause the Switch to crash.
- **Crash (PR\_1000334992)** — The Switch may crash with a message similar to:  
"Software exception in ISR at btmDmaApi.c:289 -> No resources avail-  
able".
- **Crash (PR\_1000335430)** — The Switch may crash with a message similar to:  
"Cam range reservation error" crash at aqSlaveRanges.c:172.
- **Event Log (PR\_1000308669)** — After a Switch reset, the event log does not display correct  
information.

- **Event Log (PR\_1000310958)** — Unsupported modules do not produce an event log message in the Switch.
- **Fault LED (PR\_1000314005)** — Upon a fan fault, the fault LED does not indicate an error.
- **Flash Memory (PR\_1000320941)** — An incorrect error message is displayed when the Switch experiences a Flash memory failure.
- **Flow Control (PR\_1000333879)** — Flow Control not functioning properly.
- **Help Menu (PR\_1000307772)** — The Help menu text for command "router pim rp-candidate hold-time" displayed incorrect values.
- **Help Menu (PR\_1000326670)** — Web User Interface Help file link URLs exceed maximum length.
- **ICMP (PR\_1000315805)** — When the Switch receives a UDP packet on a closed port, Switch fails to send an ICMP response message back to the sender.
- **ICMP/Rate Limiting (PR\_1000319946)** — Configuring ICMP Rate Limiting on interfaces causes the Switch to create duplicate requests, which affects the total throughput of the blade.
- **LED (PR\_1000325259)** — Test LED flashing wrong color when a defective Mini-GBIC is installed.
- **LLDP (PR\_1000319356)** — LLDP does not discover CDPv2 devices.
- **MAC Authentication (PR\_1000329738)** — Switch may improperly flush the ARP cache when adding or removing an authorized MAC address.
- **MAC Authentication (PR\_1000335314)** — While authenticating multiple ports via MAC authentication, the Switch successfully authenticates the port but fails to learn the source MAC address.
- **Meshing (PR\_1000325260)** — With meshing enabled, it is possible that packet buffers may get corrupted resulting in a Switch reboot.
- **Module (PR\_1000307404)** — With no cable attached, the X2 CX4 transceiver link LED remains on after a switch power up or hot swap of module.
- **Modules (PR\_1000314454)** — Blades fail to reboot (retry) after failing a selftest.
- **Module (PR\_1000330312)** — Booting up the Switch with an unsupported module installed may cause all existing modules to fail.
- **MSTP Enhancement (PR\_1000331792)** — Implementation of Spanning-tree BPDU Filter and SNMP Traps.

- **Power Supply (PR\_1000310159)** — After power supply failovers, the Switch incorrectly reports power being available on ports that are actually powered down.
- **QoS/Rate Limiting (PR\_1000319946)** — QoS/Rate limiting may stop working or impact unwanted traffic streams.
- **QOS (PR\_1000325028)** — Switch may crash after configuring QOS device-priority.
- **SNMPv3 (PR\_1000325021)** — SNMPv3 lines may mistakenly be removed from the configuration file.
- **STP (PR\_1000333992)** — In a redundant STP network with PIM running, PIM packets may get assigned a higher queue priority than STP packets, which may cause network loops.
- **Switch (PR\_1000327506)** — Fixed issue where Switch incorrectly allowed jumbos frames to be configured for 10/100 ports.
- **VLAN (PR\_1000334107)** — User is unable to add a port to a VLAN and the Switch responds with an invalid error message.
- **Web UI (PR\_1000308213)** — Removed Web Stacking Tab within the Web User Interface for the 5400zl products.
- **Web UI (PR\_1000308225)** — When using the Web User Interface, the device view of the Stack Close-up is missing.
- **Web UI (PR\_1000311087)** — Serial number for 5400zl products within the Web-UI exceeds the provided rectangle.
- **Web UI (PR\_1000322777)** — When using the Web User Interface in the Configuration Tab, a user is unable to modify a port name.
- **Web UI (PR\_1000329279)** — When using the web user interface Commander's Stack Close Up view, some stack members are not displayed.

## Release K.11.33

The following problems were resolved in release K.11.33

- **Buffer Leak (PR\_1000336963)** — The Switch may run out of packet buffers under certain conditions.
- **Crash/ACL (PR\_1000337717)** — The Switch may crash with a message similar to:  

```
"Software exception at alloc_free.c:422 -- in 'eDrvPoll'...-> No msg buffer", when Switch is configured for ACL logging.
```
- **Module J8705A (PR\_1000336281)** — The Switch 5400zl 20P 10/100/1000 + 4 mini GBIC module (J8705A) may stop forwarding packets.

