Release Notes

Version 06.6.36 Operating System

for the HP ProCurve Routing Switch 9304M, 9308M, and 6308M-SX, and Switch 6208M-SX

In December 2000 HP placed software release 06.6.28 on the HP Procurve website. This was followed by these software releases:

- 06.6.28 (available on the HP Procurve Website in December, 2000)
- 06.6.32 on the Product Documentation CD-ROM (Kit # 5064-9987—shipped with Redundant Management Modules beginning in April 2001)
- 06.6.33 (available on the HP Procurve Website in April, 2001)
- 06.6.36 (available on the HP Procurve Website in September, 2001).

These software versions are used as follows:

S/W Version:	Supported HP ProCurve 9304M and 9308M Routing Switch Modules:
06.6.28	These Devices: • J4141A HP ProCurve 9300 10/100 Management Module (16-port, MI) • J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port, MI) • J4146A HP ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port, MI) • HP ProCurve 6308M-SX Routing Switch (MI) • HP Procurve 6208M-SX Switch (MI)
06.6.32 06.6.33 06.6.36	These Devices: • All of the modules listed for release 6.6.28. • J4856A HP Procurve 9300 Mini-GBIC Module (8-port; unmanaged)

These release notes:

- Summarize the new operating system enhancements available in release 06.6.32. (Releases 06.6.33 and 06.6.36 include bug fixes, but do not include operating system enhancements.)
- Describe the new operating system enhancements added in software release 06.6.32.

NOTE: Descriptions of the new enhancements in releases 06.6.28 and earlier are included in the manuals for the 06.6.*xx* and 07.1.*xx* releases. You can download PDF versions of the manuals by visiting **http://www.hp.com/go/hpprocurve** and going to the **technical support** | **manuals** area.

- List earlier software operating problems fixed in the new software versions described in this document.

For release notes describing earlier software releases, go to the **technical support** | **manuals** area of the HP ProCurve website at **http://www.hp.com/go/hpprocurve**.

NOTE: This software release does not support Secure Shell (SSH) version 1. For SSH-v1 support, use software release 7.1.*xx* or greater.

Publication Number

5969-2391
Edition 1
September 2001

Applicable Product

HP Procurve 9304M Routing Switch (J4139A)
HP Procurve 9308M Routing Switch (J4138A)
HP Procurve 6308M-SX Routing Switch (J4840A)
HP Procurve 6208M-SX Routing Switch (J4841A)

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation.

Disclaimer

The information contained in this document is subject to change without notice.

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

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

Warranty

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

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

Contents

(This page is intentionally unused.)

Software Branches

Beginning with the software releases 06.6.28 and 07.1.10, HP offers two software (Operating System) branches:

- **06.6.28 and higher 06.X releases:** These releases typically include only bug fixes, and operate on the following devices:
  - HP 9304M and 9308M routing switches *without* redundant management (that is, with MI modules)
  - HP 6308M-SX routing switch
  - HP 6208M-SX switch
- **07.1.10 and higher 07.X releases:** These releases typically may include new features, enhancements to existing features, and bug fixes, and operate only with the HP 9304M and 9308M routing switches with redundant management (MII modules).

Note Regarding Removing Chassis Modules

When you remove a module from a 9304M or 9308M chassis, disable the module first before removing it from the chassis. Disabling the module before removing it prevents a brief service interruption on other forwarding modules. The brief interruption can be caused by the chassis reinitializing other modules in the chassis when you remove an enabled module.

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

```
HP9308# disable module 3
```

This command disables the module in slot 3.

Syntax: disable module <slot-num>

The <slot-num> parameter specifies the slot number.

- 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.

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

If you decide after disabling a module that you do not want to remove the module, re-enable the module using the following command:

```
HP9308# enable module 3
```

Syntax: enable module <slot-num>

NOTE: You do not need to enable a module after inserting it in the chassis. The module is automatically enabled when you insert the module into a live chassis or when you power on the chassis.

NOTE: On 9304M and 9308M devices, if you plan to replace the removed module with a different type of module, you must configure the slot for the module. To configure a slot for a module, use the **module** command at the global CONFIG level of the CLI.

