



## Release Notes:

### Version K.11.41 Software

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

---

The K.11.41 software supports these switches:

- ProCurve Switch 3500yl-24G-PWR (J8692A) and 3500yl-48G-PWR (J8693A)
- ProCurve Switch 6200yl-24G-mGBIC (J8992A)
- ProCurve Switch 5406zl (J8697A), 5412zl (J8698A ), and 5406zl-48G (J8699A)

These release notes include information on the following:

- Downloading switch software and documentation from the Web ([page 1](#))
- Clarification of operating details for certain software features ([page 8](#))
- A listing of software enhancements in this release ([page 9](#))
- A listing of software fixes included in releases K.11.11 through K.11.41 ([page 31](#))

### **Related Publications**

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

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

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

## Publication Number

5991-4720  
August 2006 -B

## 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)

## 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 .....	5
Saving Configurations While Using the CLI .....	6
ProCurve Switch, Routing Switch, and Router Software Keys .....	7
OS/Web/Java Compatibility Table .....	7
<b>Clarifications and Updates</b> .....	<b>8</b>
<b>Enhancements</b> .....	<b>9</b>
Release K.11.12 Enhancements .....	9
MSTP Default Path Cost Controls .....	9
Release K.11.13 through K.11.32 Enhancements .....	9
Release K.11.33 Enhancements .....	9
Release K.11.34 Enhancements .....	9
Increased Number of Telnet Sessions .....	10
CLI-Configured sFlow with Multiple Instances .....	10
Event Log Display Options .....	13
Scheduled Reload .....	14
Release K.11.35 Enhancements .....	15
Spanning Tree Per-Port BPDU Filtering .....	15
DHCP Option 82: Using the Management VLAN IP Address for the Remote ID .....	19
Release K.11.36 through K.11.39 Enhancements .....	21
Release K.11.40 Enhancements .....	21
Spanning Tree BPDU Protection .....	21
Release K.11.41 Enhancements .....	24
Uni-Directional Link Detection (UDLD) .....	24

<b>Software Fixes in Release K.11.12 - K.11.3x</b> . . . . .	<b>31</b>
Release K.11.12 . . . . .	31
Release K.11.13 . . . . .	32
Release K.11.14 . . . . .	32
Release K.11.15 . . . . .	32
Release K.11.16 . . . . .	33
Release K.11.17 . . . . .	33
Release K.11.32 . . . . .	33
Release K.11.33 . . . . .	36
Release K.11.34 . . . . .	37
Release K.11.35 . . . . .	37
Release K.11.36 . . . . .	38
Release K.11.37 . . . . .	38
Release K.11.38 . . . . .	38
Release K.11.39 . . . . .	38
Release K.11.40 . . . . .	39
Release K.11.41 . . . . .	39

# 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 April, 2006, 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, visit the ProCurve “Manuals” website at: [www.hp.com/rnd/support/manuals/index.htm](http://www.hp.com/rnd/support/manuals/index.htm), and click on one of the following links:

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

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



## Xmodem Download From a PC or Unix Workstation

This procedure assumes that:

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

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

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

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

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

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

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

2. Execute the following command in the CLI:

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

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

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

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

## Software Management

### Saving Configurations While Using the CLI

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

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

---

## Saving Configurations While Using the CLI

The switch operates with two configuration files:

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

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

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

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

## ProCurve Switch, Routing Switch, and Router Software Keys

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

## OS/Web/Java Compatibility Table

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

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

## Clarifications and Updates

---

The following clarification or updates apply to documentation for the ProCurve 3500yl Series, 6200yl Series, and 5400zl Series switches as of August 2006.

- Clarification to the **Operating Rules**: related to use of **Jumbo Packets** (see pages 13-28 and 13-32 in the Management and Configuration Guide), the existing documentation erroneously notes that **Flow Control** must be disabled. The switch allows flow control and jumbo packet capability to co-exist on a port, thus you do not need to disable flow control when configuring for jumbo packets.
- Correction to MSTP information on page 4-15 in the Advanced Traffic Management Guide: The 3500yl, 5300zl, and 6200yl switches support only Multiple Instance Spanning Tree (MSTP). These switches are backward compatible with switches that support STP or RSTP.
- Clarification for the Number of IP addresses and maximum VLANs that can be configured on the switch. (refer to the Advanced Traffic Management Guide for additional details):

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.

# Enhancements

---

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

## Release K.11.12 Enhancements

Release K.11.12 includes the following enhancement:

### MSTP Default Path Cost Controls

**Summary:** 802.1D and 802.1t specify different default path-cost values (based on interface speed). These are used if the user hasn't configured a "custom" path-cost for the interface. The default of this toggle is to use 802.1t values. The reason one might set this control to 802.1D would be for better interoperability with legacy 802.1D STP (Spanning Tree Protocol) bridges.

To support legacy STP bridges, the following commands (options) have been added to the CLI:

**spanning-tree legacy-path-cost** - Use 802.1D values for default path-cost

**no spanning-tree legacy-path-cost** - Use 802.1t values for default path-cost

The "legacy-path-cost" CLI command does not affect or replace functionality of the "spanning-tree force-version" command. The "spanning-tree force-version" controls whether MSTP will send and process 802.1w RSTP, or 802.1D STP BPDUs. Regardless of what the "legacy-path-cost" parameter is set to, MSTP will interoperate with legacy STP bridges (send/receive Config and TCN BPDUs).

When legacy-path-cost control is toggled, all default path costs will be recalculated to correspond to the new setting, and spanning tree is recalculated if needed.