## Release K.11.34

The following problems were resolved in release K.11.34 (not a general release)

- **CLI (PR\_1000323423)** — Entering an incorrect password three times for either the operator or manager levels causes the CLI to display erroneous characters.
- **CLI (PR\_1000322029)** — The command "**show vlans**" does not display data correctly in the status field.
- **IDM (PR\_1000334365)** — Using EAP/802.1x with IDM ACLs can result in memory leaks.
- **Management (PR\_1000337447)** — The switch is unmanageable using Telnet or SNMP.
- **OSPF (PR\_1000339542)** — When using the "**show IP route**" or "**show ip route ospf**" commands after configuring an AS External LSA (type 5) with a configured metric, the "show" commands display an incorrect metric value.
- **Web UI (PR\_1000331431)** — The QoS Configuration Tab does not work correctly when using the Web User Interface.

## Release K.11.35

The following problems were resolved in release K.11.35 (never released)

- **Authentication (PR\_1000343377)** — When running the Windows XP 802.1x supplicant and the switch sends a re-authentication, Windows XP prompts the user to re-enter their username and password again.
- **Authentication (PR\_1000344961)** — A port with multiple 802.1x users on it will allow traffic to pass for a user after that user's supplicant has been stopped.
- **DHCP (PR\_1000323679)** — Client cannot obtain an IP address when two DHCP servers are connected on different local networks.
- **Enhancement (PR\_1000336169)** — Added support for STP Per-Port BPDU Filtering and SNMP Traps.
- **Enhancement (PR\_1000311957)** — Added an option to configure the switch to use the management VLAN IP address in the Option 82 field for all DHCP requests received from various VLANs.
- **MIB (PR\_1000307831)** — The MIB value for **ipAddrTable** is not populated.
- **RIP (PR\_1000331536)** — RIP does not send a route poison update in response to a failed route.

- **Show tech (PR\_1000294072)** — Show Tech statistics displays incorrect port names for fixed ports.

## Release K.11.36

The following problems were resolved in release K.11.36 (never released)

- **10-GbE (PR\_1000346107)** — The guaranteed minimum bandwidth feature is not working on 10-GbE ports.

## Release K.11.37

The following problems were resolved in release K.11.37 (not a general release)

- **Login (PR\_1000347300)** — Login failures do not result in an "Invalid Password" response.

## Release K.11.38

The following problems were resolved in release K.11.38 (never released)

- **10-GbE (PR\_1000346107)** — The Guaranteed minimum bandwidth feature does not work on 10-GbE ports.
- **CLI (PR\_1000305349)** — The command, **no ip router-id**, does not work. Once a router-ID is set, there is no way to remove it.
- **QoS (PR\_1000346708)** — IP-Precedence does not set the correct priority if all TOS bits are set to 1.

## Release K.11.39

The following problems were resolved in release K.11.39 (never released)

- **Crash (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\_1000351693)** — The switch may crash with a message similar to  
Software Exception at rt\_table.c.758 -- in 'eRouteCtrl', task ID =  
0x8a d6b30 -> Routing Task: Route Destinations exceeded

## Release K.11.40

The following problems were resolved in release K.11.40 (not a general release)

- **CLI (PR\_1000353548)** — Use of the command **show span** incorrectly displays an error, "STP version was changed. To activate the change you must save the configuration to flash and reboot the device."
- **Crash (PR\_1000352922)** — The switch may crash with a message similar to  

```
mstp_ptx_sm.c:118 -- in 'mMstpCtrl', task ID = 0x8899e70 -> ASSERT:  
failed
```
- **Enhancement (PR\_1000346164)** — RSTP/MSTP BPDU Protection: When this feature is enabled on a port, the switch will disable (drop the link) a port that receives a spanning tree BPDU, log a message, and optionally, send an SNMP TRAP.

## Release K.11.41

The following problems were resolved in release K.11.41

- **Enhancement (PR\_1000344652)** — Added support for Unidirectional Fiber Break Detection.
- **Hang (PR\_1000346328)** — Switch hangs during initialization, switch may fail to boot. RMON alarms/events configuration files corrupted.
- **MDI/MDI-X (PR\_1000354050)** — Forced MDI and MDIX modes were reversed on the 3500yl - forced MDI was transmitting out pins 3 and 6 instead of 1 and 2, and vice versa.
- **Port Monitoring (PR\_1000354067)** — The CLI does not allow users to mirror mesh ports, resulting in "Error setting value monitor for port <n>".
- **SSH (PR\_1000350999)** — The SSH login prompts user to "press any key to continue" twice before providing a prompt.
- **Web-UI (PR\_1000354104)** — The web-UI limited the size of the "Common Name" field in the SSL configuration tab to 16 characters

## Release K.11.43

Version K.11.42 was never released.

The following problems were resolved in release K.11.43 (not a general release)



- **Crash (PR\_1000307842)** — When deleting/removing CLI ACLs, IDM ACLs, management VLAN, or virus throttle lockouts, switch crashes with error similar to:

“Delete virtual meter with nonzero rule RefCount” .