Note to IP Multicast Users

HP routing switches support the following IP multicast versions:

- IGMP V2
- PIM Dense mode (PIM-DM) V1
- PIM Sparse mode (PIM-SM) V2
- DVMRP V2

For configuration information, see the “Configuring IP Multicast Protocols” chapter in the *Book 1: Installation and Getting Started Guide*.

Clarification On Trunk Load Sharing

HP devices load share traffic across the ports in a trunk group. The method used for the load sharing depends on the following:

- Device type – 9304M/9308M (chassis) or 6308M-SX and 6208M-SX (fixed-port)
- Traffic type – Layer 2 or Layer 3
- Trunk type – Switch or server
- For certain traffic, port type on which the traffic enters the HP device (Gigabit or 10/100)

NOTE: The port type applies only to Layer 2 traffic on a server trunk group configured on a 9304M or 9308M.

Table 1 (next page) lists how HP devices load share traffic across the ports in a trunk group on a 9304M or 9308M.

Table 1: HP Trunk Group Load Sharing – 9304M/9308M

Traffic Layer	Trunk Group Type	Traffic Type	Load-Sharing Basis
Layer 2	Switch	All traffic types	Destination MAC address
	Server	IP received on 10/100 port	Hash value derived from source and destination IP addresses
		IPX received on 10/100 port	Hash value derived from source and destination IPX addresses
		AppleTalk received on 10/100 port	Hash value derived from source and destination AppleTalk addresses
		Other traffic types received on 10/100 port	Hash value derived from source and destination MAC address
		All traffic types received on Gigabit port	Gigabit Port number on which traffic was received
Layer 3	Switch	IP	Destination IP address
		IPX	Destination IPX address
		AppleTalk	Destination AppleTalk address
		All other traffic types	Destination MAC address
	Server	IP	Destination IP address
		IPX	Destination IPX address
		AppleTalk	Destination AppleTalk address
		All other traffic types	Destination MAC address

Table 2 lists how HP devices load share traffic across the ports in a trunk group on a 6308M-SX or 6208M-SX.

Table 2: HP Trunk Group Load Sharing – 6308M-SX or 6208M-SX

Traffic Layer	Trunk Group Type	Traffic Type	Load-Sharing Basis
Layer 2	Switch	All traffic types	Destination MAC address
	Server	IP	Hash value derived from source and destination IP addresses
		IPX	Hash value derived from source and destination IPX addresses
		AppleTalk	Hash value derived from source and destination AppleTalk addresses
		Other traffic types	Hash value derived from source and destination MAC address
Layer 3	Switch	IP	Source and destination IP addresses
		IPX	Source and destination IPX addresses
		AppleTalk	Source and destination AppleTalk addresses
		Other traffic types	Source and destination MAC address
	Server	IP	Source and destination IP addresses
		IPX	Source and destination IPX addresses
		AppleTalk	Source and destination AppleTalk addresses
		All other	Source and destination MAC address

Redundant Management on the 9304M and 9308M Routing Switches

Redundant Management means that the switch can operate with two management modules installed; one active and one standby. If the active management module becomes unavailable, the standby management module automatically takes over system operation. Redundant Management requires MII or MIV modules (as described below) and software release 07.1.10 or later.

Management modules WITHOUT Redundant Management are sometimes termed "MI" modules (for "Management I"). MI modules include:

- J4141A HP ProCurve 9300 10/100 Management Module (16-port)
- J4144A HP ProCurve 9300 Gigabit SX Management Module (8-port)
- J4146A HP ProCurve 9300 Gigabit 4LX/4SX Management Module (8-port)
- J4840A HP ProCurve 6308M-SX Routing Switch

If you are using a management module without redundant management, only one management module can be installed in the routing switch.

NOTE: Due to memory limitations, software release 07.x.x or greater does not operate on MI modules.

Management modules WITH Redundant Management capabilities are sometimes termed "MII" or “MIV” modules (for “Management 2" or “Management 4”). These modules include:

- J4845A ProCurve 9300 GigLX Redundant Management Module (8-port, MII)
- J4846A ProCurve 9300 GigSX Redundant Management Module (8-port, MII)
- J4847A ProCurve 9300 Redundant Management Module (0-port, MII)
- J4857A HP Procurve 9300 Mini-GBIC Redundant Management Module (8-port, MIV)

If you are using a Redundant Management module, you can install either one or two such modules in the routing switch.

