Release Notes
Version 07.8.03 Operating System
for the ProCurve 9304M, 9308M, and 9315M Routing Switches
with Redundant Management (M2, M4, EP, and T-Flow), April 2007

ProCurve Networking
HP Innovation

Software release 07.8.03 supersedes earlier software releases in the 07.*x* software branch. (For information about software branches and minimum release requirements for management module support, refer to "Software Branches" on page 3.)

The 07.8.03 release notes provide information on the following items:

• New hardware and software enhancements introduced with software release 07.8.03

• Known issues in software release 07.8.03

• Procedure for upgrading the software code on ProCurve 9304M, 9308M, and 9315M Routing Switches with M2, M4, or EP Redundant Management modules. See "Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.03" on page 7.

• General procedures, usage information, and helpful notes for operating and managing ProCurve routing switches

• Software fixes in release 07.8.03 and earlier releases

Descriptions of the enhancements in release 07.8.00 are included in the manuals for the 07.8.00 release. If you purchased a Redundant Management module with software version 07.8.00 or greater installed, the CD shipped with the module includes the 07.8.00 manuals.

If you need to access ProCurve product documentation, refer to "Downloading the Latest Software and Documentation" on page 3 for information on how to download PDF versions of the latest manuals.

NOTES:

Software Update Notice: Check the ProCurve Website frequently for free software updates for various ProCurve switch products. (Refer to "Downloading the Latest Software and Documentation" on page 3.)

Mini-GBIC ports: Hewlett-Packard offers and supports only mini-GBICs having a ProCurve label (with product number J4858B, J4859B, or J4860B) for use with the following modules:
- J4856A ProCurve 9300 Mini-GBIC Module
- J4857A ProCurve 9300 Mini-GBIC Redundant Management Module
- J4885A ProCurve 9300 EP 8-port Mini-GBIC Redundant Management Module
- J4894A ProCurve 9300 EP 16-port Mini-GBIC Module
- J8177B ProCurve Gigabit-copper mini-GBIC is supported for use in only the EP modules (J4885A and J4894A)
Use of other brands of mini-GBICs is not supported.

Flash Images: The flash image files for this software release differ depending on the type of management module you use. Refer to "Boot Code Requirements for ProCurve Software" on page 5.

SNMP: Starting with software release 05.2.16, the software does not have a default read-write SNMP community. If you use the default community name "private" as the password for web management access or for read-write access through a network management application, you need to use the CLI to add the read-write community string first.

Devices Without Redundant Management: For information about how to upgrade software on the ProCurve 9304M and ProCurve 9308M routing switches without redundant management, refer to the latest 6.6.*x* release notes. (See "Downloading the Latest Software and Documentation" on page 3.)

Publication Number

Applicable ProCurve 9300 (Current) Products

9304M Routing Switch	(J4139A)
9308M Routing Switch	(J4138A)
9315M Routing Switch	(J4874A)
EP 10/100-TX RJ-45 Module	(J4881B)
EP 10/100-TX Telco (RJ-21) Module	(J4889B)
EP Mini-GBIC RM Module	(J4885A)
EP Mini-GBIC Module.	(J4894A)
EP 100/1000-T Module.	(J4895A)
2-Port 10 Gigabit Ethernet Module	(J8174A)
EP 100Base-FX Module	(J8178A)
Gigabit-SX-LC Mini-GBIC	(J4858B)
Gigabit-LX-LC Mini-GBIC	(J4859B)
Gigabit-LH-LC Mini-GBIC	(J4860B)
1000Base-T Mini-GBIC.	(J8177B)
10 Gigabit Ethernet LR Optic	(J8173A)
10 Gigabit Ethernet SR Optic	(J8175A)
10 Gigabit Ethernet ER Optic	(J8176A)
9304M/9308M Redundant Power Supply. . . .	(J4147A)
9315M Redundant Power Supply.	(J4875A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. SuperSpan® is a trademark of Foundry Networks, Inc.

Disclaimer

Warranty

Contents

Terminology

The following table defines basic product terms used in ProCurve routing switch documentation.

Term	Definition
chassis device or chassis	A routing switch that accepts optional modules or power supplies. The ProCurve 9315M, ProCurve 9304M, and ProCurve 9308M routing switches are chassis devices.
EP (Enhanced Performance) and Standard	Routing switches can be EP or Standard devices, depending on whether the management module is an EP or Standard (M2 or M4) module. For a listing of ProCurve routing switches and their product numbers, see Table 4 on page 5.
routing switch or router	A Layer 3 device that switches and routes network traffic. The term *router* is sometimes used in this document in descriptions of a routing switch's Layer 3 routing protocol features.
switch	A Layer 2 device that switches network traffic.
`ProCurve 9300#`	An example Command Line Interface (CLI) prompt. Actual prompts show the product number for the routing switch, such as ProCurve 9300# .

Product Documentation for Software Release 07.8.03

Software release 07.8.03 includes all of the features in release 07.8.00a, plus several new features.

- For documentation on the features in 07.8.03 that were available in earlier releases, refer to the product documentation set identified for "Software Version 07.8.00a".

Table 1 describes the main topics covered in the ProCurve Routing Switch documentation set. If you do not already have a PDF version of the 07.8.00a documentation set, refer to "Downloading the Latest Software and Documentation" on page 3.

Table 1: Where To Get More Information

Title	Contents

Installation and Basic Configuration Guide	• Installation
	• Basic Features
	   • System (SNMP, SNTP, Syslog, broadcast and multicast throttling)
	   • Port configuration (speed, mode)
	   • Layer 2 (MAC table parameters, MAC filters, broadcast and multicast filters, port locks)
	   • Parameter table resizing
	   • Port monitoring
	• Link Aggregation
	• Spanning Tree Protocol
	• Virtual LANs
	• Layer 2 Multicast
	• Base Layer 3
	• Upgrading Software (**Important:** See also "Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.03" on page 7 in this document.)
	• Hardware Specifications and RFCs

Security Guide	• Security (passwords, user accounts, AAA, RADIUS, and TACACS/TACACS+) • Secure Shell (SSH) • Denial of Service Protection
Advanced Configuration and Management Guide	• QoS • ACLs • EP rate limiting • Standard rate limiting • IP • RIP • IP Multicast • OSPF • BGP4 • Network Address Translation • VRRP and VRRPE • IPX • AppleTalk
Command Line Interface Reference	Syntax information for all CLI commands.
Diagnostics Guide	• Diagnostic commands • Backplane debugging commands • Changing CAM partitions

Downloading the Latest Software and Documentation

You can download software version 07.8.03 and the latest routing switch product documentation from the ProCurve website as described below.

To Download a Software Version:

1. Go to the ProCurve website at **http://www.procurve.com**.

2. Click on **software** (in the sidebar).

3. Under "latest software", click on **switches**.

NOTE: If you are downloading software for the ProCurve 9304M or ProCurve 9308M, select the option that matches the type of management module(s) you are using in the routing switch—with redundant management or without redundant management.

To Download Product Documentation:

For the latest version of product documentation for ProCurve routing switches:

1. Go to the ProCurve website at **http://www.procurve.com**.

2. Click on **technical support**, then **manuals**.

3. Click on the name of the product for which you want manuals.

4. On the page listing the manuals, find the latest manuals under the heading "**For software version 7.8.00a**".

You will need the Adobe® Acrobat® Reader (version 4.0 or greater) to view or print the manuals.

Software Branches

Starting with software releases 06.6.28 and 07.1.10, ProCurve offers the software branches described in Table 2:

Table 2: Software Branches

Software Release	Includes:	Operates on:
06.6.28 and later 06.*x* releases	Bug fixes	ProCurve 9304M and ProCurve 9308M routing switches without redundant management (that is, with M1 modules)
		ProCurve 6308M-SX routing switch
		ProCurve 6208M-SX switch
07.1.10 and later 07.1.x releases	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M and ProCurve 9308M routing switches with redundant management (M2 modules)
07.5.04 release	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2 and M4 modules)
07.6.00 and 07.6.01b releases	Bug fixes, new features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 1-port 10GB modules
07.6.04 release 07.7.01 release	Bug fixes, new features, and enhancements to existing features, including support for the 2-port 10GB module	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules

Table 2: Software Branches

Software Release	Includes:	Operates on:
07.7.01b release	Bug fixes, 07.7.01 features and enhancements to existing features, and a new procedure for upgrading software code	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules
07.8.00a release	Bug fixes, new 07.8.00a hardware and software features, and enhancements to existing features	ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches with redundant management (M2, M4, EP, and T-Flow) and 2-port 10GB modules

Software Requirements for Management Modules

Table 3 shows the minimum software releases required to run redundant management modules.

Table 3: Minimum Software Requirements for Management Modules

Minimum Software Release Required	ProCurve 9300 Series Redundant Management Modules Supported
07.1.10 Supported only on ProCurve 9304M and 9308M	J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2) J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2) J4847A ProCurve 9300 Redundant Management Module (0-port, M2)
07.1.19 Supported only on ProCurve 9304M and 9308M	All of the redundant management modules supported for release 07.1.10 J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4)
07.5.04 Supported on ProCurve 9304M, 9308M, and 9315M	All of the redundant management modules supported for release 07.1.19 J4879A ProCurve 9300 T-Flow Redundant Management Module
07.6.00 Supported on ProCurve 9304M, 9308M, and 9315M	All of the redundant management modules supported for release 07.5.04 J4885A ProCurve 9300 EP Mini-GBIC Redundant Management Module

Software Supported on ProCurve Routing Switches

Table 4 shows the software releases supported on each ProCurve routing switch.

Table 4: Software Releases Supported on ProCurve Routing Switches

Routing Switch	Software Releases Supported			
	M2 or M4 Redundant Mgmt H2R05216.BIN H2R06605.BIN H2R06616.BIN H2R07110.BIN H2R07119.BIN H2R07122.BIN H2R07124.BIN	**M2 or M4 Redundant Mgmt** H2R07504.BIN[1] H2R07600.BIN[2] H2R07601.BIN H2R07604c.BIN H2R07701b.BIN H2R07800a.BIN H2R07801d.BIN H2R07803.BIN	**M1 Router Code only** HPR05216.BIN HPR06605.BIN HPR06616.BIN HPR06628.BIN HPR06633.BIN HPR06636.BIN	**M1 Switch Code only** HPS05216.BIN HPS06605.BIN HPS06616.BIN HPS06628.BIN HPS06633.BIN HPS06636.BIN
ProCurve 9315M (J4874A) Routing Switch with EP or Standard (M2 or M4) Redundant Management Module(s)	No	Yes	No	No
ProCurve 9304M (J4139A) and 9308M (J4138A) Routing Switches with EP or Standard (M2 or M4) Redundant Management Module(s)	Yes	Yes	No	No
ProCurve 9304M (J4139A) and 9308M (J4138A) Routing Switches without Redundant Management (with M1 Management Module)	No	No	Yes	No
ProCurve 6308M-SX (J4840A) Routing Switch	No	N/A	Yes	No
ProCurve 6208M-SX (J4841A) Switch	No	N/A	No	Yes

[1]First software release to support the ProCurve 9315M routing switch and the J4879A T-Flow module
[2]First software release to support the EP (Enhanced Performance) modules**.**

Boot Code Requirements for ProCurve Software

To run a software release on a ProCurve routing switch, you must use the minimum version of boot code for each software image described in Table 5.

Table 5: Boot Code Requirements

Routing Switch	Modules	Software Image	Minimum Boot Code Required
ProCurve 9304M ProCurve 9308M	With one of the following M1[1] modules (without Redundant Management): J4141A 10/100 J4144A Gigabit SX J4146A Gigabit 4LX/4SX	HPR06636.bin[2]	M1B07108.bin or greater recommended
ProCurve 9304M ProCurve 9308M ProCurve 9315M	With any one or two of the following Redundant Management: modules J4846A Gigabit SX[2] (M2) J4845A Gigabit LX[2] (M2) J4847A 0-Port[2] (M2) J4857A Mini-GBIC (M4) J4885A EP J4879A T-Flow	For M2, M4, and EP Redundant Management modules: - H2R07803.bin For T-Flow Redundant Management modules: - TSP07801d.bin	For M2, M4, and EP Redundant Management modules: - M2B07605.bin or greater For T-Flow Redundant Management modules: - M2B07605.bin (all MP images) - VSB07100.bin (VSM code)
—	10 Gigabit Ethernet (10GE) Modules **Note:** To upgrade FPGA code, refer to "Upgrading the FPGA on a 10 Gigabit Ethernet Module" on page 11.	The Field-Programmable Gate Arrays (FPGAs) in 10 Gigabit Ethernet Modules use the following software. J4891A FPGA: rxbmgr.bin – version 80, revision 6 rxpp.bin – version 81, revision 16 txaccum.bin – version 82, revision 6 txpp.bin – version 83, revision 13 ageram.bin – version 84, revision 4 J8174A FPGA: xpp.bin – version 88, revision 37 xtm.bin – version 89, revision 39 **Note**: To determine the FPGA versions running on a 10GE module, enter **show flash**. The version information is listed separately for each 10 Gigabit Ethernet module in the chassis.	10 Gigabit Ethernet modules do not use any of the boot images listed above.
ProCurve 6308M-SX	—	HPR06636.bin[2]	M1B07108.bin or greater recommended

Routing Switch	Modules	Software Image	Minimum Boot Code Required
ProCurve 6208M-SX	—	HPS06636.bin[2]	M1B07108.bin or greater recommended
[1]M1 management modules (without Redundant Management) have been discontinued. [2]Does not support Secure Shell (SSH) version 1.			

Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.03

This section explains how to upgrade the software used on M2, M4, and EP redundant management modules on a ProCurve 9304M, ProCurve 9308M, or ProCurve 9315M routing switch to release 07.8.03.

NOTE: As shown in Table 5, newer software versions require newer versions of boot code. Software versions use a five-digit number in the format: xx.x.xx; for example, 07.8.03. Boot code versions use a six-digit number in the format: xx.xx.xx; for example, 07.06.05.

Different procedures are used to upgrade an M2, M4, or EP management module, depending on the version of software running on the module:

• A software release earlier than 07.6.01b

• Software release 07.6.01b or greater

NOTE: M1 Management modules (discontinued) do not support software releases 07.x.xx, and are, therefore, not described in this section. The latest software release supported on an M1 management module is 06.6.36.

Restrictions

• Software release 07.8.03 requires boot code version 07.06.05 to support all hardware modules and decompress new software images.

  A new compression algorithm was introduced in software releases greater than 07.6.01b to generate software images. The new compression algorithm allows a software image to contain more features.

  Software release 07.6.01b was introduced as a special release that is used as an intermediate step when you upgrade to a later software release. After you install release 07.6.01b and reboot a routing switch, the switch is able to copy the latest software images to flash memory.

• On an M2, M4, or EP redundant management module, boot code is not automatically copied from the active to the standby management module. (However, software code is automatically copied to a standby management module.)

  To copy boot code from the active to a standby management module, you must enter the **sync boot** command.

• On a ProCurve 9315M, software release 07.5.04 is the earliest release supported. If a management module is running software earlier than release 07.5.04, you cannot upgrade the module in a 9315M chassis. Instead, you must upgrade it in a 9304M or 9308M chassis.

Upgrading to Software Release 07.8.03: Overview

To upgrade an M2, M4, or EP management module to release 07.8.03, you must follow these general steps:

A. Upgrade the boot code on the management module to version 07.06.05. If necessary, use the **sync boot** command to copy boot code from the active to a standby management module in the routing switch. Then reboot the routing switch to load boot code 07.06.05.

B. If the routing switch is running software EARLIER than release 07.6.01b, copy release 07.6.01b to flash memory. Then reboot the device to load the 07.6.01b software.

C. Copy release 07.8.03 to flash memory, and reboot the routing switch to load 07.8.03 software.

A. Upgrading Boot Code on a Management Module to Version 07.06.05

To upgrade the boot code on an M2, M4, or EP management module to version 07.06.05:

1. Store boot code version 07.06.05 (filename: M2B07605.bin) on a TFTP server that the routing switch can access.

2. Enter the following command at the privileged EXEC level of the CLI (for example: ProCurve 9300#) to copy the boot code from the TFTP server into the flash memory of the management module:

    copy tftp flash *<ip-addr> <image-file-name>* **boot**

3. Verify that the code has been successfully copied by entering the following command at any level of the CLI:

    show flash

    The boot code version is displayed on the line that begins with "Boot Image size". Ensure that boot code version 07.06.05 is displayed for the active management module.

4. If a standby (redundant) management module is installed in the routing switch, synchronize the boot code on the standby management module by entering the **sync boot** command.

    Verify that boot code 07.06.05 has been successfully copied on the standby management module by entering the **show flash** command.

5. Reboot the routing switch to load boot code 07.06.05.

B. Upgrading Software on a Management Module From a Release Earlier than 07.6.01b

To upgrade the software on an M2, M4, or EP management module from a release EARLIER than 07.6.01b to release 07.8.03:

1. Verify the version of boot code installed on the management module by entering the **show flash** command.

    The boot code version is displayed at the end of the line that begins with "Boot Image size". Ensure that boot code version 07.06.05 is displayed.

NOTE: The **show flash** command only displays the version of boot code installed on the device. It does not display the version of boot code running on the device.

If you rebooted the routing switch after installing boot code 07.06.05 (as described in "A. Upgrading Boot Code on a Management Module to Version 07.06.05"), the required boot code is running. If you are not sure, ProCurve recommends that you reboot the device now.

---

2. Store software release 07.6.01b (filename: H2R07601b.bin) on a TFTP server that the routing switch can access.

3. Upgrade the software on the management module to version 07.6.01b by entering the following command:

    copy tftp flash *<ip-address>* **H2R07601b.bin** [**primary | secondary**]

    Where:

    primary copies software to the primary (default) storage area in flash memory.

    secondary copies software to the secondary area in flash memory.

    If no redundant management module is installed, the message `TFTP to Flash Done` is displayed when the upgrade is complete.

    If a redundant management module is installed, the message `Sync Secondary code in flash...Done`

is displayed when the flash images are synchronized and the upgrade is complete.

4. Verify that the software has been successfully copied by entering the **show flash** command at any level of the CLI:

    • The software release in the primary flash is displayed at the end of the line that begins with "Compressed Pri Code Size".

    • The software release in the secondary flash is displayed at the end of the line that begins with "Compressed Sec Code Size".

    Ensure that software release 07.6.01b is stored in the primary or secondary flash area.

5. Reboot the routing switch to load software release 07.6.01b from the area of flash memory (primary or secondary) where you stored it.

6. Continue with "C. Upgrading Software on a Management Module From Release 07.6.01b or Greater" to upgrade the software to release 07.8.03.

C. Upgrading Software on a Management Module From Release 07.6.01b or Greater

To upgrade the software on an M2, M4, or EP management module from release 07.6.01b or greater to release 07.8.03:

1. Verify the version of boot code running on the management module by entering the **show flash** command.

    The boot code version is displayed at the end of the line that begins with "Boot Image size". Ensure that boot code version 07.06.05 is displayed.

    NOTE: The **show flash** command only displays the version of boot code installed on the device. It does not display the version of boot code running on the device.

    If you rebooted the routing switch after installing boot code 07.06.05 (as described in "A. Upgrading Boot Code on a Management Module to Version 07.06.05"), the required boot code is running. If you are not sure, ProCurve recommends that you reboot the device now.

    ---

2. Store software release 07.8.03 (filename: H2R07801d.bin) on a TFTP server that the routing switch can access.

3. Upgrade the software on the management module to version 07.8.03 by entering the following command:

    copy tftp flash <*ip-address*> **H2R07801d.bin** [**primary | secondary**]

    Where:

    primary copies software to the primary (default) storage area in flash memory.

    secondary copies software to the secondary storage area.

    If no redundant management module is installed, the message `TFTP to Flash Done` is displayed when the upgrade is complete.

    If a redundant management module is installed, the message `Sync Secondary code in flash...Done` is displayed when the flash images are synchronized and the upgrade is complete.

4. Verify that the software has been successfully copied by entering the **show flash** command at any level of the CLI:

    • The software release in the primary flash is displayed at the end of the line that begins with "Compressed Pri Code Size".

    • The software release in the secondary flash is displayed at the end of the line that begins with "Compressed Sec Code Size".

    Ensure that software release 07.8.03 is stored in the primary or secondary flash area.

5. Reboot the routing switch to load software release 07.8.03 from the area of flash memory (primary or secondary) where you stored it.

NOTE: When you reload the software after upgrading the software to release 07.8.03, the routing switch displays a message to say that the configuration has changed and prompts you to save the changes. This message is displayed even if you do not make any configuration changes because the software records its release number in the running-config file when the software is loaded onto the switch. Enter **Y** to reload without saving the change or save the change and reload.

Using SNMP to Upgrade Software on a Management Module

Third-party SNMP management applications such as HP OpenView can upgrade software on a routing switch.

NOTE: In software releases earlier than 07.5.04, the SNMP agent does not check for type validity with the SNMP version. In software release 07.5.04 and greater, the SNMP agent does not send a reply for a varbind, if the type of the varbind is not a known type for that version of SNMP. For example, MIB objects of type Counter64 cannot be retrieved using a v1 packet, as Counter64 is a v2c and v3 type.

Make sure you use the correct procedure for your device and processor type. For example, do not use the Management Processor procedure to upgrade the switching processors on a T-Flow module.

The syntax shown in this section assumes that you have installed HP OpenView in the "/usr" directory.

ProCurve recommends that you make a backup copy of the startup-config file before you upgrade the software. If you need to run an older release, you will need to use the backup copy of the startup-config file.

Upgrading a Management Processor using SNMP
Use the following procedure to upgrade:

•   An M2, M4, or EP module

•   Management processor on the T-Flow module

To upgrade software code on the Management Processor:

1. Configure a read-write community string on the ProCurve device, if one is not already configured. To configure a read-write community string, enter the following command from the global CONFIG level of the CLI:

    snmp-server community *<string>* **rw**

    where *<string>* is the community string and can be up to 32 characters long.

2. On the ProCurve device, enter the following command from the global CONFIG level of the CLI:

    no snmp-server pw-check

    This command disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an ProCurve device, by default the ProCurve device rejects the request.

3. From the command prompt in the UNIX shell, enter the following command:

    /usr/OV/bin/snmpset -c *<rw-community-string>* *<hp-ip-addr>* **1.3.6.1.4.1.1991.1.1.2.1.5.0 ipaddress** *<tftp-ip-addr>* **1.3.6.1.4.1.1991.1.1.2.1.6.0 octetstringascii** *<file-name>* **1.3.6.1.4.1.1991.1.1.2.1.7.0 integer** *<command-integer>*

    Where:
    <rw-community-string> is a read-write community string configured on the ProCurve device.
    <hp-ip-addr> is the ProCurve device's IP address.

<tftp-ip-addr> is the TFTP server's IP address.

<file-name> is the image file name.

<command-integer> is one of the following values:

20 – Downloads the software code into the device's primary flash area.

22 – Downloads the software code into the device's secondary flash area.

Upgrading the FPGA on a 10 Gigabit Ethernet Module

This section explains how to upgrade an FPGA (Field-Programmable Gate Array) on a 10 Gigabit Ethernet module. 10 Gigabit Ethernet modules do not have boot code separate from the management module. However, they do have FPGAs that require separate software.

NOTE: The J8174A 2-port 10 Gigabit Ethernet module with XENPAK optics uses a different FPGA file than the older J4891A 1-port 10 Gigabit Ethernet module. See Table 5 on page 6 for a list of the FPGA files supported on both the 1-port and 2-port 10 Gigabit Ethernet modules.

The J8174A 2-port 10 Gigabit Ethernet module with XENPAK optics can function in the same chassis with the older J4891A 1-port 10 Gigabit Ethernet module.

If an upgrade is required for any of the FPGA files, you must upgrade all the FPGA files.

To upgrade the FPGA on a 10 Gigabit Ethernet module:

1. Complete the upgrades of the boot code and software code, if required.

2. Enter the following command for the 10 Gigabit Ethernet module at the privileged EXEC level of the CLI:

    10gig copy tftp flash *<ip-addr> <filename>* [**module** *<slotnum>*]

    Where:

    tftp specifies the location of the FPGA file. The **tftp** parameter shows that the file is on a TFTP server.

    <ip-addr> specifies the IP address of the TFTP server, if you specify **tftp**.

    <filename> specifies the FPGA file name. The 2-port 10 Gigabit Ethernet module has only two FPGA files; xpp.bin and xtm.bin. For more information on the supported FPGA files, see Table 5 on page 6.

    module *<slotnum>* is an optional parameter that specifies the modules on which you want to install the upgrade. If you do not specify a slot number, the command upgrades the FPGA on all 10 Gigabit Ethernet modules in the chassis.

    Example

    ```
    ProCurve 9300# 10gig copy tftp flash 10.10.10.10 rxbmgr.bin
    ProCurve 9300# 10gig copy tftp flash 10.10.10.10 rxpp.bin
    ProCurve 9300# 10gig copy tftp flash 10.10.10.10 txaccum.bin
    ProCurve 9300# 10gig copy tftp flash 10.10.10.10 txpp.bin
    ProCurve 9300# 10gig copy tftp flash 10.10.10.10 ageram.bin
    ```

NOTE: You can store and copy the FPGA files using any valid filename. You are not required to store and copy the files using the names listed in "Boot Code Requirements for ProCurve Software" on page 5. The device uses information within the files to install them in the correct FPGAs, and the **show flash** command lists the FPGAs according to the names in "Boot Code Requirements for ProCurve Software" on page 5.

---

3. Reload the software by entering one of the following commands:

    •   **reload** (this command boots from the default boot source, which is the primary flash area by default)

    •   **boot system flash primary** | **secondary**

NOTE: The **show flash** command will list the new FPGA code versions but the new versions do not take effect until you reload the software.

Using Different Combinations of Management Modules

This section describes the different combinations of M1, M2, M4, EP, and T-Flow management modules supported on ProCurve 9304M, ProCurve 9308M, and ProCurve 9315M routing switches.

Table 6: Supported Management Module Combinations

Primary Management Module	Secondary Management Module	Notes
J4885A EP Mini-GBIC Redundant Management Module	Another EP Redundant Management Module	—
Any M2 or M4 Redundant Management Module (*Discontinued*)	Another M2 or M4 Redundant Management Module	When you use an M2 and M4 in the same switch, ProCurve recommends using the faster M4 as the primary redundant management module. If the M4 fails, the system will use the slower M2 module.
J4879A T-Flow Redundant Management Module (*Discontinued*)	Another J4879A T-Flow Redundant Management Module	—
Any M1 Management Module (*Discontinued*)	N/A	Supported only in the ProCurve 9304M and ProCurve 9308M routing switches. No redundant management options.