## 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 (see below)
- CLI-configured sFlow with multiple instances (see below)
- Event log display options (see page 13)
- Scheduled reload (see page 14)

## Increased Number of Telnet Sessions

Beginning with software release K.11.34, 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 three distinct sFlow instances: once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. CLI-configured sFlow instances may be saved to the startup configuration to persist across a switch reboot.

### Terminology

**sFlow** — An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

**sFlow agent** — A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

**sFlow destination** — The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

### Configuring sFlow

The following sFlow commands allow you to configure sFlow instances via the CLI.

**Syntax:** [no] sflow <receiver-instance> destination <ip-address> [udp-port-num]

*Enables an sFlow receiver/destination. The receiver-instance number must be a 1, 2, or 3. By default, the udp destination port number is 6343.*

*To disable an sFlow receiver/destination, enter no sflow <receiver-instance>.*

**Syntax:** sflow <receiver-instance> sampling <port-list> <sampling rate>

Once an sFlow receiver/destination has been enabled, this command enables flow sampling for that instance. The receiver-instance number is 1, 2, or 3, and the sampling rate is the allowable non-zero skipcount for the specified port or ports. To disable flow-sampling for the specified port-list, repeat the above command with a sampling rate of “0”.

**Syntax:** sflow <receiver-instance> polling <port-list> <polling interval>

Once an sFlow receiver/destination has been enabled, this command enables counter polling for that instance. The receiver-instance number is 1, 2, or 3, and the polling interval may be set to an allowable non-zero value to enable polling on the specified port or ports.

To disable counter-polling for the specified port-list, repeat the above command with a polling interval of “0”.

---

## Note

Under the multiple instance implementation, sFlow can be configured via the CLI or via SNMP. However, CLI-owned sFlow configurations cannot be modified via SNMP, whereas SNMP-owned instances can be disabled via the CLI using the **no sflow** <receiver-instance> command.

---

## Viewing sFlow Configuration

The following sFlow commands allow you to display sFlow configuration and status via the CLI.

**Syntax:** show sflow agent

*Displays sFlow agent information. The agent address is normally the ip address of the first vlan configured.*

**Syntax:** show sflow <receiver instance> destination

*Displays information about the management station to which the sFlow sampling-polling data is sent.*

**Syntax:** show sflow <receiver instance> sampling-polling <port-list/range>

*Displays status information about sFlow sampling and polling.*

The **show sflow agent** command displays read-only switch agent information. The version information shows the sFlow version, MIB support and software versions; the agent address is typically the ip address of the first vlan configured on the switch.

```
ProCurve# show sflow agent

Version          1.3;HP;K.11.40
Agent Address    10.0.10.228
```

**Figure 1. Example of Viewing sFlow Agent Information**

The **show sflow <instance> destination** command includes information about the management-station's destination address, receiver port, and owner.

```
ProCurve# show sflow 2 destination

Destination Instance      2
sflow                    Enabled
Datagrams Sent           221
Destination Address      10.0.10.41
Receiver Port            6343
Owner                    Administrator, CLI-owned, Instance 2
Timeout (seconds)        99995530
Max Datagram Size        1400
Datagram Version Support  5
```

**Figure 2. Example of Viewing sFlow Destination Information**

Note the following details:

- **Destination Address** remains blank unless it has been configured.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.
- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

The **show sflow <instance> sampling-polling [port-list]** command displays information about sFlow sampling and polling on the switch. You can specify a list or range of ports for which to view sampling information.

```
ProCurve# show sflow 2 sampling-polling A1-A4
```

Number denotes the sampling/polling instance to which the receiver is coupled.

Port	Sampling			Dropped					Polling						
	Enabled	Rate	Header	Samples					Enabled	Interval					
A1	Yes(2)	40	128	1	2	3	4	5	6	7	8	9	0	---	---
A2	---	---	---	0					Yes(1)	60					
A3	No(1)	0	100	898703					No	30					
A4	Yes(3)	50	128	0					No(3)	0					

**Figure 3. Example of Viewing sFlow Sampling and Polling Information**



---

## Note

The sampling and polling instances (noted in parentheses) coupled to a specific receiver instance are assigned dynamically, and so the instance numbers may not always match. The key thing to note is whether sampling or polling is enabled on a port, and the sampling rates or polling intervals for the receiver instance configured on each port.

---

## Event Log Display Options

Beginning with software release K.11.34, two new options have been added to provide greater flexibility in viewing event log entries via the CLI.

### Display the Most Current Entries First

The **show logging** command displays all event log entries in chronological order from the oldest to the newest entry. Beginning with software release K.11.34, the following **-r** option has been added to reverse the standard display such that the most current recent log entries are listed first.

**Syntax:** show logging [-r]

*Lists all recorded log messages since the last reboot, with the most recent entries listed first.*

### Clear Event Log Entries

Beginning with software release K.11.34, a **logging** option has been added to the existing CLI **clear** command to remove all event log entries from the **show logging** display output.

**Syntax:** clear logging

*Removes all entries from the event log display output.*

---

## Note

The **clear logging** command causes event log entries to be hidden from display when using the standard **show logging** command. The **show logging -a** command option can still be used to display all hidden items, including event log entries recorded prior to the last reboot.

---

## Scheduled Reload

In earlier software releases, the **reload** command had no scheduling capabilities. Beginning with software release K.11.34, additional parameters have been added to the reload command to allow for a scheduled reboot of the switch via the CLI.

**Syntax:** reload [after <[dd:]hh:]mm> | at <hh:mm[:ss]> [<mm/dd/[yy]yy>] | cancel]

*Enables a scheduled warm reboot of the switch. Parameters include:*

- **after:** Schedules a warm reboot of the switch after a given amount of time has passed.
- **at:** Schedules a warm reboot of the switch at a given time.
- **cancel:** Removes a pending reboot request.