- **Crash (PR\_1000334982)** — When web authentication is used with open VLANs, a software exception may occur, with the switch reporting something similar to this.

```
Software exception at wma_vlan_sm.c:289 -- in 'mWebAuth',  
task ID = 0x81e408e0 -> ASSERT: failed
```

- **Enhancement (PR\_1000358903)** — 802.1X Controlled Directions enhancement. With this change, Administrators can use “Wake-on-LAN” with computers that are connected to ports configured for 802.1X authentication.
- **VRRP (PR\_1000356388)** — VRRP returns the physical MAC address instead of the virtual MAC address when replying with proxy-ARP.

## Release K.11.44

The following problems were resolved in release K.11.44 (not a general release)

- **Enhancement (PR\_1000361504)** — This enhancement allows STP to detect and block network topology loops on a single port.

## Release K.11.46

Version K.11.45 was never released.

The following problems were resolved in release K.11.46 (not a general release)

- **CLI (PR\_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **CLI (PR\_1000305584)** — The output from the "show power" commands on the ProCurve 3500yl switches references slot letters when it should display port numbers.
- **Crash (PR\_1000357083)** — The switch management may run out of packet buffers and crash with a message similar to:

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

- **Hang (PR\_1000359640)** — The switch may hang on initialization and become unresponsive.

## Release K.11.47

The following problems were resolved in release K.11.47 (not a general release)

- **Management VLAN (PR\_1000299387)** — The management VLAN does not allow connectivity from valid addresses.
- **SNMP (PR\_1000358129)** — The command line interface (CLI) becomes unresponsive after running RMON traps code.

## Release K.11.48

The following problems were resolved in release K.11.48 (not a general release)

- **CLI (PR\_1000345301)** — The output from the "show config state" CLI command doesn't always report changes made to the configuration.
- **Crash (PR\_1000334710)** — When saving changes to the IGMP configuration, the switch may crash with a message similar to this.  

```
TLB Miss: Virtual Addr=0x00000000 IP=0x80591238 Task='mSess1'
```
- **Crash (PR\_1000351243)** — The switch may crash at boot-up if more than 1000 VLANs are configured.
- **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.
- **OSPF (PR\_1000363648)** — The "restrict" CLI command in OSPF redistribution does not filter the default route.

## Release K.11.49

The following problems were resolved in release K.11.49 (not a general release)

- **802.1X (PR\_1000358534)** — For the Controlled Directions feature of 802.1X to operate correctly, spanning tree must be enabled and authenticator ports must be set as edge ports. This fix removes a limitation that requires these steps be done in a specific order.
- **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'
```
- **Enhancement (PR\_1000366744)** — DHCP Protection enhancement. For more information about this feature, please watch the ProCurve web site.

- **sFlow (PR\_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.

## Release K.11.61

Versions K.11.50 through K.11.59 were never built.

Version K.11.60 was never released.

The following problems were resolved in release K.11.61 (not a general release)

- **802.1X (PR\_1000367404)** — Increased the maximum number of 802.1X users per port to 32.
- **Crash (PR\_1000366583)** — When a large config is saved using the "write memory" CLI command, the switch may crash with a message similar to:

```
NMI event SW:IP=0x00897870 MSR:0x00029210 LR:0x00100c80 Task=' mSess1'  
Task ID=0x8d13fe0.
```

## Release K.11.62

The following problems were resolved in release K.11.62 (not a general release)

- **ACL (PR\_1000368901)** — Outbound access control lists (ACLs) do not function after a reboot.
- **Authorization (PR\_1000365285)** — IP Authorized Managers feature 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.
- **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
```

- **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.
- **sFlow (PR\_1000361604)** — Changed the maximum sFlow skipcount to 24 bits.
- **VLAN (PR\_1000356062)** — When configuring from the menu interface, the 3500y1 series switches will not allow the following name format for a new VLAN:

"VLANx" (where "x" is a VLAN number).

## Release K.11.63

The following problems were resolved in release K.11.63

- **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".
- **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.
```
- **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.
- **PCM Traffic Monitoring/Performance Degradation (PR\_1000370061)** — The switch is affected by PCM traffic monitoring, causing throughput degradation.
- **RADIUS (PR\_1000358525)** — Attributes that were overridden by RADIUS (CoS, Rate, and ACL) remain active if an authenticated user fails to send EAP-LOGOFF.

## Release K.11.64

The following problems were resolved in release K.11.64 (not a general release)

- **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.
```
- **Enhancement (PR\_1000376406)** — Loop Protection feature additions, including packet authentication, loop detected trap, and receiver port configuration.
- **Event Log (PR\_1000373796)** — Selecting "Save", within the IP Configuration screen of the Menu causes unnecessary Event Log messages.
- **sFlow/Flow-Control (PR\_1000375851)** — To protect performance if Flow-Control is enabled on any one or more ports, egress sFlow sampling will be disabled on all ports and a CLI/Event Log message will be generated.
- **VLAN/CLI (PR\_1000368900)** — VLAN names over 12 characters in length cause the output from the command "show ip route" to be displayed incorrectly.