NOTE: The following types of management modules are *mutually exclusive*:
- M1 management modules
- M2 or M4 redundant management modules
- EP redundant management modules
- T-Flow redundant management modules
A ProCurve routing switch does not operate if two redundant management modules of different types are installed. Also, M1 management modules do not operate in a ProCurve 9315M routing switch.

Redundant management means that a device can operate with two management modules installed; one active (primary) and one standby (secondary). If the active management module becomes unavailable, the standby management module automatically takes over system operation.

Management modules with redundant management capabilities include the following M2, M4, EP, and T-Flow modules:

• J4885A ProCurve 9300 EP Mini-GBIC Redundant Management Module (8-port)

• J4879A ProCurve 9300 T-Flow Redundant Management Module (0-port — *discontinued*)

• J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, M4 — *discontinued*)

• J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, M2 — *discontinued*)

• J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, M2 — *discontinued*)

• J4847A ProCurve 9300 Redundant Management Module (0-port, M2 — *discontinued*)

If you are using a Redundant Management module, you can install either one or two such modules in the routing switch, as shown in Table 6. For more information, see "Using Redundant Management Modules" in the *Installation and Basic Configuration Guide* included on the *Documentation CD-ROM* shipped with your

---

management module, and also downloadable from the ProCurve website (see "To Download Product Documentation:" on page 3).

Non-Redundant Management on ProCurve 9304M and ProCurve 9308M Routing Switches

Management modules without Redundant Management are sometimes termed "M1" modules (for "Management 1"). These modules, now discontinued, operate only in the ProCurve 9304M and ProCurve 9308M routing switches. M1 modules include:

• J4141A ProCurve 9300 10/100 Management Module (16-port — *discontinued*)

• J4144A ProCurve 9300 Gigabit SX Management Module (8-port — *discontinued*)

• J4146A ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port — *discontinued*)

NOTE: M1 management modules do not operate in the ProCurve 9315M routing switch. Also, if you are using an M1 management module in a ProCurve 9304M or ProCurve 9308M, no other management module (non-redundant or redundant) can be installed in the routing switch.

Maximum Size of Startup-Config and Running-Config Files

Each ProCurve device has a maximum supported size for the running-config and the startup-config file. If you use TFTP to load additional information into a device's running-config or startup-config file, it is possible to exceed the maximum supported size. If this occurs, you will not be able to save the configuration changes.

Table 7 lists the maximum size of the running-config and the startup-config files on ProCurve devices.

Table 7: Maximum Sizes Supported for running-config and the startup-config Files

Device	Maximum Size of running-config and startup-config files
ProCurve 9315 using Management II or higher	256 kilobytes (KB)
ProCurve 9304M or ProCurve 9308M using Management II or higher	256 KB
ProCurve 9304M or ProCurve 9308M using Management I (*discontinued*)	128 KB
ProCurve 6308M-SX or ProCurve 6208M-SX (*discontinued*)	64 KB

NOTE: The maximum supported file size of each file is not the combined size of the running-config and startup-config files. The running-config and startup-config files can each be the size listed in Table 7.

To determine the size of an ProCurve device's running-config or startup-config file, copy the file to a TFTP server. Then use the directory services on the server to list the size of the copied file. To copy the running-config or startup-config file to a TFTP server, use one of the following commands.

• To copy the running-config to a TFTP server:

   copy running-config tftp *<ip-addr> <filename>*

• To copy the startup-config file to a TFTP server:

   copy startup-config tftp *<ip-addr> <filename>*

Removing a Module from an Active Device

Before you remove a module from a routing switch in operation, first disable the module. Disabling the module before removing it prevents a brief service interruption on other unmanaged modules. The brief interruption can be caused by the device re-initializing other modules when you remove an enabled module.

NOTE: This section does not apply to the active or standby Redundant Management modules. The **disable module** and **enable module** commands are not supported on management modules.

To disable a module, enter the following command at the Privileged EXEC level of the CLI:

disable module *<slot-num>*

Where *<slot-num>* specifies the slot number as follows:

- Slots in a 4-slot chassis are numbered 1 – 4, from top to bottom.

- Slots in an 8-slot chassis are numbered 1 – 8, from left to right.

- Slots in a 15-slot chassis are numbered 1 – 15, from left to right.

Example

```
ProCurve 9300# disable module 3
```

This command disables the module in slot 3.

NOTE: If you remove the module without first disabling it, the routing switch re-initializes the other modules in the device, causing a brief interruption in service after which the device resumes normal operation.

You do not have to enable a module after inserting it in the chassis. The module is automatically enabled when you insert the module into a running device or when you power on the device.

To replace a removed module with a different type of module, you must configure the slot for the new module. To configure a slot for a module, use the **module** command at the global CONFIG level of the CLI.

After disabling a module, if you decide not to remove the module, re-enable the module using the following command:

enable module *<slot-num>*

Example

The following command re-enables the module in slot 3:

```
ProCurve 9300# enable module 3
```

Configuring the ProCurve 9315M

When configuring a ProCurve 9315M 15-slot routing switch, take into account the guidelines and restrictions in this section.

Minimum Software Release Supported

The ProCurve 9315M requires software release 07.5.04 or greater.

NOTE: On a ProCurve 9315M, software release 07.5.04 is the earliest release supported. If a management module is running software earlier than release 07.5.04, you cannot upgrade the module in a 9315M chassis. Instead, you must upgrade it in a 9304M or 9308M chassis. For more information, see "Upgrading Software on an M2, M4, or EP Management Module to Release 07.8.03" on page 7.

Inserting or Removing an EP Module on a ProCurve 9315M

NOTE: This section applies only to a ProCurve 9315M (15-slot chassis) with EP modules.

Do not insert or remove EP modules in a ProCurve 9315M until the device has fully booted. Generally, booting takes around two minutes. You can determine whether the device has fully booted by looking at the management console. Once the device boots, a command prompt or login prompt is displayed.

After the device has booted, allow time for the device to fully complete the removal or insertion before removing or inserting another module. Generally, this takes about 30 seconds. After you remove or insert a module, the CLI displays a message confirming completion of the change. Wait for this message before removing or inserting another module.

Slot Locations for Redundant Management Modules

The 15 slots in the ProCurve 9315M are divided among 4 internal regions. Slots 1 – 4 belong to the same region; slots 5 – 8 belong to the same region; slots 9 – 12 belong to the same region, and slots 13 – 15 belong to the same region. If you are using redundant management modules, ProCurve recommends that you place both management modules in slots belonging to the same region. For example, if you place one management module in slot 5, ProCurve recommends that you place the other management module in slot 6, 7, or 8.

MAC Addresses

The ProCurve 9315M makes use of locally administered MAC addresses. If your site already uses locally administered MAC addresses of the vendor OUI, which is 00e052, there could be a MAC address conflict with one of the ports on the ProCurve device.

Server Trunk Groups

If you plan to configure ports on a module into a server trunk group, use the following guideline:

•   For a multi-slot trunk group (one configured on two forwarding modules), the modules must both be in the same set of slots (slots 1 – 7 or 9 – 15).

You do not need to follow this guideline for a switch trunk group.

NOTE: In software releases earlier than 07.6.00, the management module(s) and the module that had the server trunk group's ports were required to be in the same set of slots (slots 1 – 7 or 9 – 15). In software release 07.6.00 and later, there is no longer a restriction on the location of the management module relative to the module used for server trunking. However, it is still a requirement that the module that has the server trunk group's lead ports cannot reside in slot 8.

VLANs

In release 07.6.01b, you could configure only up to 2195 Layer 2 VLANs on the ProCurve 9315M routing switch. The **system-max vlan <num>** command allowed you to allocate a higher number of VLANs, but the software allowed you to actually create only 2195 of the allocated VLANs.

Starting with release 07.6.04, this restriction has been removed. You can create the full number of allocated Layer 2 VLANs on the 15-slot ProCurve 9315M routing switch, up to 4095.

Enhancements and Configuration Notes in 07.8.03

On ProCurve 9300M Series routing switches, no new software enhancements are supported in software release 07.8.03.

Software Fixes

The fixes for software bugs found on ProCurve 9300M Series routing switches in software releases 07.8.00h through 07.8.03 are described in the following table. Software fixes are listed by bug ID for the software release in which they were implemented.