The scheduled reload feature supports the following capabilities:

- It removes the requirement to physically enter a reload command at inconvenient times (for example, at 1:00 in the morning). Instead, a **reload at 1:00 mm/dd** command can be executed (where *mm/dd* is the date the switch is scheduled to reboot).
- It provides a safety net in situations where a change is made from a remote location to the running config that inadvertently causes loss of management access. For example, a newly configured ACL might deny access to the switch from the management station's IP address such that the telnet session ceases to function. Scheduling a **reload after** command (timed to execute after the necessary configuration work is completed) will ensure that the switch will reboot automatically. Assuming the ACL changes were not saved to the startup config, telnet access will then be restored. If the ACL work is completed successfully, with no loss of access, the scheduled reboot can be cancelled with the **reload cancel** command.

## Operating Notes

- If no parameters are entered after the **reload** command, an immediate reboot is executed.
- The **reload at** and **reload after** command information is not saved across reboots. If the switch is rebooted before a scheduled reload command is executed, the command is effectively cancelled.
- When entering a **reload at** or **reload after** command, a prompt will appear to confirm the command before it can be processed by the switch.
- For the **reload at** command, if mm/dd/yy are left blank, the current day is assumed.

## Command Examples

To schedule a reload in 15 minutes:

```
ProCurve# reload after 15
```

To schedule a reload in 3 hours:

```
ProCurve# reload after 03:00
```

To schedule a reload for the same time the following day:

```
ProCurve# reload after 01:00:00
```

To schedule a reload for the same day at 12:05:

```
ProCurve# reload at 12:05
```

To schedule a reload on some future date:

```
ProCurve# reload at 12:05 01/01/2007
```

## Release K.11.35 Enhancements

Release K.11.35 includes the following enhancement:

- Added support for STP Per-Port BPDU Filtering and SNMP Traps. (See “Spanning Tree Per-Port BPDU Filtering” on page 15.)
- 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. (See “DHCP Option 82: Using the Management VLAN IP Address for the Remote ID” on page 19.)

## Spanning Tree Per-Port BPDU Filtering

The STP BPDU filter feature allows control of spanning-tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets and stay locked in the spanning-tree forwarding state. All other ports will maintain their role.

Here are some sample scenarios in which this feature may be used:

- To have STP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.
- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of standard spanning-tree operations.

- To protect the network from denial of service attacks with spoofing spanning-tree BPDUs by dropping incoming BPDU frames.

---

## Note

BPDU protection imposes a more secure mechanism that implements port shut down and a detection alert when an errant BPDU frame is received (see page 21 for details). BPDU protection will take precedence over BPDU filtering if both features have been enabled on the same port.

---

## Configuring STP BPDU Filters

The following commands allow you to configure BPDU filters via the CLI.

**Syntax:** [no] spanning-tree <port-list | all> bpdu-filter

*Enables/disables the BPDU filter feature on the specified port(s).*

For example, to configure BPDU filtering on port a9, enter:

```
ProCurve(config)# spanning-tree a9 bpdu-filter
```

---

## Caution

Ports configured with the BPDU filter mode remain active (learning and forward frames); however, spanning-tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and remove ("no") the bpdu-filter.

---

## Viewing Status of BPDU Filtering

The **show spanning-tree <port-list> detail** command has been extended to show per-port BPDU filter mode as shown below.

```

ProCurve# show spanning-tree a9 detail

Status and Counters - CST Port(s) Detailed Information

Port                : A1
Status              : Up
BPDU Filtering      : Yes
Errant BPUDUs received : 65
MST Region Boundary : Yes
External Path Cost  : 200000
External Root Path Cost : 420021
Administrative Hello Time : Use Global
Operational Hello Time  : 2
AdminEdgePort       : No
OperEdgePort        : No
AdminPointToPointMAC : Force-True
OperPointToPointMAC  : Yes
Aged BPDUs Count    : 0
Loop-back BPDUs Count : 0
TC ACK Flag Transmitted : 0
TC ACK Flag Received  : 0

MST BPDUs Tx  MST BPDUs Rx  CFG BPDUs Tx  CFG BPDUs Rx  TCN BPDUs Tx  TCN BPDUs Rx
-----
8          28          0          0          0          0
  
```

The diagram includes two callout boxes with arrows pointing to specific fields in the command output:

- A box pointing to the 'BPDU Filtering : Yes' and 'Errant BPUDUs received : 65' lines, with the text: "Rows indicating BPDU filtering has been enabled and number of errant BPDUs received."
- A box pointing to the 'MST BPDUs Rx' field in the summary table, with the text: "Column indicating BPDU frames accepted for processing when permitted by BPDU filter."

**Figure 4. Example of BPDU Filter Fields in Show Spanning Tree Detail Command**

The **show spanning-tree** command has also been extended to display BPDU filtered ports.

```
ProCurve# show spanning-tree

Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-7
...

Protected Ports :
Filtered Ports   : A6-A7
....
```