## Version K.11.65

The following problems were resolved in release K.11.65 (not a general release)

- **Alarms/Log (PR\_1000371908)** — The ambient temperature measured by the 5406zl chassis is 4 degrees C too high, causing the generation of false high temperature alarms.
- **CLI (PR\_1000377318)** — The output from the CLI command, 'show dhcp-relay' is truncated.
- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the "show tech" command output.
- **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."
- **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 the MIB.
- **VRRP (PR\_1000380627)** — VRRP packets are received on a non-VRRP VLAN causing excessive event log/syslog messages.

## Version K.11.66

The following problems were resolved in release K.11.66 (not a general release)

- **CLI (PR\_1000379455)** — The output from some CLI "show" commands produces incorrectly formatted output on the screen.
- **CLI (PR\_1000309983)** — Using the "show tech" command immediately after boot and before the modules have initialized causes the command to fail, and leaves the user in an unsupported CLI state.
- **CLI (PR\_1000364628)** — The command output from "show ip rip peer" yields an improperly formatted peer IP address.
- **Meshing (PR\_1000386393)** — A 5412zl switch may crash with a bus error, when 4 Port CX4 module (J8708A) in Slot L is configured for Meshing. The crash message is similar to the following.  

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x08af5298 HW Addr=0x4b5a697c IP=0x00372ed8  
Task='mLdBalCtrl' Task 0 fp: 0x00000018
```
- **sFlow (PR\_1000378885)** — The sFlow samplePool for trunks is sometimes unchanged between samples. This may cause inaccurate spikes in traffic monitoring applications that measure the utilization on trunk ports.

**Software Fixes in Release K.11.12 - K.12.25**  
Version K.11.67

- **Web/RADIUS (PR\_1000368520)** — Web Authentication doesn't authenticate clients due to a failure to send RADIUS requests to the configured server.
- **WebUI (PR\_1000371598)** — Unable to Access Stack Members through Commander WebUI. Use of the WebUI "stack access" drop-down list on the stacking commander returns a "Page not found" error.

## Version K.11.67

The following problems were resolved in release K.11.67 (not a general release)

- **MSTP (PR\_1000385573)** — MSTP instability when root switch priority is changed. This causes other switches with better priority to assert themselves as root, thus causing a root war to occur.

## Version K.11.68

Software never released.

- **CLI/LLDP (PR\_1000377191)** — Output from the CLI command, "show lldp info remote-device <port>" shows a blank field for the chassis ID.
- **Crash (PR\_1000390591)** — Software exception at sflow.c:3903 after re-starting sflow sampling. Switch may crash with a message similar to:  

```
Software exception at sflow.c:3903 -- in 'mSnmpEvt',  
task ID = 0x8248e90-> ASSERT: failed
```
- **DHCP (PR\_1000386886)** — DHCP-relay uses an inconsistent address when the VLAN is multinetted. This fix forces the lowest IP address to be used for DHCP.
- **Enhancement (PR\_1000388709)** — SFlow does not accommodate bursty traffic.
- **ROM update (PR\_1000390486)** — ROM update to version K.11.03, required to support the upcoming K.12 software update.
- **Trunking (PR\_1000238829)** — Trunks numbered trk10 and greater cause the output from the CLI command "show span" output to be misaligned.

## Version K.11.69

The following problems were resolved in release K.11.69

- **Routing (PR\_1000392086)** — The switch learns a bogus MAC address when the next hop address is unknown, causing the switch to stop forwarding traffic.

Release K.11.69 is the last release of the K.11.*xx* software. The 3500yl, 6200yl, and 5400zl switch series software code was rolled to the K.12.0*x* code branch with no intervening releases.

## Version K.12.01

The following problems were resolved in release K.12.01

- **ACL (PR\_1000393287)** — When the same ACL is applied (in or out) to more than 2 VLANs it does not get applied to the third VLAN or higher.
- **ACL (PR\_1000389442)** — Numbering restrictions are not enforced at the CLI; ACLs numbered 200 or higher are considered valid. This fix enforces ACL numbering restrictions and converts existing ACLs numbered 200 or higher into named ACLs. If an invalid name of form XXX is found, it will be converted to "invalidXXX".

---

### Note:

*If you have ACLs configured with numbers greater than or equal to 200, you need to reconfigure those ACLs with either a valid name or valid number prior to loading K.12.01 software, or it will be tagged as invalid. For example, if you have an ACL called 222 and it is applied to a vlan, the K.12.01 script will convert the 222 ACL to "invalid222" and apply it to the vlan.*

---

- **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\_1000385237)** — Applying an access control list with more than 105 entries to a VLAN interface causes the switch to crash with a message similar to:

```
Software exception at enDecode.c:54 -- in 'mSess1',  
task ID = 0x8e7da60 -> out of memory!
```

- **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\_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 the ProCurve 100-FX SFP-LC Transceiver (J9054B).
- **Enhancement (PR\_1000376626)** — Enhance 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.
- **Event Log (PR\_1000330310)** — Failed attempts to communicate with an unknown module type fill the event log message buffer.
- **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.
- **OSPF (PR\_1000374003)** — The switch assigns itself a router-id of the neighbor router's in a virtual link.

---

**Note:**

*Existing OSPF virtual link configurations may be lost with the update to K.12.01. Either save the K.11 configuration and reload it once the switch is running K.12, or plan to reconfigure any virtual links at the CLI after booting into the K.12.01 software.*

---

- **SNMP (PR\_1000392847)** — RMON alarms that monitor port-specific OIDs are lost if the switch is rebooted.

## Version K.12.02

The following problems were resolved in release K.12.02

- **Crash (PR\_1000398746)** — The switch may crash with the task "swlnitTask". 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:0x08a7c870
```
- **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.
- **Proxy-ARP (PR\_1000393571)** — Proxy-ARP sends responses to gratuitous ARPs.
- **Remote Mirroring/Trunking (PR\_1000397196)** — Remote mirroring configured on a trunk does not restart after the switch is rebooted. Workaround: after a switch reboot, reconfigure the trunk remote as a mirroring source.
- **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.

## Version K.12.03

The following problems were resolved in release K.12.03 (not a general release)

- **CLI (PR\_1000373443)** — The CLI **update** command help text and confirmation message is misleading and confusing.
- **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 = 0x8347161
```
- **Crash (PR\_1000401664)** — Use of the CLI command **dir** with a very large path name may cause the switch to crash with a message similar to:

```
PC Data Storage (Bus Error) exception vector 0x300:
Stack Frame=0x08e54928 HW Addr=0x00b3eefc IP=0x0018a740
Task='mSess2' Task ID=00 fp: 0x00000000 sp:
```
- **Enhancement (PR\_1000379804)** — Historical information about MAC addresses that have been moved has been added to the **show tech** command output.

- **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.
- **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..

## Version K.12.04

Software never released.

- **ACL (PR\_1000402901)** — The ACL resequencing feature may discard some ACEs in a random fashion.
- **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
```

- **Enhancement MSTP (PR\_1000369492)** — Update of MSTP implementation to the latest IEEE P802.1Q-REV/D5.0 specification to stay in compliance with the protocol evolution.

---

### Note

The updated standard provides auto-edge-port operation for MSTP, and supports the automatic detection of edge ports. The port will look for BPDUs for 3 seconds; if there are none, it begins forwarding packets. For more information on selected configuration options and updated MSTP port parameters, see [“Release K.12.04 Enhancements” on page 19](#).

---

- **Remote Mirroring/SNMP (PR\_1000395595)** — Removing a VLAN via SNMP does not remove the related ACL relationship to that VLAN.
- **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.

## Version K.12.05

The following problems were resolved in release K.12.05.

- **BootROM (PR\_1000402707)** — BootROM does not update to latest version when updating code to primary flash.
- **CLI (PR\_1000309998)** — Management module is incorrectly displayed as J8627A rather than the correct J8726A product number in response to the **show modules** command.
- **Enhancement (PR\_1000408960)** — RADIUS-Assigned GVRP VLANs enhancement. For more information, see [“Release K.12.05 Enhancements” on page 22](#).
- **Menu (PR\_1000392862)** — The menu will allow invalid values (greater than 720 sec) to be entered for the SNMP poll interval.

## Version K.12.06

Software never released.

- **Enhancement (PR\_1000308332)** — Passwords (hashed) are saved to the configuration file. For more information, see [“Release K.12.06 Enhancements” on page 29](#).

## Version K.12.07

The following problems were resolved in release K.12.07.

- **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 config <filename>** does not remove a file containing the problem characters.
- **Config (PR\_1000410790)** — Errors are returned when applying the **interface <port-list> speed-duplex auto-10-100** command to interfaces 45 through 48 on a 3500y1-48G-PWR switch.
- **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 reboot.

## Version K.12.08

Software never released.

- **Enhancement (PR\_1000413764)** — Increase the size of the `sysLocation` and `sysContact` entries from 48 to 255 characters. For more information, see [“Release K.12.08 Enhancements” on page 43](#).