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
	07.8.00h			
25991	In the display of InUcastPkts and OutUcastPkt 64-bit packet counters, the packet counts wrap after 32 bits.	Other		07.8.00
31045	The default route learned through OSPF is not displayed in the routing table if you enter the **clear ip route 0.0.0.0/0.0.0.0** command.	OSPF		07.8.00
32896	802.1w packets are not forwarded by the routing switch.	Spanning Tree		07.8.00
35710	If you enter the **no web management** command, access on port 80 is disabled while access on port 280 is allowed.	Web Management		07.8.00
35727	During a system reload, the following error message is displayed even when the number of Spanning Tree Protocol (STP) instances is reduced by using topology groups: `Error - failed to bind STP to vlan xxx`	Spanning Tree		07.8.00
3676	After you modify an access control list (ACL), protection against a reload is performed.	ACL		07.8.00
40829	A Border Gateway Protocol (BGP) reload is performed when the preceding NLRI entry is NULL.	BGP		07.8.00
41630	When private VLANs are configured, if you remove the lowest numbered port mapping in the primary VLAN, higher port mappings are disabled.	VLAN		07.8.00
44374	An error message is displayed when you configure multiple IP address on a group router interface.	Other		07.8.00
44949	ARP learning is performed much slower when Layer 3 bidirectional traffic is transmitted at a 100M rate.	Other		07.8.00
45104	A watchdog reset is caused when BGP passes out of the Direct Memory Access (DMA) range.	BGP		07.8.00
45198	Port 280 remains up if you enter the **no web-management http** command followed by the **no web-management hp-top-tools** command.	Web Management		07.8.00
45277	A system reload is performed following a link-list subroutine error.	Other		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
45318	After you disable and swap a module, the active management module crashes.	System		07.8.00
45319	When you enter the **ip rebind-acl all** command, the following message is logged: `Exceed max DMA 9 L4 cam resource, using flow based ACL instead`	ACL		07.8.00
45415	SSH may reload if a different client public-key is received for authentication.	SSH		07.8.00
45550	A 10 Gigabit Ethernet port is not displayed in **show fdp interface** command output.	CLI		07.8.00
46777	The globally configured value for the sFlow sampling rate is not applied to the secondary trunk links when you enter the **config-trunk-ind** command in the startup configuration.	sFlow		07.8.00
46924	The **sflow sample** command entered at the trunk level is not supported on a routing switch during a reload.	sFlow		07.8.00
47464	A variable is not initialized to zero. As a result, a large data chunk may be allocated, causing a system reload.	System		07.8.00
47599	If route-only mode is configured, forwarding stops when you exit from monitor mode.	System		07.8.00
47855	The OSPF timer displays the following message: `Warning Checksum bad in Link State Database error.`	OSPF		07.8.00
48115	The **debug ip igmp physical_port** command is not performed on ports 32 to 48 on an EP 48-Port 10/1000-TX RJ45 module.	IGMP		07.8.00
48132	When a trunk server is used, the first packet in a flow is sent twice.	System		07.8.00
48313	A Protocol Independent Multicast (PIM) reload is performed after detecting a virtual port (instead of a physical port) configured in the forwarding OIF.	PIM		07.8.00
48383	ACL-denied packets are not copied to a redirected interface.	ACL		07.8.00
48442	The BGP route dampening feature does not always dampen flapping routes after four flaps. Some routes are still dampened after two flaps.	BGP		07.8.00
48721	The routing switch reloads if an SSH client starts a session when SSH debugging is enabled.	SSH		07.8.00
48823	If you configure multiple addresses on an interface and reload the switch, RIPv2 advertises from only the lowest IP address.	RIPv2		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
48927	Port-based rate-limiting on outbound traffic may not function properly if a large output rate is configured.	Rate Limiting		07.8.00
	07.8.00i			
29031	In **show ip nat trans** command output, a maximum of 3000 Network Address Translation (NAT) sessions are displayed.	NAT		07.8.00
29530	A write error message for the VLAN table is displayed: `00d00h00m00s:E:Vlan table write error(00070064: 00801cac(40a10001).`	VLAN		07.8.00
33503	An interior Border Gateway Protocol (IBGP) route is selected over an OSPF route after exterior Border Gateway Protocol (EBGP) routes are withdrawn.	BGP		07.8.00
34609	A 10 Gigabit Ethernet link stays up when the peer on the other side of the link is disabled. No link-fault signal (LFS) is configured.	System		07.8.00
35968	A Web server is not functional and shows XSS vulnerability after running NeWT (Nessus Windows Technology).	System		07.8.00
40784	When a new RSA key is being generated, an error message is displayed: `RSA key can not be generated now, please try later.`	RSA		07.8.00
42047	An interface with advanced Quality of Service (QoS) policy configured stops responding to pings if a different interface is configured with an ACL on incoming traffic.	ACL		07.8.00
43253	In dot1x-enable configuration mode, the configured **mac-session-aging max-age** value is not displayed in the **show running config** command output.	CLI		07.8.00
43721	After you insert a 2-Port 10 Gigabit Ethernet module, entering the **dm delete mod_slot**<*number*> command causes a system reload.	CLI		07.8.00
44996	A PC cannot ping the Virtual Switch Redundancy Protocol (VSRP) virtual IP address (VIP) when it is connected to a port configured for **no include** and when the only other port that is up is on the management module.	VSRP		07.8.00
47159	When you configure the **mac-session-aging max-age** value, the **mac-session-aging no-aging permitted-mac-only** value needs to be unconfigured.	System		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
47395	If the primary link in an Link Aggregation Control Protocol (LACP) 802.3ad trunk goes down for more than 90 seconds and then comes back up, port flapping occurs.	LACP		07.8.00
47826	The system reloads when the ARP table contains more entries than the configured **maximum arp table** value.	System		07.8.00
47830	When an incorrect virtual router ID (**vrid**) value is configured, Virtual Router Redundancy Protocol (VRRP) corruption occurs.	VRRP		07.8.00
48064	In OSPF, a double link-list operation is faulty.	OSPF		07.8.00
48859	A BGP tag change is not updated in an OSPF route.	BGP		07.8.00
49028	When you enable Multicast forwarding, the routing switch runs out of valid forwarding identifiers (FIDs).	Multicast		07.8.00
49135	If an existing OSPF route with the same prefix as an EBGP route is removed, the EBGP route is not installed.	OSPF		07.8.00
49319	OSPF cannot add a route from the link-state (LS) database after you enter the **no ip forward route** command.	OSPF		07.8.00
49434	Continuous pings received on a virtual routing interface (VE) from a PC directly connected to the routing switch results in intermittent timeouts.	VE		07.8.00
49614	If you enter **logging host** followed by any single letter and then press the Tab key, the **udp-port** attribute is appended.	CLI		07.8.00
49695	OSPF sends an link-state (LS) update with an age time-out value of 3600 when the route map is changed.	OSPF		07.8.00
49839	When an ACL is applied to inbound traffic, routed packets for non-direct destinations are not sampled by sFlow.	ACL		07.8.00
49848	When you enter the **show support l4** command, the system reloads.	CLI		07.8.00
49914	When you reconfigure the router ID (by modifying the IP address of the loopback interface), OSPF stops advertising the default route.	OSPF		07.8.00
49934	A routing switch crashes continuously during boot-up when loading a customer configuration file.	System		07.8.00
50091	When you enter the **no interface** command, the fixed speed and duplex settings are not removed from an interface.	CLI		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
50092	When you enter the **no speed-duplex** command including speed and duplex attributes, the specified fixed speed and duplex settings are not removed.	CLI		07.8.00
50203	A routing switch does not flush a MAC address on the Metro Ring Protocol (MRP).	MRP		07.8.00
50347	Multicast forwarding is not supported with jumbo packets.	Multicast		07.8.00
50429	A system reload may occur after you disable multicast forwarding.	Multicast		07.8.00
50441	A watchdog reset is performed in the SSH code.	SSH		07.8.00
50592	Multicast forwarding of jumbo packets is not supported on a 10 Gigabit Ethernet module.	Multicast		07.8.00
50659	A system reload is performed during a Secure Copy (SCP) operation when a startup configuration is copied from Linux to a ProCurve 9300M Series routing switch.	System		07.8.00
51175	After you enter the **management-ip-disable** command on a VE interface and then enter the **sflow enable** command at the global configuration level, the routing switch fails to boot up properly.	VE		07.8.00
51394	When a Prune message is received, the routing switch stops sending multicast traffic to a client connected on the same port.	Multicast		07.8.00
51495	In a group VLAN, when a port is brought up or goes down, the console hangs and inbound and outbound traffic on the VE interface is dropped.	VLAN		07.8.00
	07.8.00j			
47730	After a reboot, the management module may reload with the following error message: `Active management module crashed.`	System		07.8.00
	07.8.00k			
35631	The routing switch crashes when running an IWL RMON test suite after you enter the **show run** command.	RMON		07.8.00
40149	When you enable monitoring, routing is stopped.	System		07.8.00
42129	The **debug ip arp** command output is displayed on the console when the destination value is set to **telnet**.	System		07.8.00
44892	The MTU in OSPF database description (DBD) packets is set to a non-zero value even when the **no rfc1583-compatibility** attribute is not configured.	OSPF		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
49218	LACP implementation causes a trunk instance to be recreated if a primary trunk port attached to a Cisco 6500 goes down or comes up.	LACP		07.8.00
49294	If you do not enter the **no rfc153-compatibility** command, type 3 summary link-state advertisements (LSAs) with maximum cost are sent. To activate the software fix, refer to the RFC 1583-type3-cost.	LSA		07.8.00
51320	In **show support l4** command output, IP Content Addressable Memory (CAM) information is listed for all slots but is truncated and not displayed after the first eighteen lines.	CLI		07.8.00
51505/ 51606	A memory leak in the web engine occurs because the http_receive_packet routine is not freed correctly when a client resets the connection.	System		07.8.00
51959	After you enter the **debug ip ospf flood** command, messages are displayed even if LSAs are sent to the adjacent router.	OSPF		07.8.00
52399	The **no ip follow acl** command does not work properly.	ACL		07.8.00
52419	During an SSH session, an SSH client is disconnected after the configured idle timer expires.	SSH		07.8.00
52617	The system reloads when you add a tagged port to a VLAN.	VLAN		07.8.00
	07.8.00m			
36085	A system reload may occur if the MRP ring interface is enabled.	MRP		07.8.00
42147	There is no command to disable the sending of SNMP traps for ACL log messages.	ACL		07.8.00
47254	On a tagged port, the incorrect ACL is applied to packets.	ACL		07.8.00
48029	The system may reload if MRP is configured.	MRP		07.8.00
50734	A log entry is only generated for permitted host; a log entry is not generated for a permitted network.	System		07.8.00
50939	The **no access-list** command leaks a denied packet although the ACL is not related to the interface.	ACL		07.8.00
51696	An SSHv2 key sometimes fails synchronize with a standby module after you enter the **write memory** command or after a boot-up.	SSH		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
52419	SSH disconnects an SSH client after the configured idle time expires even during an active SSH session.	SSH		07.8.00
53721	A reload is performed due to the lack of memory allocated to the "vlan_router_int_list" pointer.	VLAN		07.8.00
54207	A Data Access Exception reload in the cam_clear_dma_flags routine occurs.	System		07.8.00
54250	The **debug span all_802_1D_events vlan** command is not supported although it is displayed as a valid command option.	Spanning Tree		07.8.00
54251	The **debug 802.1w all_802_1W_events vlan** command does not send output to a console, Telnet, or SSH session.	Spanning Tree		07.8.00
54269	When Internet Group Management Protocol (IGMP) snooping is configured on a routing switch, it performs Layer 2 forwarding if there is no client session on the port.	IGMP		07.8.00
54375	A Data Access Exception crash occurs after you enter the **no untagged ethernet 21 ethernet 22 ethernet 23 ethernet 24** command.	System		07.8.00
54449	When a tagged port is assigned to multiple VE interfaces running OSPF, slow convergence is detected if the port goes down.	OSPF		07.8.00
54527	The **debug ip ssh** command supports **level 0** as a valid attribute.	SSH		07.8.00
54542	If you delete a group VLAN ID from the routing table, the route is not deleted.	VLAN		07.8.00
54655	The **show run** command output does not display the **gig-default neg-off** value configured on the secondary port when link aggregation is performed.	CLI		07.8.00
54752	After a route table is full, it sends a new link-state advertisement (LSA) only after five seconds.	System		07.8.00
54791	When a tagged port configured with two VLANS that use the same MAC address goes down, only one MAC address in one of the VLANs is aged out.	VLAN		07.8.00
55122	A Data Access Exception (l2_flooding_entry_refresh_impl) crash occurs when you enter the **trunk deploy** command.	Trunking		07.8.00
	07.8.00n			
44687	When creating a Reverse Path Forwarding (RPF) route, the switch software does not check for a valid port.	System		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
50323	802.1w is disabled if you configure a topology group (802.1w in the master VLAN) and more VLANs than the configured **system-max spanning-tree** value.	VLAN		07.8.00
51621	A GBIC that is installed in an SFP slot, which is configured for the Simple Network Time Protocol (SNTP) but has no cable attached, shows port flapping (up and down).	SNTP		07.8.00
52810	After you apply an ACL that filters a TCP range, connections using the upper TCP value appear to be switched instead of routed.	ACL		07.8.00
53925	A Data Access Exception reload occurs when there is a change in port membership in a VLAN. The routing switch does not check for a valid port.	VLAN		07.8.00
55204	ACL-based QoS is not applied to incoming frames that have a port-priority virtual MAC address as the destination address.	ACL		07.8.00
55379	A Data Access Exception reload occurs in NAT.	NAT		07.8.00
55657	A system reload was caused through input from the web management interface.	Web Management		07.8.00
56011	TACACS authentication is not supported in release 07.8.01 and greater.	TACACS		07.8.00
55559	The MAC address filter does not filter MAC address over a trunk server configuration.	System		07.8.00
56816	After you apply an ACL that contains a **qos-tos** mapping, the routing switch cannot ping a directly connected host.	ACL		07.8.00
	07.8.00o			
32021	The routing switch ignores the VSRP TTL value.	VSRP		07.8.00
32502	The following error message is displayed on the console: `Error: Inconsistent cam index free list! dma=57`	System		07.8.00
47724	In **show ip bgp nei adv** command output, all advertised routes are sometimes not displayed. (This is a display issue only.)	CLI		07.8.00
48614	A Data Access Exception crash occurred.	System		07.8.00
51302	When using a RADIUS server for 802.1x authentication for any authentication method, the missing RADIUS error message (#24) in access-challenge sets the RADIUS server in an unavailable state, causing authentication sessions to fail.	RADIUS		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
51933	A traffic flow is over-reporting the number of outbound bytes transmitted as compared with the number of interface counters recorded by SNMP.	SNMP		07.8.00
52074	When NAT and ACL are configured on the same interface, NAT does not translate packets after you modify the ACL configuration.	NAT		07.8.00
52269	ARP does not synchronize between the backplane and management plane on a routing switch.	System		07.8.00
52503	Unsuccessful logins via HTTPS lock up a Web management session.	Web Management		07.8.00
54854	A Program Exception crash occurred.	System		07.8.00
55268	The system crashed during a management session through the Web interface.	Web Management		07.8.00
55495	A BGP route cannot be deleted when a replacement route with the same local autonomous system (AS) is received.	BGP		07.8.00
55620	A Data Access Exception crash occurred.	System		07.8.00
56017	After a system reload, the mirroring configuration on an individual trunk is changed.	Port Mirroring		07.8.00
56317	A crash occurred in Multicast IGMP snooping.	Multicast		07.8.00
56400	The configuration of an ACL entry is supported after the **system-max** threshold configured with the **ip-filter-sys** command is reached.	ACL		07.8.00
56401	A Data Access Exception crash occurred.	System		07.8.00
56487	Multicast packets are transmitted on an MRP-blocked port.	Multicast		07.8.00
56946	An invalid ACL configuration is supported when a port already configured with an ACL-based rate limit allows an ACL binding to a VE interface to be configured on the port.	ACL		07.8.00
57172	The output port number in the PIM mcache is not correct.	PIM		07.8.00
57315	Two equal secure MAC addresses in different VLANs on the same port do not properly age out.	VLAN		07.8.00
57447	After system reload, a 10 Gigabit Ethernet module does not boot and displays the following error message because the configured module type does not match the hardware type: `The Module is "Marked Not Operational".`	System		07.8.00
57475	A Data Access Exception crash occurred.	System		07.8.00
57564	OSPF deletes summary routes when interfaces in area 0 come up.	OSPF		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
57594	The child route (more specific route) ages out from CAM before the parent route, resulting in blackholing of traffic.	System		07.8.00
57774	A Data Access Exception crash occurs when a trunk is created without entering the **trunk deploy** command and when the lead port is configured for 802.1w admin-pt2pt.	Spanning Tree		07.8.00
	07.8.00p			
57806	When you enter the **no port security** command, all interface-level configurations are deleted.	Port Security		07.8.00
58718	FDP packets sent on a 10 Gigabit tagged interface have incorrect VLANs. As a result, the FDP neighbors are not seen.	FDP		07.8.00
58852	Software images earlier than release 07.8.00p stored BGP community attributes that are only 256 bytes long.