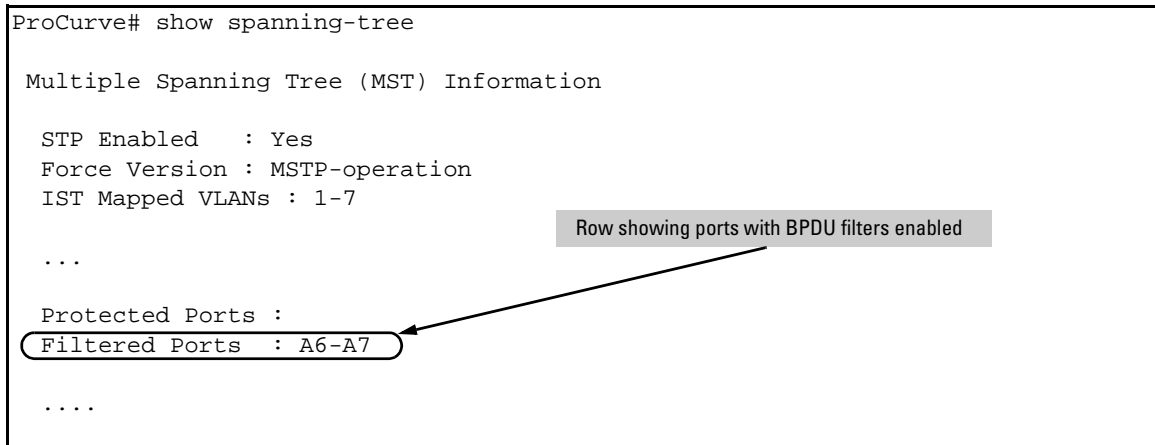


Figure 5. Example of BPDU Filtered Ports Field in Show Spanning Tree Command

### Viewing Configuration of BPDU Filtering

The BPDU filter mode adds an entry to the spanning tree category within the configuration file.

```
ProCurve(config)# show configuration
. . .
spanning-tree
spanning-tree A7 bpdu-filter
spanning-tree C9 bpdu-filter
spanning-tree Trk2 priority 4
. . .
```

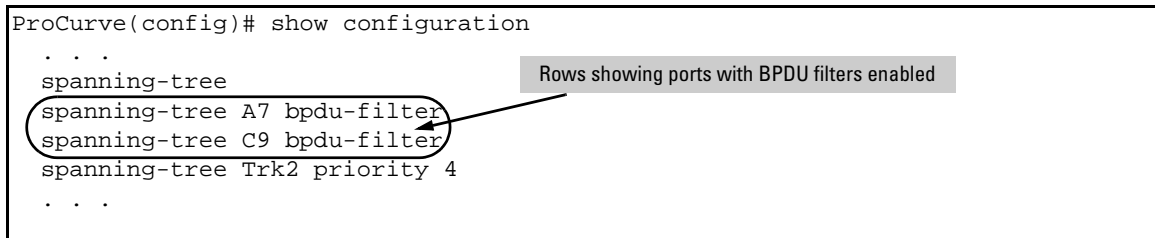


Figure 6. Example of BPDU Filters in the Show Configuration Command

The **spanning-tree show < port> configuration** command displays the BPDU's filter state.

```
ProCurve(config)# show spanning-tree a8 config

...

Port Type      | Cost      Priority Edge Point-to-Point MCheck Filter
-----+-----
A8 100/1000T | Auto     128    Yes  Force-True   Yes   No
```

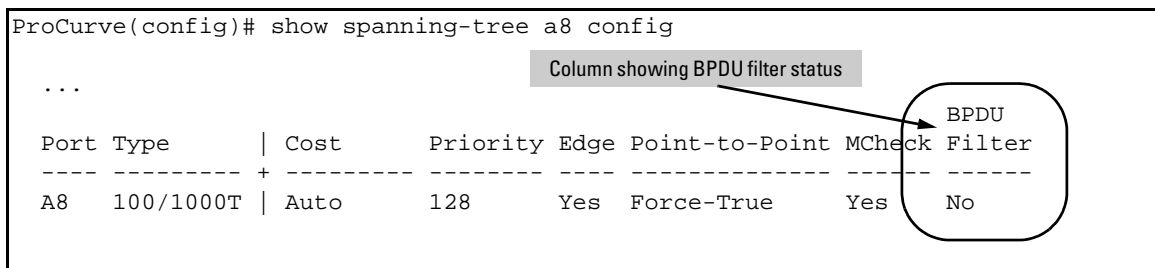


Figure 7. Example of BPDU Filter Status in Show Spanning Tree Configuration Command

## DHCP Option 82: Using the Management VLAN IP Address for the Remote ID

This section describes the Management VLAN enhancement to the DHCP option 82 feature. For more information on DHCP option 82 operation, refer to “Configuring DHCP Relay” in the chapter titled “IP Routing Features” in the *Advanced Traffic Management Guide* for your switch.

When the routing switch is used as a DHCP relay agent with Option 82 enabled, it inserts a relay agent information option into client-originated DHCP packets being forwarded to a DHCP server. The option automatically includes two suboptions:

- Circuit ID: the identity of the port through which the DHCP request entered the relay agent
- Remote ID: the identity (IP address) of the DHCP relay agent

Using earlier software releases, the remote ID can be either the routing switch’s MAC address (the default option) or the IP address of the VLAN or subnet on which the client DHCP request was received. Beginning with software release K.11.35, if a Management VLAN is configured on the routing switch, then the Management VLAN IP address can be used as the remote ID.

**Syntax:** `dhcp-relay option 82 < append | replace | drop > [ validate ] [ ip | mac | mgmt-vlan ]`

**[ ip | mac | mgmt-vlan ] :** *Specifies the remote ID suboption the routing switch will use in Option 82 fields added or appended to DHCP client packets. The choice depends on how you want to define DHCP policy areas in the client requests sent to the DHCP server. If a remote ID suboption is not configured, then the routing switch defaults to the **mac** option.*

**mgmt-vlan:** *Specifies the IP address of the (optional) Management VLAN configured on the routing switch. Requires that a Management VLAN is already configured on the switch. If the Management VLAN is multinetted, then the primary IP address configured for the Management VLAN is used for the remote ID.*

**ip:** *Specifies the IP address of the VLAN on which the client DHCP packet enters the routing switch. In the case of a multinetted VLAN, the remote ID suboption uses the IP address of the subnet on which the client request packet is received.*