## Version K.12.09

The following problem was resolved in release K.12.09 (Not a general release).

- **Crash (PR\_1000385844)** — With `sFlow` sampling enabled, the switch may crash with a message similar to:

```
Software exception at ngDmaTx.c:729 -- in 'tDevPollTx',  
task ID = 0x4305bba8 -> HW DMA DRIVER unable to transmit anymore
```

## Version K.12.10

The following problems were resolved in release K.12.10.

- **ARP (PR\_1000414347)** — ARP table address learning is slow; once the switch has its ARP table cleared, the clients will be unable to communicate for approximately 30 seconds.
- **Config (PR\_1000416508)** — Cannot create alternate startup-config file. Although **show config files** shows an available slot, the switch does not allow copying from an existing config file to create a new config file in the vacant slot.
- **Crash (PR\_1000421322)** — Following execution of config-related CLI commands (such as **show running-config** or **show tech**) or when PCM attempts to retrieve the configuration file using TFTP from a switch having a large configuration file, the switch may crash with a message similar to:

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

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

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

- **Enhancement (PR\_1000419653)** — The **show vlan** command was enhanced to display each port in the VLAN separately, display the friendly port name (if configured), and display the VLAN mode (tagged/untagged/forbidden) for each port. For more information, see [“Release K.12.10 Enhancements” on page 44](#).

- **SNMP (PR\_1000374893)** — When retrieving the switch serial number via SNMP, the management module serial number is returned instead of the chassis serial number.
- **SNMP (PR\_1000422129)** — HP Fault Finder doesn't send the interface index with the SNMP trap, even though it is listed in the system log.

## Version K.12.11

Software never released.

## Version K.12.12

The following problems were resolved in release K.12.12 (Not a general release).

- **Crash (PR\_1000420709)** — Entering a backslash at the CLI may cause the switch to crash with a message similar to:  

```
PPC Data Storage (Bus Error) exception vector 0x300:  
Stack Frame=0x08e66508 HW Addr=0x00b4f2ac IP=0x0018a864  
Task='mSess1' Task ID=0x8e67170 fp: 0x3be00000 sp:
```
- **Link LED (PR\_1000425143)** — The Small Form-factor Pluggable (SFP) link LED does not work when SFP is hot-swapped into the switch.

## Version K.12.13

Software never released.

## Version K.12.14

The following problems were resolved in release K.12.14.

- **Authentication (PR\_1000422933)** — Issue with local password authentication.
- **CLI/Clear button (PR\_1000424194)** — The command **no password manager** deletes the password, but fails to delete the username. Similarly, pressing the clear button deletes the password but not the username.
- **SNMP (PR\_1000423362)** — Setting username via SNMP (**hpSwitchAuthMIB**) deletes the password.

- **Hotswap (PR\_1000422714)**—Hotswapping a module may result in a false module self-test failure. After hotswapping the module, the following messages may appear in the event log:

```
I 05/27/06 12:06:54 00076 ports: port B23 is now on-line
W 05/27/06 12:07:00 00564 ports: port B23 PD Invalid Signature indication
I 05/27/06 12:32:47 00068 chassis: Slot B Inserted
I 05/27/06 12:32:48 00068 chassis: Slot B Inserted
I 05/27/06 12:32:49 00068 chassis: Slot B Inserted
I 05/27/06 12:32:50 00067 chassis: Slot B Removed
I 05/27/06 12:32:50 00077 ports: port B23 is now off-line
W 05/27/06 12:33:11 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:34 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:33:57 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:19 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:34:42 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
I 05/27/06 12:34:44 00179 mgr: SME CONSOLE Session - MANAGER Mode
W 05/27/06 12:35:05 00374 chassis: Slot B Slave ROM Tombstone: 0x00000000
W 05/27/06 12:35:05 00274 chassis: Slot B self test failure or unsupported
```

Multiple insertion messages may be included. The errors appear in the log as either a tombstone, HSL failure, or a loss of communications.

## Version K.12.15

The following problems were resolved in release K.12.15.

- **Enhancement (PR\_1000427592)**— This enhancement adds the client's IP address to the RADIUS accounting packets sent to the RADIUS server by the switch.
- **Crash (PR\_1000407238)**— Execution of the "show config" command when the startup configuration is different than the running configuration may cause the switch to crash with a message similar to:

```
Software exception at cli_mirror.c:6201 -- in 'mSess1', task ID =
0x8e53690 -> ASSERT: failed
```
- **SNMP (PR\_1000406398)**— The URL embedded SNMP traps are not sent as SSL (https) when SSL is enabled, but are sent as plain-text (http) instead. This may result in the trap receiver (such as PCM) being unable to display the URL if SSL is enabled.
- **Enhancement (PR\_1000428642)**— The SNMP v2c describes two different notification-type PDUs: traps and informs. Prior to this software release, only the trap's sub-type was supported. This enhancement adds support for informs.
- **Crash (PR\_1000427674)**— False positive memory testing may result in an ACL interrupt crash with an event log message similar to:

```
chassis: Slot L ACL Int status=0x2000000 25=0x80000005:
Task=tDevPollRx Task ID=0x4305d314 IP=0x40087044
```

- **Rate-Limiting (PR\_1000420720)** — Rate limiting is broken beyond 9.5 Mbps. For any rate limit set to more than 9.5 Mbps, the actual rate drops to 1 Mbps.