Starting in release 07.8.00p, BGP community attributes with lengths up to 4096 bytes can be stored. | BGP | | 07.8.00 |
59014	Removing a VLAN group from a routing switch, on which a large number of VLANs are configured, causes a watchdog reset.	VLAN		07.8.00
59277	When you configure port mirroring and monitoring using the Web interface, an error message is displayed.	Web interface		07.8.00
59582	OSPF routes associated with an area are displayed in the routing table for 60 minutes after changing the area ID.	OSPF		07.8.00
60358	If the routing switch detects a BGP AS Path pointer to be invalid, the switch resets the pointer to Null.	BGP		07.8.00
60732	When the PIM multicast routing protocol is enabled for VLANs with tagged ports, the multicast packets cause loss of buffers on the second packet processor on the routing switch. Over time, this results in buffer depletion and causes a loss of connectivity.	PIM		07.8.00
61237	SSH corrupts data when the length of keys stored in EEPROM is invalid.	SSH		07.8.00
61547	A memory leak occurs over time if you use SSHv2 to connect to the routing switch.	SSH		07.8.00

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
	07.8.01			
14668	Although rare in occurrence, in some configurations with EBGP, IBGP, and OSPF routes, a routing switch may not always select the best route. For example, the device might install an IBGP route in the routing table, even though the IBGP route has a higher administrative distance than OSPF. This could happen if the switch previously selected an EBGP route as the best route. If this problem occurs, you must clear the routing table for a routing switch to select the best route.	BGP		07.8.01

25042	On the EP 8 Port Mini-GBIC Redundant Management module, if you configure a port name on the primary port of a trunk group, the switch generates an error message when it boots up. For example, the following configuration generates an error at boot-up:
	
	 `ProCurve(config)#interface ethernet 1/3`
	 `ProCurve(config-if-e1000-1/3)# port-name "testtrunk"`
	
	 However, if you configure a port name on all of the members of the trunk group, this error does not occur. For example:
	
	 `ProCurve(config)#trunk switch ethernet 1/3 to 1/4`
	 `ProCurve(config-trunk-1/3-1/4)#port-name "testtrunk"`
		CLI		07.8.01

25049, 25455	A port operating at **10-half** (10 Mbps at half duplex) drops 80% of broadcast traffic to other ports in the VLAN. This does not occur if the port is configured to operate at 100-full.	IP Stack		07.8.01
29177	On an 8 Port Mini-GBIC Redundant Management module, a **deny** clause in an outbound ACL does not filter traffic correctly if the destination IP address has been aggregated using the **IP net aggregate** command.	ACL		07.8.01
29465	On an EP 24 Port 100Base-FX module (J8178A**)**, MRP disables 10/100 copper MRP ring interfaces that are set to **100-full** speed and duplex mode. In addition, the **show interface brief** command output displays the interfaces as "blocked".	24-port 10/100 Module		07.8.01
29469	The **peer MAC address or IP** field for the VSRP standby displays "unknown" even if the VSRP standby knows the IP address of the master routing switch.	VSRP		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
29670	If you enable 802.1w (**spanning-tree** command) on a port-based VLAN before configuring the port as tagged or untagged, 802.1w fails to initialize. In addition, the **show 802-1w** command output shows that Rapid Spanning Tree Protocol (RSTP) is not configured. Note that if you define the port as tagged or untagged before enabling 802.1w, this problem does not occur.	RSTP - IEEE 802.1w		07.8.01
29755	The following display message contains a typo: `mtu config change detected, if NOT hot swaping, please save and reload!` The message should read "swapping" instead of "swaping".	Jumbo IP Packet Support		07.8.01
29759	If jumbo packets (**default-mtu 14336** command) are enabled globally on a routing switch and the switch has an empty module slot or slots, the ports on the empty module slots are configured with **mtu 1518** instead of **mtu 14336**. This occurs after you enter the **write memory** command.	Jumbo IP Packet Support		07.8.01
29846	If you hot swap a module by inserting it in a switch that is globally configured to support jumbo frames (**default-mtu 14336** command), the newly installed module should automatically inherit the jumbo configuration without requiring a system reload. However, this does not occur and jumbo frame support is not recognized on the newly installed module unless you reload the switch.	Jumbo IP Packet Support		07.8.01
30248	If a routing switch has numerous BGP entries, the page break (page display) does not work properly with the **show ip bgp peer** command. After entering the **show ip bgp peer** command, the command output scrolls continuously on the screen at first, then goes into page-by-page prompting mode.	BGP		07.8.01
30685	A routing switch deletes a route from the routing table even though the same entry exists in the OSPF LSA database.	OSPF		07.8.01
30702	The **no ip ospf cost** command does not apply the default value to the OSPF cost.	OSPF		07.8.01
30998	A routing switch prefers OSPF routes instead of EBGP routes after a system reload. If you clear BGP sessions or IP routes, this problem does not occur.	BGP		07.8.01
31047	If a routing switch has one BGP neighbor, the switch increases the ARP timer and eventually ages out the ARP entry for the peer. This error does not occur if there are two BGP neighbors. In this case, the ARP timers remain between 0 and 1.	BGP4+		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
31084	On an EP 8 Port Mini-GBIC Redundant Management module, a system reload occurs when a BGP packet with an invalid header length is received.	BGP4+		07.8.01
31157	A BGP routing switch fails to send notification after clearing a peer session.	BGP4+		07.8.01
31166	OSPF fails to delete a redistributed static route from the routing table even though the static route has been removed.	OSPF		07.8.01
31543	On an EP 8 Port Mini-GBIC Redundant Management module, a system reload may occur in an OSPF configuration when Remote Fault Notification (RFN) is enabled or disabled on a Gigabit Ethernet fiber port.	OSPF		07.8.01
31649	If the active EP 8 Port Mini-GBIC Redundant Management module fails over to the standby management module, the standby management module does not inherit the jumbo frame configuration from the active management module.	Jumbo IP Packet Support		07.8.01
31734	A routing switch reloads if its configuration includes Internet Group Management Protocol (IGMP) snooping and the hash table has a NULL value.	Other		07.8.01
31925	The copper mini-GBICs can operate in 1000 Mbps auto-negotiation mode only. You cannot configure them to operate in other modes. However, if you insert a mini-GBIC (M-TX) into an LX or SX port, the CLI allows you to configure the mini-GBIC to a speed other than 1000 Mbps.	CLI		07.8.01
32021	The routing switch does not decrease the time-to-live (TTL) value when a VSRP packet is transmitted.	VSRP		07.8.01
32192	VRRP-E link state flapping (fluctuating between up and down) causes a system reload. This occurs on a routing switch in which a non-T-Flow management module is installed.	Other		07.8.01
32230	On an 8 Port Mini-GBIC Redundant Management module, when a TCP-established clause is used in an ACL, the ACL incorrectly permits a series of synchronization (SYN) packets after it receives an acknowledgement (ACK) packet with a TTL of 0 (zero).	ACL		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
32360	On an EP 48-Port 10/1000-TX RJ45 module, the routing switch does not successfully remove some ACL remarks and line entries from the configuration. This occurs if you delete an ACL (for example, **no access-list 130**) and then later create an ACL with the same ACL number (for example, **access-list 130**). In this case, the system incorrectly inserts some of the remarks and entries from the previously deleted ACL.	ACL		07.8.01
32448	On an EP 8 Port Mini-GBIC Redundant Management module, PIM registration packets are sent with an incorrect source IP address.	PIM Sparse		07.8.01
32462	The **show debug** command output does not indicate that **debug span** or **debug 802.1w** commands are enabled on the routing switch.	CLI		07.8.01
32735	The routing switch corrupts the Autonomous System (AS) path if all three of the following conditions exist: • The routing switch is configured (using the **remove-private-as** command) to remove private AS numbers from update messages sent to a neighboring device. • The routing switch is configured (using the **as-set** parameter in the **aggregate-address** command) to aggregate AS path information for all the routes in the aggregate. • The first **as-set** segment has a private AS number.	BGP		07.8.01
32854	On an EP 24 Port 100Base-FX module (J8178A), a port's Full Duplex (FDX) LED does not illuminate even though the port has a fixed configuration of 100 full-duplex, and the port is connected to another routing switch that also has a fixed 100 full-duplex configuration.	MAC		07.8.01
32857	Connectivity issues may occur If MAC authentication is enabled on an M4 Redundant Management module.	MAC Authorization		07.8.01
32906	The system truncates the number of days timestamp for buffered Syslog messages. For example, if the actual system uptime is: 382 days 23 hours 17 minutes 26 seconds The software displays: 38 days 23 hours 17 minutes 26 seconds	Syslog		07.8.01

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
33511	If a port in a trunk group goes down then comes up again, the routing switch incorrectly load balances traffic across the ports in the trunk group. In normal operation, the switch re-balances the traffic so that all of the ports in the trunk group are properly utilized.	Other		07.8.01
33834	The software incorrectly attempts to free a transmission control block (TCB) that was already previously released. This causes the routing switch to display a warning message on the console.	TCP Stack		07.8.01
34493	If an ACL statement contains a range of values, the ACL **log** option, **dscp-marking**, and other ACL options may not be available in the CLI. For example, if you create an ACL entry that denies a TCP port range (for example, **access-list 1 deny tcp any any range 127 129**), some ACL configuration options that are normally available immediately following this command are not supported.	ACL		07.8.01
34507	In an MRP configuration with four devices in a ring and two rings in two different VLANs (for example, one ring in VLAN 10 and another ring in VLAN 30), an MRP ring fails to come up after a reboot.	MRP		07.8.01
	07.8.01a			
34160	When port mirror and monitoring is enabled, routing to the monitor port is stopped. (Duplicate of software fix 40149.)	Port Mirroring		07.8.01a
35710	The **no web management** command disables access on port 80, but access on port 280 is permitted.	Web Management		07.8.01a
37911	The **radius-server** <*hostname*> command re-orders parameters incorrectly.	RADIUS		07.8.01a
40619	The **crypto random gen** command is incomplete.	Encryption		07.8.01a
43703	Management access is granted to a routing switch without password verification.	Password		07.8.01a
	07.8.01b			
31957	When you enter the **write memory** command from a Telnet session, an error message is displayed: `w_mtu_buffer_type_config_write() to standby management jumbo e2 prom error`	CLI	07.8.00	07.8.01b
33508	CPU utilization increases when you enter the **show tech** command from an SSH session. As a result, VRRP failovers and some 802.1w transitions may occur.	VRRP-E, RSTP, 802.1w	07.6.06	07.8.01b

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
34609	A 10 Gigabit Ethernet link stays up when the egress side of the link is disabled. No link-fault signal (LFS) is configured.	10GE link	07.6.06	07.8.01b
35199	When forwarding sFlow packets, the routing switch crashes with a data access exception in the "sw_l2_get_outgoing_port_by_da_match" routine due to an invalid port number.	sFlow	07.6.06	07.8.01b
36363	After you add a VLAN group with a large number of configured VLANs or after a system reload, the following error message is displayed repeatedly: `WARN: Out of timer entry`	VLAN	07.8.01	07.8.01b
41689	The **show pid** value displayed in **show tech** command output causes a brief CPU utilization spike.	CPU	07.6.06	07.8.01b
43660	If you generate an SSH key by entering the **crypto key generate rsa** command, the routing switch crashes with a Data Access Exception in the "ssh-vsnprintf_internal" routine.	SSHv2	07.8.01	07.8.01b
43861	When you enable SSH, a routing switch may reload with a Program Exception in the "ssh_private_key_derive_public_key" routine.	SSH	07.8.00	07.8.01b
44042	A system reload may occur when you start an SSH session on a routing switch with a crash dump that includes "ssh_server_destroy".	SSH	07.8.00	07.8.01b
44364	The OSPF neighbor fails to come up because of an authentication key failure.	OSPF	07.6.06	07.8.01b
45071	After you delete the ACL statement, **access-list 100 deny ip 0.0.0.0 0.255.255.255 any**, error messages and locked CAM entries are displayed.	ACL, CAM	07.6.06	07.8.01b
45198	Port 280 stays open if you enter the following commands: **no web-management http** **no web-management hp-top-tools**	Web Management	07.8.01	07.8.01b
45319	When you enter the **ip rebinding acl all** command, the following error message is displayed in the log: `Exceed max DMA 9 L4 cam resource, using flow-based ACL instead.`	ACL	07.8.00	07.8.01b
46742	An ACL on a Web access-group router does not send a reset (RST) bit until after the TCP 3-way handshake completes.	ACL	07.8.01	07.8.01b
46777	When the **config-trunk-ind** value is configured, the global configuration of the sFlow sampling rate is not applied to secondary trunk links on system startup.	sFlow	07.6.06	07.8.01b

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
46924	After a system reload, the **sFlow sample** command at the trunk configuration level is no longer supported.	sFlow	07.6.06	07.8.01b
47724	The **show ip bgp nei adv** command output may not display all advertised routes. (This is a display issue only.)	CLI	07.8.00	07.8.01b
47855	The following error message is displayed continuously: `OSPF TIMER: Warning Checksum bad in Link State Database!`	OSPF	07.8.00	07.8.01b
48823	If you configure multiple addresses on an interface and reload the routing switch, RIPv2 advertises from only the lowest IP address.	RIPv2	07.8.00	07.8.01b
49395	On a switch trunk configured in a Layer 3 environment, if one of the trunk ports goes down and comes up again, outgoing traffic is not redistributed correctly on the member ports of the trunk group.	Trunk Group	07.6.06	07.8.01b
49672	If you configure a high numeric port number, the routing switch crashes during the "12ka-pre_process_port_event" routine.	System	07.8.01	07.8.01b
49695	OSPF send a link-state update with age=3600 when you modify the route map.	OSPF	07.6.06	07.8.01b
49914	When you reconfigure the router ID by changing the IP address assigned to the loopback interface, OSPF stops advertising the default route.	OSPF	07.8.01	07.8.01b
	07.8.01c			
22489	When the primary link-aggregation (802.3ad) LACP port is disconnected, the secondary port is in STP "disabled" state.	LACP	07.6.04	07.8.01c
33503	BGP routes are selected instead of an OSPF route after the BGP routes are withdrawn.	BGP, OSPF	07.8.00	07.8.01c
33598	A routing switch responds to SNMP get requests sent to destination IP address X.X.X. X. and MAC address FFFF.FFFF.FFFF.	SNMP	07.8.00	07.8.01c
35968	After running NeWT (Nessus Windows Technology) on a web server, the server is not functional and exhibits XSS Vulnerability.	Web Management	07.8.00	07.8.01c
40784	When you try to generate a new RSA key, the following error message is displayed: `RSA key cannot be generated now, please try later.`	RSA	07.6.05	07.8.01c