NOTE: MI management modules and MII/MIV redundant management modules are mutually exclusive. That is, the routing switch does not operate if an MII or MIV redundant management module is installed while an MI management module is also installed.

For more information, see the chapter titled "Using Redundant Management Modules" in *Book 1: Installation and Getting Started* (p/n 5969-2337, 2/00 or a later version), shipped with your routing switch. You can also find this manual in PDF format on the CD-ROM included with the routing switch or a management module, as well as at **http://www.hp.com/go/hpprocurve**. (Click on **technical support**, then **manuals**.

Mini-GBIC ports: Hewlett-Packard offers and supports only mini-GBICs that include an HP label (with product number J4858A or J4859A) for use with the J4856A HP Procurve 9300 Mini-GBIC Module and the J4857A HP Procurve 9300 Mini-GBIC Redundant Management Module. Using other brands of mini-GBICs is not supported.

Flash Images: The flash image files for this software release differ depending on the product. See “Software Image Files” on page 12.

SNMP: Beginning 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.

These notes also contain information regarding what happens when you disable BGP4, OSPF, or VRRP. See “Usage Guidelines for Access Control Lists (ACLs)” on page 12.

Downloading Software and Documentation

You can download software versions 06.6.36 and the corresponding product documentation from HP's Procurve website as described below.

To Download a Software Version:

1. Go to HP's ProCurve website at **http://www.hp.com/go/hpprocurve**
2. Click on **software** (in the sidebar).
3. Under "latest software", click on **switches**.

Note: If you are downloading software for a 9304M or 9308M, select the option that matches the type of management module(s) you are using in the device (WITH redundant management or WITHOUT redundant management).

To Download Product Documentation:

1. Go to HP's ProCurve website at **http://www.hp.com/go/hpprocurve**
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 new manuals under the heading "**For software version 06.6.33 or greater**".

You will need the Adobe® Acrobat® Reader to view and/or print the manuals.

Software/Device Compatibility

Table 1. Device Compatibility with Software Versions

Device	Supported Software Versions:				
	04791	**05084**	**H2R05216.BIN H2R06605.BIN H2R06616.BIN H2R07110.BIN H2R07122.BIN H2R07124.BIN**	**HPR05216.BIN HPR06605.BIN HPR06616.BIN HPR06628.BIN HPR06633.BIN HPR06636.BIN**	**HPS05216.BIN HPS06605.BIN HPS06616.BIN HPS06628.BIN HPS06633.BIN HPS06636.BIN**
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *WITH Redundant Management Module(s) (MII or MIV)*	*No*	*No*	**Yes**	*No*	*No*
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *WITHOUT Redundant Management Modules (MI)*	**Yes**	**Yes**	*No*	**Yes**	*No*
HP ProCurve Routing Switch 6308M-SX (J4840A)	*n/a*	*n/a*	*No*	**Yes**	*No*
HP ProCurve Switch 6208M-SX (J4841A)	*n/a*	*n/a*	*No*	*No*	**Yes**

Note: The flash image files for these software releases differ depending on the product.

If you have a 9304M or 9308M routing switch that was shipped before the software versions described in this document were available, you may want to download either of these releases from HP's ProCurve website. To do so, see the chapter titled "Using Redundant Management Modules" in *Book 1: Installation and Getting Started Guide*, that was shipped with your routing switch or switch.

For information on how to update your routing switch software, refer to the chapter titled "Updating Software Images and Configuration Files" in the documentation you received with the device.

Software Image Files

To run software release 06.6.36, you need the indicated boot and flash images listed in the following table.

Product	Boot Image	Flash Image
HP 9304M HP 9308M With one of these MI modules; that is, WITHOUT Redundant Management: • J4140A • J4144A • J4146A)	M1B07108.bin or later recommended	HPR06636.bin*
HP 9304M HP 9308M With any one or two of these MII or MIV modules; that is, WITH Redundant Management: • J4846A • J4845A • J4847A • J4857A	M2B07108.bin or later recommended	H2R07124.bin
HP 6308M-SX	• M1B07108.bin or later recommended	• HPR06636.bin*
HP 6208M-SX	• M1B07108.bin or later recommended	• HPS06636.bin*

*These software images do not support Secure Shell (SSH) version 1.