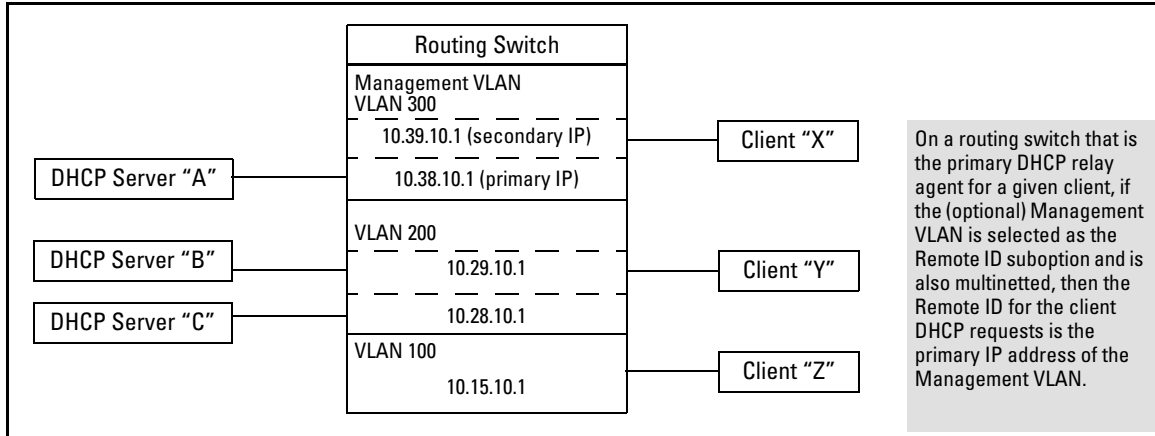
**mac:** *Specifies the routing switch’s MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.)*  
(Default: **mac**)

### Example

In the routing switch shown below, option 82 has been configured with **mgmt-vlan** for the Remote ID.

```
ProCurve(config)# dhcp-relay option 82 append mgmt-vlan
```

The resulting effect on DHCP operation for clients X, Y, and Z is shown in [table 1](#).



**Figure 8. DHCP Option 82 When Using the Management VLAN as the Remote ID Suboption**

**Table 1. DHCP Operation for the Topology in Figure 8**

Client	Remote ID	giaddr*	DHCP Server	
X	10.38.10.1	10.39.10.1	A only	If a DHCP client is in the Management VLAN, then its DHCP requests can go only to a DHCP server that is also in the Management VLAN. Routing to other VLANs is not allowed.
Y	10.38.10.1	10.29.10.1	B or C	Clients outside of the Management VLAN can send DHCP requests only to DHCP servers outside of the Management VLAN. Routing to the Management VLAN is not allowed.
Z	10.38.10.1	10.15.10.1	B or C	

\*The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (*gateway interface address*). This is the IP address of the VLAN on which the request packet was received from the client. For more information, refer to RFC 2131 and RFC 3046.

## Operating Notes

- Routing is not allowed between the Management VLAN and other VLANs. Thus, a DHCP server must be available in the Management VLAN if there are clients in the Management VLAN that require a DHCP server.
- If the Management VLAN IP address configuration changes after **mgmt-vlan** has been configured as the remote ID suboption, the routing switch dynamically adjusts to the new IP addressing for all future DHCP requests.
- The Management VLAN and all other VLANs on the routing switch use the same MAC address.



## Release K.11.36 through K.11.39 Enhancements

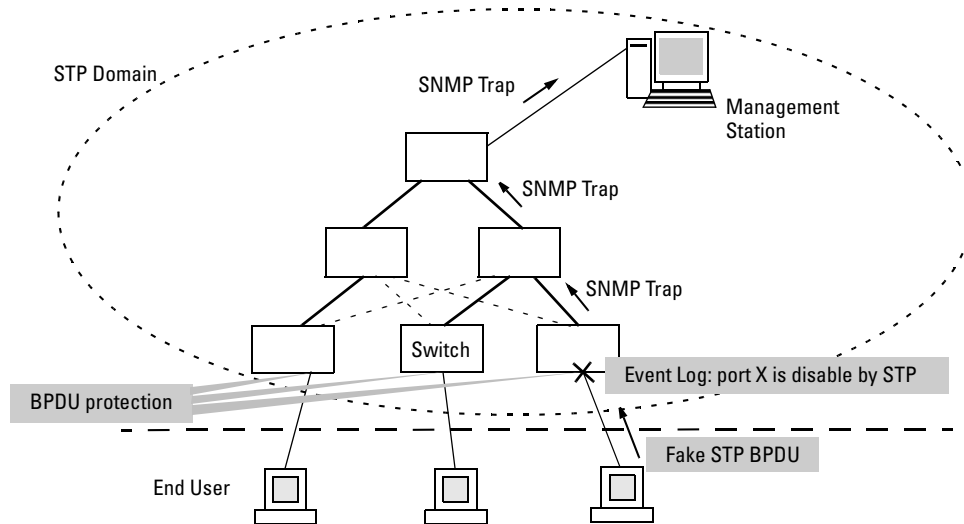
*No enhancements, software fixes only.*

## Release K.11.40 Enhancements

- **Enhancement (PR\_1000346164)** — 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.

### Spanning Tree BPDU Protection

The BPDU protection feature is a security enhancement to Spanning Tree Protocol (STP) operation. It can be used to protect the active STP topology by delimiting its legal boundaries, thereby preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection would be applied to edge ports connected to end user devices that do not run STP. If STP BPDU packets are received on a protected port, the feature will disable that port and alert the network manager via an SNMP trap as shown in Figure 9.