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
43721	After you install a 2-port 1-Gigabit Ethernet module, the **dm delete** *<slot-number>* command causes the routing switch to reload.	10GE link	07.6.05	07.8.01c
44138	CPU spikes occur for about 8 seconds when you add or remove ports with an outbound ACL on a VLAN.	CPU, ACL	07.6.06	07.8.01c
45057	The **show cpu** command displays 1% CPU utilization even though there are a very large number of packets transmitted through the CPU.	CPU	07.8.00	07.8.01c
47395	If the primary link in an LACP 802.3ad trunk goes down for more than 90 seconds, then comes back up, port flapping occurs.	LACP	07.8.00	07.8.01c
47584	When you add a MAC address in a trunk group, a data access exception may occur in the "ipc_r_read" routine.	Trunk Group	07.6.06	07.8.01c
47825	RIP redistribution does not update the OSPF forwarding address field when RIP is updated.	RIP, OSPF	07.6.06	07.8.01c
48859	BGP router A redistributes a tagged BGP route as an OSPF link-state advertisement (LSA) to router B running OSPF. Router B sends the OSPF LSA to router C. If BGP router A changes the tag, router C's OSPF database is updated, but not the OSPF route.	BGP, OSPF	07.6.06	07.8.01c
49240	If you disconnect a 10 Gigabit Ethernet port when a large number of modules are installed in a switch, packet loss may result in a 10GE link for three to five seconds.	10GE link	07.6.04	07.8.01c
49319	After you enter the **no ip forward route** command, OSPF cannot add a route from link-state (LS) database.	OSPF	07.6.00	07.8.01c
49731	The **trunk threshold** command does not take effect until you reload the routing switch. Also, when you remove a trunk and re-create a new trunk, the existing threshold value is applied to the newly created trunk.	Trunk Group	07.8.1	07.8.01c
49914	When you change the router ID (by modifying the IP address of loopback), OSPF stops advertising the default route. This problem is not detected when the the **default-information-originate** value is configured.	OSPF	07.8.00	07.8.01c
50203	The routing switch does not flash a MAC address when the MRP topology changes, even if the routing switch receives a topology change packet.	MRP	07.8.00	07.8.01c
50541	Network latency jumps from sub-millisecond to 300+ milliseconds when MAC filters are applied.	MAC filters	07.8.01	07.8.01c

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
50592	Multicast jumbo packets are not supported on the 10 Gigabit Ethernet module.	Multicast	all	07.8.01c
51482	The system reloads when you enter the **ip tftp source loopback 19899960** command in config mode. This is because the Valid Port Range value is not checked.	CLI	07.8.00	07.8.01c
	07.8.01d			
34400	sFlow does not detect an IP router ID or any physical address other than the default value. If sFlow is running when you modify the address, the new agent address is displayed in **show sflow** command output displays, but is not displayed in a trace. (The trace displays the default address.)	sFlow	07.8.00	07.8.01d
44260	Accessing HTTP may cause the system to reload at "ProcessCookie".	HTTP	07.8.01	07.8.01d
45319	When you enter the **ip rebind-acl all** command, the following error message is displayed: `Exceed max DMA 9 L4 cam resource, using flow based ACL instead.`	ACL	07.6.06	07.8.01d
47254	On a tagged port, an incorrect ACL value is applied to filter packets	ACL	07.8.00	07.8.01d
51175	A route fails to boot up properly when you configure sFlow globally by entering the **sflow enable** command and disable remote access to management functions by entering the **management-ip-disable** command on a VE interface.	sFlow	07.8.00	07.8.01d
51482	The system crashes at "ip_get_port_ip_address" after you enter the **ip tftp source loopback 19899960** command because the valid port range value is not checked.	CLI	07.8.00	07.8.01d
52419	SSH disconnects the SSH client after the configured idle time expires even during active CLI activity in an SSH session.	SSH	07.8.00	07.8.01d
52659	An IGMP query (for example, to 224.0.0.1) is sent on a blocking port. This happens only with different IGMP versions or when one port in the VLAN is a non-querier.	IGMP	07.8.01	07.8.01d
53881	SNMP OID "snAgentConfigModule" type displays the incorrect type for certain modules.	SNMP	07.8.00	07.8.01d
54208	The configuration of a TFTP or Telnet source interface is not supported.	CLI	07.8.01	07.8.01d
54250	The **debug span all_802_1D_events vlan** <*vlan-id*> command is not supported even though it is listed as a valid command option.	802.1d, CLI	07.8.00	07.8.01d