## Version K.12.16

The following problems were resolved in release K.12.16.

- **Crash (PR\_1000415621)** — Removing a VLAN that has OSPF configured may cause the switch to crash with a message similar to:

```
NMI event HW:IP=0x0084a0a4 MSR:0x00029210 LR:0x00513ee4 Task='eRou-  
teCtrl' Task ID=0x89658b0'
```

- **Crash (PR\_1000428582)** — Typing non-alphanumeric characters at the CLI prompt may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300:Stack  
Frame=0x08e36878 HW Addr=0x00b4f2ec IP=0x0018a974 Task='mSess1' Task  
ID=0x0fp: 0x18020800 sp:
```

## Version K.12.17

The following problems were resolved in release K.12.17.

- **STP (PR\_1000420442)** — The switch erroneously allows configuration of spanning tree parameters on an interface that is a member of a trunk (link aggregation group), which creates an invalid configuration.
- **CLI (PR\_1000429474)** — The "all" parameter is missing from the "password" command.
- **Radius (PR\_1000432556)** — When DHCP snooping is enabled on the client VLAN, and the client is on a VLAN other than the default VLAN, the Framed-IP-Address attribute is not added to the RADIUS accounting packet as it should be.
- **Crash (PR\_1000416453)** — Execution of the "show tech" command in an SSH session may cause the switch to crash with a message similar to:

```
Software exception - Assert in pmgr_util.c:1155 -- in 'mSess2', task  
ID = 0x85adf60
```

## Version K.12.18

The following problems were resolved in release K.12.18.

**Software Fixes in Release K.11.12 - K.12.25**  
Version K.12.19

- **CLI (PR\_1000419379)** — The “interface” command does not exist in the VLAN context, resulting in an inability to shift to the interface configuration context directly from the VLAN context.
- **Hang (PR\_1000434809)** — The switch may hang, causing all the port LEDs to remain lit, and stop transmitting traffic.
- **Enhancement (PR\_1000428213)** — This software enhancement adds the ability to configure a secondary authentication method to be used when the RADIUS server is unavailable for the primary port access method.
- **Crash (PR\_1000436274)** — Typing a question mark (“?”) at the "multi-line" input prompt (“>”) may cause the switch to crash. The crash occurs when the switch is trying to print the error message that states:  

```
Expansion help not available on multi-line input.
```
- **CLI (PR\_1000433948)** — When command authorization is in use, the "show tech" command fails at the “show tech buffer” component, even when the permission list indicates that it should be allowed.
- **Enhancement (PR\_1000415155)** — The ARP age timer was enhanced from the previous limit of 240 minutes to allow for configuration of values up to 1440 minutes (24 hours) or "infinite" (99,999,999 seconds or 32 years).
- **Enhancement (PR\_1000438015)** — The banner message of the day (MOTD) size has been increased to support up to 3070 characters.

## Version K.12.19

The following problems were resolved in release K.12.19.

- **ACL (PR\_1000432563)** — ACLs with the "permit" parameter on L4 ports and using operators ‘gt’/‘lt’/‘range’ do not function as expected. The ACL does not drop traffic with non-permitted L4 ports. Instead, all traffic with L4 ports is forwarded.
- **CLI (PR\_1000438486)** — When using the "port-access mac-based" CLI command, the client MAC address is sent in lower case and as the username to the RADIUS server. This fix adds an option so that the MAC address is in uppercase when sent to the RADIUS server. This fix adds additional parameters to the CLI command to support this: "aaa port-access mac-based addr-format."
- **10-GbE Log (PR\_1000424384)** — The switch is not checking for the presence of the J8694A ProCurve yl 10G X2-CX4 module early enough in the boot process, triggering a log message when the check is executed.



## Version K.12.20

The following problems were resolved in release K.12.20 (never released).

## Version K.12.21

The following problems were resolved in release K.12.21 (never released).

- **ARP Protection (PR\_1000438129)** — ARP and ARP protection data may not display correctly following a CLI or SNMP status query.
- **Enhancement (PR\_1000440049)** — Classifier-Based Rate Limiting capability was added. Classifier-Based Rate Limiting (also known as Rate Limit Port ACLs or RL-PACLs) allows you to create an ACL and apply it on a per-port basis to rate-limit network traffic.
- **CLI (PR\_1000342461)** — If a trunk is configured, output from the CLI command “show lldp info remote <port number>” reports incorrect information for the remote management address.
- **Enhancement (PR\_1000374051)** — The 5400zl switches are not detecting packets from an Avaya G700 PBX or Cajun switch due to irregular Ethernet packets sent by those devices. This is a workaround that will alter the 5400zl software to allow 100Mb operation on the upcoming "C" revision of the 1000 Base-T Mini-GBICs (J8177C) that fit in the J8705A module. The port containing the 1000 Base-T Mini-GBIC can be configured with new speed options of "auto-100," "100-full," and "100-half."
- **Crash (PR\_1000434888)** — A switch module may crash with a message similar to:

```
ACL Int status=0x10000000 28=0x80002f3a: Task=tDevPollTx Task
ID=0x4305c504 IP=0x400693e8
```
- **Enhancement (PR\_1000443349)** — This enhancement is to allow the concurrent use of SFTP with TACACS+ authentication for SSH connections.
- **VRRP/Meshing (PR\_1000435853)** — A MESHed link in the path between a VRRP Owner and VRRP Backup may lead to a situation where both VRRP routers remain in Master state for a VRID after that VRID fails over to the Backup and then the Owner comes back online.
- **Routing (PR\_1000432449)** — If the switch is configured with both port security and routing, a physical port transition on the host may cause the switch to stop transmitting routed traffic to that host. Clearing the ARP cache resolves this problem until another port transition occurs.

- **RADIUS (PR\_1000442879)** — If RADIUS (or TACACS+) keys are configured, and then the switch is updated to a software revision with the ability to save the security credentials in the configuration file (K.12.06 or later), the RADIUS keys are no longer shown in output from the "show run" or "show config" commands until the "include-credentials" command is issued.

## Version K.12.22

The following problems were resolved in release K.12.22.

- **Enhancement (PR\_1000443026)** — Support for the new revision "C" Mini-GBICs was added to the CLI and the "show tech" command.
- **Enhancement (PR\_1000444415)** — OSPF Passive Interface support was added.
- **Crash (PR\_1000442695)** — Pasting a VRRP configuration into the running configuration via a telnet session may cause the switch to crash with a message similar to:

```
Software exception at vrrp_statemach.c:205 -- in 'mVrrpCtrl', task
ID = 0x8b154a0-> internal error
```

## Version K.12.23

The following problems were resolved in release K.12.23.

- **Crash (PR\_1000415534)** — Execution of the "lockout-mac" CLI command, may cause the switch to crash with a message similar to:

```
PPC Data Storage (Bus Error) exception vector 0x300: Stack
Frame=0x0ab9a738 HW Addr=0x00b3f104 IP=0x00801d2c Task='eDrvPoll'
Task ID=0xab9ad20 fp: 0x0f3808c0 sp
```

- **AAA/CLI (PR\_1000445886)** — This changes the syntax of 'aaa authentication <port-access | mac-based | web-based>' commands which were previously added in PR\_1000438486.
- **CLI (PR\_1000403478)** — Power over Ethernet (802.3af) CLI commands were removed from platforms that do not support PoE (such as the ProCurve 6200yl switch).
- **Broadcast-limit (PR\_1000429594)** — The broadcast limit feature affects multicast traffic. This fix modifies the feature so that it only affects broadcast traffic.
- **MSTP (PR\_1000439775)** — The switch generates a topology change when a port goes offline. With MSTP enabled and all ports left at default (auto-edge-port), when a port transitions to offline, a TC will be generated, and the topology change counter increases.

- **Multicast (PR\_1000436118)** — Multicast forwarding with IGMP is slow and causes an unacceptable delay in servicing.
- **Enhancement (PR\_1000449129)** — This enhancement allows MAC or Web-based authentication to use PEAP/MS-CHAPv2 protocols in addition to the default setting of CHAP.
- **Crash (PR\_1000444112)** — Downloading a configuration file to the switch may cause a crash with a message similar to:  

```
Software exception at cli_config_action.c:5479 -- in 'mftTask'
```
- **SNMP (PR\_1000448463)** — The SNMP Engine ID Discovery process described in RFC 3414 is not working properly.

## Version K.12.24

The following problems were resolved in release K.12.24.

- **Hang (PR\_1000448429)** — A bank of ports may fail the self test, crash or stop functioning after several weeks of use.

## Version K.12.25

The following problems were resolved in release K.12.25.

- **Config (PR\_1000451779)** — Software update, TFTP restoration of the configuration or reloading the switch on software version K.12.22 may delete a Mini-GBIC VLAN port assignment.



© 2006 - 2007 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

August 2007  
Manual Part Number  
5991-4720