**Figure 9. Example of BPDU Protection Enabled at the Network Edge**

### Terminology

**BPDU** — Acronym for bridge protocol data unit. BPDUs are data messages that are exchanged between the switches within an extended LAN that use a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends

up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by placing redundant switch ports in a backup, or blocked, state.

**BPDU Filtering** — Spanning-tree configuration mode that prevents the switch from receiving and transmitting BPDU frames on a specific port.

**BPDU Protection** — Spanning-tree configuration mode which disables a port where BPDU frames are received.

**MSTP** — Multiple Spanning Tree Protocol, defined in IEEE 802.1s. Each MSTI (multiple spanning tree instance) on a physical port provides loop free connectivity for the group of VLANs associated with that instance. This means that traffic transported on different VLANs can be distributed for load-balancing among links between switches.

**RSTP** — Rapid Spanning Tree Protocol, defined in IEEE 802.1w and ratified in IEEE 802.1D-2004.

**Spanning-tree** — Generic term to refer to the many spanning-tree flavors: now deprecated STP, RSTP and VLAN-aware MSTP.

**STP** — Spanning Tree Protocol, part of the original IEEE 802.1D specification. The 2004 edition completely deprecates STP. Both RSTP and MSTP have fallback modes to handle STP.

**SNMP** — Simple Network Management Protocol, used to remotely manage network devices.

---

## Note

The switches covered in these Release Notes, use the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Under standard settings, your MSTP-configured switch interoperates effectively with both STP (IEEE 802.1D) and RSTP (IEEE 802.1w) spanning-tree devices. For more information, refer to the chapter entitled *Multiple Instance Spanning-Tree Operation* in the *Advanced Traffic Management Guide* for your switch.

---

## Configuring STP BPDU Protection

The following commands allow you to configure BPDU protection via the CLI.

**Syntax:** [no] spanning-tree <port-list> bpdu protection

*Enables/disables the BPDU protection feature on a port*

**Syntax:** [no] spanning-tree traps errant bpdu

*Enables/disables the sending of errant BPDU traps.*

For example, to configure BPDU protection on ports 1 to 10, enter:

```
ProCurve(config)# spanning-tree 1-10 bpdu protection
```

When BPDU protection is enabled, the following steps are set in process:

1. When an STP BPDU packet is received, STP treats it as an unauthorized transmission attempt and shuts down the port that the BPDU came in on.
2. An event message is logged and an SNMP notification trap is generated.
3. The port remains disabled until re-enabled manually by a network administrator.

---

### Caution

This command should only be used to guard edge ports that are not expected to participate in STP operations. Once BPDU protection is enabled, it will disable the port as soon as any BPDU packet is received on that interface.

---

### Viewing BPDU Protection Status

The **show spanning-tree** command has additional information on BPDU protection as shown below.

```

ProCurve# show spanning-tree 1-10

Multiple Spanning Tree (MST) Information

STP Enabled      : Yes
Force Version    : MSTP-operation
IST Mapped VLANs : 1-7
...
Protected Ports  : 3-7,9
Filtered Ports   : 10
  
```

Port	Type	Cost	Priority	State	Designated Bridge	Hello Time	PtP	Edge
1	100/1000T	200000	128	Forwarding	000883-024500	2	Yes	No
2	100/1000T	200000	128	Forwarding	000883-122740	2	Yes	No
3	100/1000T	200000	128	BpduError		2	Yes	Yes
4	100/1000T	Auto	128	Disabled				
5	100/1000T	200000	128	Forwarding		2	Yes	Yes
6	100/1000T	200000	128	Forwarding		2	Yes	Yes
7	100/1000T	200000	128	Forwarding		2	Yes	Yes
8	100/1000T	Auto	128	Disabled				
9	100/1000T	Auto	128	Disabled				
10	100/1000T	200000	128	Forwarding		2	Yes	Yes

*Note: In the original image, callouts indicate that ports 3-7,9 are protected, port 3 has an errant BPDU detected, and port 3 is the only port with BPDU protection enabled.*

**Figure 10. Example of BPDU Protection Additions to Show Spanning Tree Command**

## Release K.11.41 Enhancements

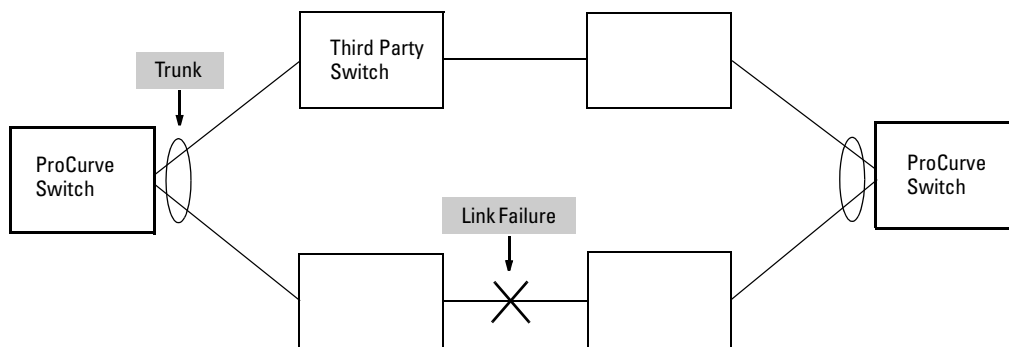
- **Enhancement (PR\_1000344652)** — Added support for Unidirectional Fiber Break Detection.

### Uni-Directional Link Detection (UDLD)

Uni-directional Link Detection (UDLD) monitors a link between two ProCurve switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks. Figure 11 shows an example.

**Scenario 1 (No UDLD):** Without UDLD, the switch ports remain enabled despite the link failure. Traffic continues to be load-balanced to the ports connected to the failed link.