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
54251	The **debug 802.1w all_802_1W_events vlan** command does not send output to a console, Telnet, or SSH session.	802.1d, CLI	07.8.00	07.8.01d
54375	A Data Access Exception crash occurs when you enter the **no untagged ethernet 21 ethernet 22 ethernet 23 ethernet 24** command after you enter the **qos-tos trust dscp** command.	DSCP, QOS	07.8.00	07.8.01d
54527	The **debug ip ssh** command supports "level 0" as a valid value.	CLI, SSH	07.8.00	07.8.01d
54542	When deleting a group VLAN, if you enter the **no topology-group 1** or **no vlan-group 1** command to delete the virtual group router-interface, the route is not deleted from the routing table.	CLI	07.8.00	07.8.01d
54572	During an SSH connection attempt, the routing switch reloaded and displayed the message: `TRAP REASON - External Interrupt`	SSH	07.8.01	07.8.01d
55039	The OSPF age value in a link-state (LS) update or Data description packet may get corrupted. For example, the configured OSPF link-state advertisement (LSA) age is 19218 on two routing switches. This setting causes the switches to send LSA updates to each other every second. These LSAs cannot be aged out.	OSPF	07.8.01	07.8.01d
55290	The **de buffers** command causes display buffer leak. The "INFO: all 11 display buffers are busy" message is displayed in **show** command output.	CLI	07.8.00	07.8.01d
	07.8.02			
31281	When you unlock a locked Gigabit Ethernet port, the DMA chip may be initialized incorrectly, resulting in a Data Access Exception.	ACL		07.8.02
31779	On an EP 16-Port 10/1000-T module, reconfiguring the port speed to 1000-F or 1000-M prevents the routing switch from communicating with a server.	Auto-negotiation		07.8.02
32534	A routing switch rejects a 2-Port 10 Gigabit Ethernet module when the module is inserted after the switch reboots.	System		07.8.02
32541	The hot swapping of a a 2-Port 10 Gigabit Ethernet module or its Xenpak modules causes the DMA CAM entries to be deleted.	System		07.8.02
34508	When you enter the **no cpupro-action hardware-flooding enable** command, the switch takes an excessively long time to delete the CAM entries, causing a system reload.	Other		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
36440	The routing switch does not forward the MAC group address 01-80-C2-00-00-03 that was filtered by an IEEE 802.1D MAC bridge.	MAC Addressing		07.8.02
38066	When you add a single, multicast static MAC address to a port that is a member of a VLAN may result in packet loss.	MAC Addressing		07.8.02
38276	When you install a n EP 8 Port Mini-GBIC Redundant Management module in a routing switch, an error message indicating an unsupported DMA version is displayed.	System		07.8.02
38383	When you remove a 1-Port 10 Gigabit Ethernet module, the following error message is displayed: `Error - IP routing was configured on ports 14/48`	System		07.8.02
39902	A routing switch configured with rate limiting caused a system reload when an invalid port data entry was accessed.	Rate Limiting		07.8.02
40150	Adding a VLAN to a VLAN group creates an invalid VLAN number. For example, if you add VLAN 181 to VLAN Group 200, VLAN 181200 is added to the VLAN group.	VLAN		07.8.02
41967	Changes to the running configuration and startup configuration during an SSH session may report the IP address 0.0.0.0 in the trap and Syslog messages for the Telnet client.	SSH		07.8.02
43422	A next-hop movement message is displayed on the console when a station is moved and an ARP entry is deleted.	IP Stack		07.8.02
44042	On an EP 8 Port Mini-GBIC Redundant Management module, a system reload occurs when an SSH session is closed with inconsistent data.	SSH		07.8.02
44046	When you connect an Ethernet loopback cable to a port on an EP 48-Port 10/1000-TX RJ45 module, the port goes into forwarding state and interrupts the flow of traffic.	System		07.8.02
45575	A routing switch sends the configured **nas-port-type** value to the RADIUS server instead of to the NAS port for MAC authentication.	MAC Authentication		07.8.02
47163	On an EP 8 Port Mini-GBIC Redundant Management module, a start-of-packet counter is incorrectly displayed in the RX_NO_SOP_CNT counters.	System		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
47254	On an EP 8 Port Mini-GBIC Redundant Management module, when you configure sFlow and an ACL so that packets that were being forwarded by the CPU are filtered by the ACL, an incorrect VLAN ID is matched with the ACL.	ACL		07.8.02
47542	A system reload may occur when you enter a **show run** command during a Telnet session in which you bind ACLs to a port.	ACL/Telnet		07.8.02
47724	When you enter the **show ip bgp neighbor** <*x*> **adv** command, all advertised routes are not always displayed, although the routes are advertised correctly.	BGP		07.8.02
47725	On an EP 48-Port 10/1000-TX RJ45 module, binding and unbinding a single ACL-based rate limiting policy too many times causes memory corruption and results in a system reload.	Rate Limiting		07.8.02
48474	On an EP 8 Port Mini-GBIC Redundant Management module, when MRP2 is enabled and hellos are sent, a member ring blocked the port, instead of processing and forwarding hellos. Only the master ring should block the port.	MRP2		07.8.02
48521	On an EP 8 Port Mini-GBIC Redundant Management module, disabling a port on one MRP ring causes a port on a different ring in a blocking state to transit through the forwarding state.	MRP		07.8.02
48525	On an EP 8 Port Mini-GBIC Redundant Management module, you are not allowed to configure a static trunk if the ports in the trunk are members of an MRP2 ring.	MRP		07.8.02
48587	On an EP 8 Port Mini-GBIC Redundant Management module, when you change the primary and secondary port of a lower priority ring, ports on the higher priority ring are affected.	MRP		07.8.02
48660	On an EP 8 Port Mini-GBIC Redundant Management module, after an SSH key is generated, you are incorrectly prompted for a configuration change immediately after you enter the **write memory** command.	System		07.8.02
48747	When you reboot a routing switch with an EP 48-Port 10/1000-TX RJ45 module on which MRP is configured, a debug error message is displayed on neighbor devices, even after a neighbor has stabilized.	MRP		07.8.02
48753	On an EP 8 Port Mini-GBIC Redundant Management module, 10 seconds to 3 minutes are required for traffic to recover after a failed MRP link returns to a forwarding state.	MRP		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
49141	On an EP 8 Port Mini-GBIC Redundant Management module, you cannot reassign the same interfaces to an MRP ring.	MRP		07.8.02
49240	On a 2-Port 10 Gigabit Ethernet module, when you configure a jumbo MTU, packet loss may result when a link on a 10 Gigabit port is removed and re-inserted.	System		07.8.02
49461	On an EP 8 Port Mini-GBIC Redundant Management module, transient Ring Health packets (RHPs) are flushed during a topology change, causing high CPU usage.	MRP		07.8.02
50203	When MRP2 is configured, the routing switch does not flush out learned MAC addresses during topology changes, even if the device receives a Topology Change (TC) packet.	MRP		07.8.02
50541	On an EP 8 Port Mini-GBIC Redundant Management module on a POE switch, network latency jumps from sub-millisecond to 300+ milliseconds when MAC filters are applied.	System		07.8.02
50550	On an EP 8 Port Mini-GBIC Redundant Management module, when you remove the trunk port mirroring configuration, a trunk port continues to mirror outbound packets.	Port Mirroring		07.8.02
50685	Applying outbound rate limiting on a port several times may cause that port to toggle between a link up or link down state.	Rate Limiting		07.8.02
50735	On an EP 48-Port 10/1000-TX RJ45 module, the **show rate hardware** command output does not display the rate limiting that was configured on the port.	Rate Limiting		07.8.02
52810	On an EP 8 Port Mini-GBIC Redundant Management module, if an ACL with a DiffServ Control Point (DSCP) mapping is applied to a virtual routing interface, the ACL incorrectly matches the VLAN. This causes control packets, such as OSPF packets, to be discarded.	OSPF		07.8.02
53602	Uni-Directional Link Detection (UDLD) does not function properly or does not recover after a system reload.	UDLD		07.8.02
54375	Entering the **no untag** command with the **qos-tos trust DSCP** attribute may cause a stack overflow, which can result in a system reload.	System		07.8.02
54502	A routing switch that has 802.1w and many VLANs configured lost one link in a trunk group, causing a console lockup and topology change.	VLAN		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
54622	On an EP 8 Port Mini-GBIC Redundant Management module, a port in a virtual router interface on which an ACL is applied was changed, added, or removed and the ACL was re-applied. This behavior may result in a system reload.	ACL		07.8.02
54724	Installing an EP 48-Port 10/1000-TX RJ45 module in one slot can result in a packet loss on interfaces on a module in a different slot, on which outbound ACLs are configured. When an outbound ACL is configured, CAM entries are incorrectly aged out.	ACL		07.8.02
55354	On an EP 8 Port Mini-GBIC Redundant Management module, starting in release 07.8.02, BGP route selection is based on administrative cost rather than selecting a local route with a lower precedence over a BGP-advertised route from a peer device (as in earlier releases).	BGP		07.8.02
55572	On an EP 8 Port Mini-GBIC Redundant Management module, several topology changes caused the system to reload. This resulted in accessing an invalid VLAN index.	Spanning Tree		07.8.02
55689	When you enter the **ip access-group 0 in** command, all configured ACL entries are removed from physical and virtual routing interfaces.	ACL		07.8.02
55772	The routing switch performed a system reload triggered by the watchdog timer when a large number of CAM entries were aged out.	System		07.8.02
55773	A system reload occurs when an ACL is modified to re-assign traffic to a different priority queue.	ACL		07.8.02
56078	Valid values for Virtual Router Redundancy Protocol Extended (VRRPE) slow-start are 1-255, but the values 0 to 65535 can be entered.	VRRPE		07.8.02
56079	When ACL clauses are configured with the IP address 0.0.0.0 and with varying masks, the mask is not checked when you delete the clauses.	ACL		07.8.02
56080	ACLs configured with clauses containing DSCP mapping or priority mapping do not match the DSCP map or priority mapping field. As a result, if there are multiple clauses, packets are matched incorrectly.	ACL		07.8.02
56083	If you delete an EP 8 Port Mini-GBIC Redundant Management module and then re-insert the module back into the device after the **aggregated-vlan** command and the default maximum transmission unit (MTU) value are configured, the MTU changes back to the default value after the insertion.	System		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
56399	When rate limiting is enabled, the **ip rebind** [*acl-num*] command does not function correctly and some ACL definitions are changed.	ACL		07.8.02
56846	When an EP 8 Port Mini-GBIC Redundant Management module is installed, if you configure the **ip high-perf** command on a ProCurve module, the UDLD configuration does not recover after a system reload.	UDLD		07.8.02
56946	You can bind ACLs to a virtual routing interface even if one or more ports that belong to the virtual routing interface have an ACL-based rate limiting policy configured. If an ACL-based rate limit is configured on a port, no ACL can be configured on that port or any virtual routing interface that includes the port. The ACL-based rate limiting policy needs to be removed before you can apply the ACL to the port or any virtual routing interface that includes the port.	ACL		07.8.02
56961	The **no access-list** <*group-number*> command is not supported to remove all ACL entries from a group.	ACL		07.8.02
57006	On an EP 8 Port Mini-GBIC Redundant Management module, ACL statements that contain **tos-masking** and **tos-marking** entries are not checked for duplicated entries.	ACL		07.8.02
57387	When an EP 8 Port Mini-GBIC Redundant Management module is deleted from the routing switch, the CPU deletes the Layer 4 CAM entry from the module. The software then accesses the incorrect hardware device, causing a system reload.	System		07.8.02
57422	On an EP 8 Port Mini-GBIC Redundant Management module, an incorrect MAC address for an unsuccessful SSH session is displayed in **show log** command output.	SSH		07.8.02
57588	On the EP 8 Port Mini-GBIC Redundant Management module, enabling the CPU Protection feature causes OSPF to drop adjacencies.	OSPF		07.8.02
57678	The routing switch translates the destination of NAT packets incorrectly when the following conditions apply: • When an IP address in the NAT destination with static port mapping is used. • If more than one port mapping is configured for same IP address.	NAT		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
57758	On a network with OSPF Equal-Cost Multi-Path (ECMP) enabled, only the two next hops can be viewed when four next-hops exist.	OSPF		07.8.02
57806	When you enter the **no port security** command, all interface-level configurations are removed.	Port Security		07.8.02
57847	On an EP 24 Port 100Base-FX module (J8178A), when an outbound ACL is applied to a virtual routing interface, the ACL does not block traffic from interfaces on the same module.	ACL		07.8.02
58095	After you enter the **show version** command, the following error message is displayed to indicate an incorrect device ID for E2PROM: `Read from device id 6 failed.` Starting in release 07.8.02, the valid device ID is checked before it is accessed.	ACL		07.8.02
58101	Secure MAC addresses configured for a port are displayed in **show mac** command output, even though port security was disabled on the port.	Port Security		07.8.02
58397	When rate-limiting is configured, the correct value for port utilization is not displayed in **show stat** command output.	SNMP		07.8.02
58420	Data exception messages are displayed when you click the logout button on the Web management interface on a device that has the **allow-no-password** setting configured for web management.	Web Management		07.8.02
58428	On a 2-Port 10 Gigabit Ethernet module, a memory leak occurs on a 2-port trunk when the trunk is configured and then unconfigured.	Trunking		07.8.02
58567	On an EP 8 Port Mini-GBIC Redundant Management module, when you configure port security on a tagged port, MAC addresses are learned on an incorrect VLAN.	Port Security		07.8.02
58718	On a 1-Port 10 Gigabit Ethernet module, the HP Discovery Protocol (FDP) cannot transmit traffic on an outbound 10 Gigabit tagged port.	FDP		07.8.02
58732	When a routing switch forwards a packet via the CPU, the port mask may be sometimes accessed incorrectly, resulting in a system reload.	IP Stack		07.8.02
58831	A packet is not flooded in a port VLAN when its destination IP address does not match any of the configured IP subnet VLANs.	VLAN		07.8.02
58852	Earlier software images stored BGP community attributes that can be up to 256 bytes long. Starting in release 07.8.02, BGP community attributes with lengths up to 4096 bytes are supported.	BGP		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
58868	You cannot disable the HP Discovery Protocol (FDP) or Cisco Discovery Protocol (CDP) on a secondary trunk port if you have entered the **no fdp enable** or **no cdp enable** command on a primary trunk port.	FDP and CDP		07.8.02
58909	A route learned via RIPv1 disappears if a port in the RIPv1 route has a statically added route.	RIPv1		07.8.02
59169	A routing switch does not properly flush the PIM mcache after an MRP master goes down. As a result, packets are forwarded to the interface on which they are dropped.	PIM		07.8.02
59519	When OSPF is configured on fixed full-duplex (10-Full or 100-Full) interfaces, the external route summarization fails when the configuration is loaded during system boot.	OSPF		07.8.02
59698	On an EP 8 Port Mini-GBIC Redundant Management module, the incorrect MAC address that is used in an unsuccessful SSH session is displayed in **show log** command output.	SSH		07.8.02
59749	When you enter the OSPF **area range advertise** command, a specific summary route is not advertised if a route first matches another **area range** command that has a less specific route.	ACL		07.8.02
59925	If CAM entries are inconsistent on a routing switch, a system reload can occur when you enter the **no vlan** command.	VLAN		07.8.02
60057	On an EP 8 Port Mini-GBIC Redundant Management module, OSPF external routes are not matched correctly with the subnet mask. As a result, these routes are incorrectly deleted.	Other		07.8.02
60249	When a new BGP route is being processed in a routing switch, the BGP route is missing from the Patricia Tree in some error situations. This may cause a system reload when the route is added to the BGP routing table.	BGP		07.8.02
60277	When a large number of CAM entries are being processed on an EP 8 Port Mini-GBIC Redundant Management module, a system reload may occur.	System		07.8.02
60330	The routing switch either performs a software reload or locks the console for 40 seconds when you add or remove ports from a VLAN.	ACL		07.8.02
60358	On an EP 16-Port 10/1000-T module, if the routing switch detects a BGP AS path pointer to be invalid, the switch resets the pointer to Null.	BGP		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
60395	Although a device has a route in the OSPF routing table, the device may add an IP cache entry that is flagged as "DI", meaning the packet destination is unknown. This problem occurs when you disable IP load-sharing.	OSPF		07.8.02
60400	If you reconfigure OSPF by modifying hello and dead intervals and then reload the routing switch, the link between OSPF neighbors can go down during a two-way handshake.	ACL		07.8.02
60732	When PIM multicast routing protocol is enabled for VLANs with tagged ports, the multicast packets cause loss of buffers on the second packet processor on ProCurve 9300M Series modules. Over time, this results in buffer depletion, causing loss of connectivity.	PIM		07.8.02
61581	Configuring OSPF point-to-point results in loss of buffers, which then results in buffer depletion. This affects the IP connectivity to the device.	ACL		07.8.02
61653	On an EP 16-Port 10/1000-T module which has a large number of port VLANs and a large number of entries in the ARP table configured, and has multiple outbound mirror ports enabled, the switch intermittently loses connectivity to the directly connected hosts and displays pending entries in the ARP table.	IP Stack		07.8.02
62312	A system reload occurs when a routing switch accesses an internal port data entry that has been freed.	IP Stack		07.8.02
	07.8.02b			
43300	When a variable related to the ACL processing is not correctly freed after use, a system reload may occur.	System		
44945	When static routes are configured, when you configure the cost or administrative distance of a static route, the route table is not updated.	IP Routing		07.8.02
52397	If sFlow is configured, the **no sflow agentip** command is not supported.	SFlow		07.8.02
59070	If you configure Policy Based Routing (PBR) and a router map has two instances with a different next-hop, the next hop for the second instance is never selected.	PBR		07.8.02
59277	When you configure port mirroring and monitoring on a routing switch using the Web interface, an error message is displayed.	Web Management		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
59468	If OSPF is configured, the OSPF configuration is not displayed in **show ip ospf config** command output until the configuration is saved and the switch is rebooted.	OSPF		07.8.02
59698	If SSH is configured, a system reload sometimes occurs due to insufficient stack space.	SSH		07.8.02
59925	The incorrect deletion of CAM entries may cause a routing switch to reload.	System		07.8.02
60117	If you enable the VSRP and CPU Protection features, when a link flaps, the VSRP forwarding state is not correctly set. As a result, the CAM for the master is not updated correctly, resulting in a Layer 2 packet loop.	VSRP		07.8.02
60227	When you configure an incorrect speed on a virtual interface, the valid physical port is not checked, resulting in a system reload.	System		07.8.02
60249	If BGP4 is configured and a BGP update is received for an existing prefix, in some cases the BGP route does not include the BGP tree node. This can cause the system to reload.	BGP4		07.8.02
60330	If a large number of VLANs are configured, when you remove or add a tagged port from a VLAN, high CPU utilization occurs.	System		07.8.02
60396	When a static MAC address is configured on multiple ports, the address is not displayed on all ports in **show mac ethernet** *<slot/port>* command output.	System		07.8.02
60401	When you configure a username password using all numeric characters, it is necessary to re-enter the **service password-encryption** command after you add each password. To create an MD5 password, use one of the following commands: • **username** *<username>* **create-password** *<password-string>* • **username** *<username>* **privilege** *<number>* **create-password** *<password-string>* Both commands generate the same syntax. • **username** *<username>* **password** *<number>* *<encryptedpassword-string>* Or • **username** *<username>* **privilege** *<number>* **password** *<number>* *<encrypted-password-string>*	System		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
60916	Traffic is not evenly balanced on the members of a trunk after you enter the **ip net-aggregate** command and configure multislot switch trunks.	IP Routing		07.8.02
60979	If BGP4 is configured and you enter the **remove private-as** command on a neighboring device so that the routing switch receives an update from a private AS for which it is configured, the BGP update is sent out with the AS numbers stripped out. If the AS numbers are private only, the AS path attribute will be empty. This causes the neighbor to reset the BGP peering.	BGP4		07.8.02
61211	If you configure a Gigabit fiber port using the **gigabit auto rfn** command, and the port is physically connected and then disconnected to a Cisco router, the port does not always come up.	System		07.8.02
61383	When an ACL is configured, the **ip access-group in ethernet** <*slot*/*port*> command does not correctly apply the ACL to only the specified port.	ACL		07.8.02
61434	When the STP boundary is changed dynamically, the new value is not displayed in **show superspan** command output. The workaround is to remove the value by entering the **no stp-boundary** <*value*> command before configuring a new value.	Spanning Tree		07.8.02
61501	If a spanning tree is configured and a port is tagged for the default VLAN, the spanning tree state on the default VLAN is not updated. As a result, the outbound traffic is forwarded on the blocked port causing a loop.	Spanning Tree		07.8.02
62071	If OSPF is configured and there are multiple neighbors on an interface, the OSPF routes are not learned from the interface unless all the neighbors are established.	OSPF		07.8.02
62367	If VSRP is configured, port indication on a change in the port state incorrectly programs forwarding information. As a result, port 1/1 does not send outbound traffic.	VSRP		07.8.02
62826	If UDLD is configured, an incorrect error message may be displayed: `Link-keepalive and trunk-threshold cannot be enabled.`	UDLD		07.8.02
62893	If the primary port of the trunk goes down due to a port security violation, the other members of the trunk are displayed incorrectly as "state: Down".	Port Security		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
62894	If the ports within a trunk are disabled due to a port security violation, the **disable** command is not displayed as part of the **show running-config** command output.	Port Security		07.8.02
63138	On an interface on which both sFlow and an inbound ACL are configured, in the display of sFlow traffic statistics, the number of packets received is lower than the actual number received.	sFlow		07.8.02
63138	The following debug message may incorrectly be displayed on the console: `Warning: Shadow CAM data Entry`	System		07.8.02
63525	When you configure IP multicast snooping on a routing switch, the switch can perform a system reload due to corruption of multicast snooping database entries.	IP Multicast Snooping		07.8.02
63525	When you enable IGMP snooping by entering the **ip multicast active** and **ip multicast filter** commands, a routing switch performs a system reload.	PIM Dense		07.8.02
64104	When a routing switch is configured with output ACLs, sFlow, and multi-slot trunks, the management module may show high CPU usage.	ACL		07.8.02
64169	If sFlow is configured and a broadcast or multicast packet is sampled for exporting, it may cause the management module to reset.	sFlow		07.8.02
	07.8.02c			
61801	If BGP4 is configured, when an aggregate route is advertised using a route map that contains the **as-set** and **summary-only** attributes, the advertised route does not inherit the AS number from the component routes.	BGP4		07.8.02
62627	If IP routing is configured, the addition of a static route via an SNMP set request does not install an IP route in the routing table.	SNMP		07.8.02
63329	If trunk and port security are configured and you have not entered the **config-trunk-ind** command to enable or monitor individual trunk ports, a violation on a secondary member disables only one of the members.	Port Security		07.8.02
63429	When a configuration file containing an ACL is downloaded via TFTP on a routing switch, the system may reload.	ACL		07.8.02
63629	If OSPF is configured, the **show ip ospf routes** command displays the last route twice.	OSPF		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
63975	A routing switch in which ProCurve 9300M Series modules are installed can sometimes reload due to incorrect logic for lockup detection.	System		07.8.02
	07.8.02d			
62862	If RIP routes are configured and redistributed to OSPF, when an interface that is learning RIP routes is temporarily disabled, the RIP routes that are redistributed to OSPF are removed correctly, but are not restored when the interface comes back up.	RIP		07.8.02
63310	If IP multicast is configured, IP control packets in the range 224.0.0.1 to 224.0.0.255 may be incorrectly discarded.	System		07.8.02
64951	If SSH is configured and you reload the switch, the configuration may sometimes reset due to invalid length of SSH keys.	SSH		07.8.02
65342	The lockup detection mechanism is sometimes applied incorrectly, resulting in a system reload.	System		07.8.02
65869	If the SuperSpan feature is globally enabled and you remove the SuperSpan configuration at the VLAN level, it is also removed at the global configuration level.	SuperSpan		07.8.02
65957	During the reload of a routing switch on which Policy Based Routing (PBR) is configured, the time required to resolve next-hop ARP entries and program the CAM is significantly longer, resulting in a delay when accessing the console.	PBR		07.8.02
	07.8.02f			
34083	If BGP is configured, the switch takes a long time to transmit the complete BGP route table to a neighboring peer.	BGP		07.8.02
54245	When you delete CAM entries with MAC addresses, a system reload may occur.	System		07.8.02
54250	If the Spanning Tree Protocol (STP) is configured, the **debug span all_802_1d_events vlan** <*vlan_id*> command is not parsed correctly as a valid command.	Spanning Tree		07.8.02
54251	If the Rapid Spanning Tree Protocol (RSTP) is configured, the **debug 802.1w all_802_1d_events vlan** <*vlan_id*> command does not send debug events to a console, Telnet, or SSH session.	RSTP		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
59279	If supernet routes are used and the IP Routing feature is configured, the CAM entry of a child route sometimes gets aged out, leaving the CAM entry of parent route programmed. This can cause misforwarding of traffic.	IP Routing		07.8.02
59502	A system reload is sometimes performed if the IP Routing feature configured when the system runs out of IP cache entries and frees an existing entry.	IP Routing		07.8.02
60525	A system reload is sometimes performed if the IP Routing feature configured if the outbound interface used to forward IP traffic is invalid.	IP Routing		07.8.02
64091	Entering the **show flash** command over a Telnet connection to a routing switch may cause a system reload.	System		07.8.02
64230	If the Multicast Source Discovery Protocol (MSDP) and BGP are configured, the TCP pool can sometimes be corrupted by MSDP and cause a system reload.	IP Routing		07.8.02
64339	If OSPF is configured, when an Equal-Cost Multi-Path (ECMP) route is received with an overlapping route in the route table, the ECMP route is not added to the IP route table.	IP Routing		07.8.02
64605	If a tag type is configured and you delete the tag type using the **no tag-type** command, the **tag-type** value is not checked.	System		07.8.02
64621	If the authentication, authorization, and accounting (AAA) feature is configured using a RADIUS server as the default, you must press "CR" key twice after you enter a password to gain access to the switch.	AAA		07.8.02
64910	If VSRP is configured, the number of active ports does not include the lowest numbered port. You must disable the port and then re-enable it in order for the correct number of active VSRP ports to be used. This action may result in a loss of connectivity.	VSRP		07.8.02
64961	A system reload may occur when packets that match a Layer 3 CAM entry are sent to the processor.	System		07.8.02
65231	On an EP 16-Port 10/1000-T module, a Gigabit interface does not exchange 802.3x flow control capability in auto-negotiation mode with a link partner.	System		07.8.02
65286	When you start an outbound Telnet session on a routing switch, the switch incorrectly uses the "CR" character instead of the key sequence "CR NULL".	System		07.8.02