**Scenario 2 (UDLD-enabled):** When UDLD is enabled, the feature blocks the ports connected to the failed link.



**Figure 11. UDLD Example**

In this example, each ProCurve switch load balances traffic across two ports in a trunk group. Without the UDLD feature, a link failure on a link that is not directly attached to one of the ProCurve switches remains undetected. As a result, each switch continues to send traffic on the ports connected to the failed link. When UDLD is enabled on the trunk ports on each ProCurve switch, the switches detect the failed link, block the ports connected to the failed link, and use the remaining ports in the trunk group to forward the traffic.

Similarly, UDLD is effective for monitoring fiber optic links that use two uni-direction fibers to transmit and receive packets. Without UDLD, if a fiber breaks in one direction, a fiber port may assume the link is still good (because the other direction is operating normally) and continue to send traffic on the connected ports. UDLD-enabled ports, however, will prevent traffic from being sent across a bad link by blocking the ports in the event that either the individual transmitter or receiver for that connection fails.

Ports enabled for UDLD exchange health-check packets once every five seconds (the link-keepalive interval). If a port does not receive a health-check packet from the port at the other end of the link within the keepalive interval, the port waits for four more intervals. If the port still does not receive a health-check packet after waiting for five intervals, the port concludes that the link has failed and blocks the UDLD-enabled port.

When a port is blocked by UDLD, the event is recorded in the switch log or via an SNMP trap (if configured); and other port blocking protocols, like spanning tree or meshing, will not use the bad link to load balance packets. The port will remain blocked until the link is unplugged, disabled, or fixed. The port can also be unblocked by disabling UDLD on the port.

## Configuration Considerations

- UDLD is configured on a per-port basis and must be enabled at both ends of the link. See the note below for a list of ProCurve switches that support UDLD.
- To configure UDLD on a trunk group, you must configure the feature on each port of the group individually. Configuring UDLD on a trunk group's primary port enables the feature on that port only.
- Dynamic trunking is not supported. If you want to configure a trunk group that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the trunk group, you can re-add the UDLD configuration.

---

### Note

UDLD interoperates with the following ProCurve switch series: 3400, 3500, 5300, 5400, 6200, 6400, and 9300. Consult the release notes and current manuals for required software versions.

---

## Configuring UDLD

The following commands allow you to configure UDLD via the CLI.

**Syntax:** [no] interface <port-list> link-keepalive

*Enables UDLD on a port or range of ports.*

*To disable the feature, enter the **no** form of the command.*

*Default: UDLD disabled*

**Syntax:** link-keepalive interval <interval>

*Determines the time interval to send UDLD control packets. The <interval> parameter specifies how often the ports send a UDLD packet. You can specify from 10 – 100, in 100 ms increments, where 10 is 1 second, 11 is 1.1 seconds, and so on.*

*Default: 50 (5 seconds)*

**Syntax:** link-keepalive retries <num>

*Determines the maximum number of retries to send UDLD control packets. The <num> parameter specifies the maximum number of times the port will try the health check. You can specify a value from 3 – 10.*

*Default: 5*

**Syntax:** [no] interface <port-list> link-keepalive vlan <vid>

*Assigns a VLAN ID to a UDLD-enabled port for sending of tagged UDLD control packets. Under default settings, untagged UDLD packets can still be transmitted and received on tagged only ports—however, a warning message will be logged.*

*The **no** form of the command disables UDLD on the specified port(s).*

*Default: UDLD packets are untagged; tagged only ports will transmit and receive untagged UDLD control packets*

**Enabling UDLD.** UDLD is enabled on a per port basis. For example, to enable UDLD on port a1, enter:

```
ProCurve(config)#interface a1 link-keepalive
```

To enable the feature on a trunk group, enter the appropriate port range. For example:

```
ProCurve(config)#interface a1-a4 link-keepalive
```

---

## Note

When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLD-configured ports in the same vlan. That is, UDLD control packets will “pass through” a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

---

**Changing the Keepalive Interval.** By default, ports enabled for UDLD send a link health-check packet once every 5 seconds. You can change the interval to a value from 10 – 100 deciseconds, where 10 is 1 second, 11 is 1.1 seconds, and so on. For example, to change the packet interval to seven seconds, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive interval 70
```

**Changing the Keepalive Retries.** By default, a port waits five seconds to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries four more times by sending up to four more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

You can change the maximum number of keepalive attempts to a value from 3 – 10. For example, to change the maximum number of attempts to 4, enter the following command at the global configuration level:

```
ProCurve(config)# link-keepalive retries 4
```

**Configuring UDLD for Tagged Ports.** The default implementation of UDLD sends the UDLD control packets untagged, even across tagged ports. If an untagged UDLD packet is received by a non-ProCurve switch, that switch may reject the packet. To avoid such an occurrence, you can configure ports to send out UDLD control packets that are tagged with a specified VLAN.

To enable ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter a command such as the following at the interface configuration level:

```
ProCurve(config)#interface 1 link-keepalive vlan 22
```

---

## Notes

- You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.
  - If a VLAN ID is not specified, then UDLD control packets are sent out of the port as untagged packets.
  - To re-assign a VLAN ID, re-enter the command with the new VLAN ID number. The new command will overwrite the previous command setting.
  - When configuring UDLD for tagged ports, you may receive a warning message if there are any inconsistencies with the port's VLAN configuration (see page 30 for potential problems).
-

## Viewing UDLD Information

The following show commands allow you to display UDLD configuration and status via the CLI.

**Syntax:** show link-keepalive

*Displays all the ports that are enabled for link-keepalive.*

**Syntax:** show link-keepalive statistics

*Displays detailed statistics for the UDLD-enabled ports on the switch.*

**Syntax:** clear link-keepalive statistics

*Clears UDLD statistics. This command clears the packets sent, packets received, and transitions counters in the show link-keepalive statistics display.*

**Displaying Summary UDLD Information.** To display summary information on all UDLD-enabled ports, enter the **show link-keepalive** command. For example:

```
ProCurve(config)# show link-keepalive

Total link-keepalive enabled ports: 4
Keepalive Retries: 3           Keepalive Interval: 1 sec

Port  Enabled  Physical  Keepalive  Adjacent  UDLD
      Status   Status   Status    Switch    VLAN
-----
1  Yes   up       up         00d9d-f9b700  200
2  Yes   up       up         01560-7b1600
3  Yes   down    off-line
4  Yes   up       failure
5  No    down    off-line
```

**Figure 12. Example of UDLD Information displayed using Show Link-Keepalive Command**



**Displaying Detailed UDLD Status Information.** To display detailed UDLD information for specific ports, enter the **show link-keepalive statistics** command. For example:

```
ProCurve(config)# show link-keepalive statistics
```

Port:	1	Neighbor MAC Addr:	0000a1-b1c1d1
Current State:	up	Neighbor Port:	5
Udld Packets Sent:	1000	State Transitions:	2
Udld Packets Received:	1000	Link-vlan:	1
Port Blocking:	no		
Port:	2	Neighbor MAC Addr:	000102-030405
Current State:	up	Neighbor Port:	6
Udld Packets Sent:	500	State Transitions:	3
Udld Packets Received:	450	Link-vlan:	200
Port Blocking:	no		
Port:	3	Neighbor MAC Addr:	n/a
Current State:	off line	Neighbor Port:	n/a
Udld Packets Sent:	0	State Transitions:	0
Udld Packets Received:	0	Link-vlan:	1
Port Blocking:	no		
Port:	4	Neighbor MAC Addr:	n/a
Current State:	failure	Neighbor Port:	n/a
Udld Packets Sent:	128	State Transitions:	8
Udld Packets Received:	50	Link-vlan:	1
Port Blocking:	yes		

Ports 1 and 2 are UDLD-enabled and show the number of health check packets sent and received on each port.

Port 4 is shown as blocked due to a link-keepalive failure

**Figure 13. Example of Detailed UDLD Information displayed using Show Link-Keepalive Statistics Command**

**Clearing UDLD Statistics.** To clear UDLD statistics, enter the following command:

```
ProCurve# clear link-keepalive statistics
```

This command clears the Packets sent, Packets received, and Transitions counters in the **show link keepalive statistics** display (see Figure 13 for an example).

## Configuration Warnings and Event Log Messages

**Warning Messages.** The following table shows the warning messages that may be issued and their possible causes, when UDLD is configured for tagged ports.

**Table 2. Warning Messages caused by configuring UDLD for Tagged Ports**

CLI Command Example	Warning Message	Possible Problem
link-keepalive 6	Possible configuration problem detected on port 6. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to enable UDLD on a port that is a tagged only port, but did not specify a configuration for tagged UDLD control packets. In this example, the switch will send and receive the UDLD control packets untagged despite issuing this warning.
link-keepalive 7 vlan 4	Possible configuration problem detected on port 7. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to configure tagged UDLD packets on a port that does not belong to the specified VLAN. In this example, if port 7 belongs to VLAN 1 and 22, but the user tries to configure UDLD on port 7 to send tagged packets in VLAN 4, the configuration will be accepted. The UDLD control packets will be sent tagged in VLAN 4, which may result in the port being blocked by UDLD if the user does not configure VLAN 4 on this port.
no vlan 22 tagged 20	Possible configuration problem detected on port 18. UDLD VLAN configuration does not match the port's VLAN configuration.	You have attempted to remove a VLAN on port that is configured for tagged UDLD packets on that VLAN. In this example, if port 18, 19, and 20 are transmitting and receiving tagged UDLD packets for Vlan 22, but the user tries to remove Vlan 22 on port 20, the configuration will be accepted. In this case, the UDLD packets will still be sent on Vlan 20, which may result in the port being blocked by UDLD if the users do not change the UDLD configuration on this port.

**Note:** If you are configuring the switch via SNMP with the same problematic VLAN configuration choices, the above warning messages will also be logged in the switch's event log.

**Event Log Messages.** The following table shows the event log messages that may be generated once UDLD has been enabled on a port.

**Table 3. UDLD Event Log Messages**

Message	Event
I 01/01/06 04:25:05 ports: port 4 is deactivated due to link failure.	A UDLD-enabled port has been blocked due to part of the link having failed.
I 01/01/06 06:00:43 ports: port 4 is up, link status is good.	A failed link has been repaired and the UDLD-enabled port is no longer blocked.

# Software Fixes in Release K.11.12 - K.11.3x

---

Software fixes are listed in chronological order, oldest to newest. To review the list of fixes included since the last general release that was published, go to [“Release K.11.34” on page 37](#).

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.11.12

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. Is this category name correct?
  - **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.
-

## Software Fixes in Release K.11.12 - K.11.3x

### Release K.11.13

- **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'
```

**Software Fixes in Release K.11.12 - K.11.3x**  
Release K.11.32

- **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.

## Software Fixes in Release K.11.12 - K.11.3x

### Release K.11.33

- **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.

**Software Fixes in Release K.11.12 - K.11.3x**  
Release K.11.36

- **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



© 2004 - 2006 Hewlett-Packard Development  
Company, LP. The information contained  
herein is subject to change without notice.

August 2006 -B  
Manual Part Number  
5991-4720