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
65342	When detecting a port lockup condition on a routing switch, a system reload may occur.	System		07.8.02
65418	If you configure the Port Security feature with an ACL that permits Internet Control Message Protocol (ICMP) traffic, ICMP packets may sometimes be dropped.	System		07.8.02
65740	If IGMP snooping is configured, the switch incorrectly forwards the IGMP report to a client port, causing the host to suppress its reports. This results in the multicast stream being pruned prematurely.	IGMP Snooping		07.8.02
66444	A system reload may occur on a routing switch when a packet with an invalid source port field in the internal packet header is received.	System		07.8.02
67266	If sFlow and Layer 4 services are configured, collecting sFlow-specific Layer 3 information for export from a sampled packet may result in a system reload.	sFlow		07.8.02
67734	On an interface on which UDLD is configured, the logical link does not come up.	UDLD		07.8.02
	07.8.03			
55771	If OSPF is configured, an OSPF route is not removed from the OSPF routing table when the source of the route is removed.	OSPF		07.8.03
56958	Deleting a MAC address entry from CAM can sometimes cause a system reload.	System		07.8.03
62887	If OSPF is configured, the OSPF cost configured on Gigabit interfaces does not take effect.	OSPF		07.8.03
62982	On an EP 48-Port 10/1000-TX RJ45 module, MDI/MDIX capability does not function correctly after you reconfigure an interface from 100M full-duplex to auto-negotiation mode.	System		07.8.03
63081	On an EP 48-Port 10/1000-TX RJ45 module, a 10M full-duplex interface shows some packet loss while processing incoming packets.	System		07.8.03
63830	If VRRP is configured, if the interface using the VRRP master port is disabled, a gratuitous ARP packet with the physical MAC address is transmitted.	VRRP		07.8.03
65526	After you remove a 10 Gigabit Ethernet module with XENPAK optics from a routing switch, the module cannot be re-inserted without causing a system reload.	System		07.8.03

Bug ID	Bug Description	Protocol/ Feature	Version Found	Version Fixed
65528	Removing a module from a routing switch may cause Port Database entries on the module to be inaccessible, resulting in a system reload.	System		07.8.03
66003	After a module is removed from a routing switch, a syslog message is sometimes generated that lacks information to sufficiently describe the cause. This fix provides the following possible causes in the syslog: • The module is removed by the user. • Hardware failure of the module occurred. • A failure to read Board ID occurred.	System		07.8.03
66207	When 10 Gigabit Ethernet modules (MSA) are installed, entering the **debug** command to perform backplane debugging can sometimes cause a system reload.	System		07.8.03
67109	If RIPv2 and redistribution are configured and you remove a static route, an incorrect metric instead of a poison metric of 16 is sent out.	RIPv2		07.8.03
67172	An Inter Process Communication-related message may cause a system reload.	System		07.8.03
67848	If you configure an IP MTU, the **show ip interface** <*slot/port*> command does not correctly display the configured IP MTU value.	IP Stack		07.8.03
67854	If you configure an IP MTU and later modify the MTU value, the new value is not updated.	IP Stack		07.8.03
68140	If you configure OSPF and enable traps, OSPF neighbor state changes are not logged if the interface is not the designated router (DR).	OSPF		07.8.03
68295	The configuration of time zones in 30-second increments is not supported on the Simple Network Time Protocol (SNTP) clock.	SNTP		07.8.03
68645	When you download an image via INM with the option to save the configuration on a routing switch, a log message is generated with an invalid user name and remote IP address.	System		07.8.03
69093	When you run diagnostics on a routing switch by using the **dm diag** command, a system reload may occur.	System		07.8.03
69140	If you configure a single spanning tree, if the configuration has a large number of VLANs (several hundred), a system reload may occur when you enter the **show span** command.	Spanning Tree		07.8.03

Known Issues in 07.8.03

This section lists the known issues in software release 07.8.03.

Table 8: Known Software Issues in Release 07.8.03

Bug ID	Bug Description	Protocol Feature
59070	When PBR is configured with a route map that has multiple instances, each with a different match criteria and respective next-hop, the CAM entries are programmed for matched traffic with the next hop of the first instance. If the other instances of the route map match, the CAM is still programmed with the next hop of the first instance of route-map.	PBR
60396	A static MAC address for only one port is displayed in **show interface** command output if the address is configured for multiple ports.	Static MAC
61392	When CPU protection is enabled, a hardware flooding CAM entry does not match the unknown traffic. As a result, these packets are not forwarded or are discarded in hardware.	CPU Protection
61914	Strict security is not supported by 802.1X.	802.1X
62370	When CPU protection is enabled, CPU utilization is always around 50% when sending unknown unicast traffic.	CPU Protection
62562	Changes in an outbound rate-limiting configuration may require 300 seconds to take effect.	EP Rate Limiting

ProCurve 9300M Series Modules

Table 9 lists the modules that are currently available for use in ProCurve 9300M Series routing switches. (Discontinued modules are also listed.)

Table 9: ProCurve 9300M Series Modules

Module Type	Part Number and Description	Module String
EP Redundant Management Modules	**J4885A** ProCurve 9300 EP 8-Port Mini-GBIC Redundant Management Module	EP-8-port-mini-GBIC-management
EP Non-Management Modules	**J4881B** ProCurve 9300 EP 48-Port 10/100-TX RJ-45 Module	EP-48-port-10/100-TX-RJ45-module
	J4889B ProCurve 9300 EP 48-Port 10/100-TX Telco (RJ-21) Module	EP-48-port-10/100-TX-telco-module
	J4894A ProCurve 9300 EP 16-Port Mini-GBIC Module	EP-16-port-mini-GBIC-module
	J4895A ProCurve 9300 EP 16-Port 100/1000-T Module	EP-16-port-100/1000-T-module
	J8178A ProCurve 9300 EP 24-Port 100Base-FX Module	EP 24 Port 100Base-FX Module
Redundant Management modules (M2 and M4)	**J4845A** ProCurve 9300 GigLX Redundant Management Module (8-port)	8-port-gig-management-module Discontinued

Module Type	Part Number and Description	Module String
	J4846A ProCurve 9300 GigSX Redundant Management Module (8-port)	8-port-gig-management-module Discontinued
	J4847A ProCurve 9300 Redundant Management Module (0-port)	0-port-management-module Discontinued
	J4857A ProCurve 9300 Mini-GBIC Redundant Management Module (8-port)	8-port-gig-m4-management-module Discontinued
	J4879A ProCurve 9300 T-Flow Redundant Management Module (0-port)	— Discontinued
Management modules (M1) Supported only on the ProCurve 9304M and ProCurve 9308M. (M1 modules are not supported on the ProCurve 9315M.)	**J4141A** ProCurve 9300 10/100 Management Module (16-port)	16-port-copper-management-module Discontinued
	J4144A ProCurve 9300 Gigabit SX Management Module (8-port)	8-port-gig-management-module Discontinued
	J4146A ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port)	8-port-gig-management-module Discontinued
Unmanaged Modules (Standard, non-EP)	**J4140A** ProCurve 9300 10/100 Module (24-port)	24-port-copper-module Discontinued
	J4142A ProCurve 9300 100Base FX Module (24-port MT-RJ)	24-port-100fx-module Discontinued
	J4143A ProCurve 9300 Gigabit SX Module (8-port)	8-port-gig-module Discontinued
	J4145A ProCurve 9300 Gigabit 4LX/4SX Module (8-port)	8-port-gig-module Discontinued
	J4842A ProCurve 9300 1000Base-T Module (8-port)	8-port-gig-copper-module Discontinued
	J4844A ProCurve 9300 GigLX Module (8-port)	8-port-gig-module Discontinued
	J4856A ProCurve 9300 Mini-GBIC Module (8-port)	8-port-gig-module Discontinued
10 Gigabit Ethernet Modules (Unmanaged, supported with both Standard and EP Management Modules)	**J4891A** ProCurve 9300 1-port 10 Gb Module	1-port-10Gig-module Discontinued
	J8174A ProCurve 9300 2-port 10 Gb Module	2-port-10Gig-module

—This page intentionally left blank—

ProCurve Networking
HP Innovation