Usage Guidelines for Access Control Lists (ACLs)

This section provides some guidelines for implementing ACLs to ensure wire-speed ACL performance.

For optimal ACL performance, use the following guidelines:

- Apply ACLs to inbound traffic rather than outbound traffic.
- Use the default filtering behavior as much as possible. For example, if you are concerned with filtering only a few specific addresses, create deny entries for those addresses, then create a single entry to permit all other traffic. For tighter control, create explicit permit entries and use the default deny action for all other addresses.
- Use deny ACLs sparingly. When a deny ACL is applied to an interface, the software sends all packets sent or received on the interface (depending on the traffic direction of the ACL) to the CPU for examination.
- Adjust system resources if needed:
  - If IP traffic is going to be high, increase the size of the IP forwarding cache to allow more routes. To do so, use the system-max ip-cache <num> command at the global CONFIG level of the CLI.
  - If much of the IP traffic you are filtering is UDP traffic, increase the size of the session table to allow more ACL sessions. To do so, use the system-max session-limit <num> command at the global CONFIG level of the CLI.

Avoid the following implementations when possible:

- Do not apply ACLs to outbound traffic. The system creates separate inbound ACLs to ensure that an

outbound ACL is honored for traffic that normally would be forwarded to other ports.

- Do not enable the strict TCP ACL mode unless you need it for tighter security.
- Avoid ICMP-based ACLs where possible. If you are interested in providing protection against ICMP Denial of Service (DoS) attacks, use HP's DoS protection features. See the "Protecting Against Denial of Service Attacks" appendix in *Book 2: Advanced Configuration and Management Guide*. For information on this guide, see "Downloading Software and Documentation" on page 10.

If the IP traffic in your network is characterized by a high volume of short sessions, this also can affect ACL performance, since this traffic initially must go to the CPU. All ICMP ACLs go to the CPU, as do all TCP SYN, SYN/ACK, FIN, and RST packets and the first UDP packet of a session.

ACL Support on the HP Products

HP ACLs have two basic types if uses:

- Filtering forwarded traffic through the device
- Controlling management access to the device itself

In general, routing switches support both types of ACLs. However, the 6208M-SX switch supports ACLs only for access control.

The following table lists the ACL functions supported on each HP routing switch and Layer 2 Switch supported in this software release.

Product	Packet Forwarding ACLs Supported	Management Access ACLs Supported
9304M	Yes	Yes
9308M	Yes	Yes
6308M-SX	Yes	Yes
6208M-SX	No	Yes

Using ACLs and Network Address Translation (NAT) on the Same Interface

You can use ACLs and NAT on the same interface, so long as you follow these guidelines:

- Do not enable NAT on an interface until you have applied ACLs (as described below) to the interface. If NAT is already enabled, you must disable it, apply the ACLs, then re-enable NAT on the interface.
- Enable the strict TCP mode.
- On the inside NAT interface (the one connected to the private addresses), apply inbound ACLs that permit TCP, UDP, and ICMP traffic to enter the device from the private sub-net.

You can use a standard ACL to permit all traffic (including TCP, UDP, and ICMP traffic) or an extended ACL with separate entries to explicitly permit TCP, UDP, and ICMP traffic.

NOTE: You do not need to apply ACLs to permit TCP, UDP, and ICMP traffic unless you are applying other ACLs to the interface as well. If you do not plan to apply any ACLs to a NAT interface, then you do not need to apply the ACLs to permit TCP, UDP, and ICMP traffic.

Here is an example of how to configure device to use ACLs and NAT on the same interfaces. In this example, the inside NAT interface is port 1/1 and the outside NAT interface is port 2/2.

The following commands enable the strict TCP mode and configure an ACL to permit all traffic from the 10.10.200.x sub-net. A second ACL denies traffic from a specific host on the Internet.

```
HP9308(config)# ip strict-acl-tcp
```

```
HP9308(config)# access-list 1 permit 10.10.200.0 0.0.0.255
HP9308(config)# access-list 2 deny 209.157.2.184
```

The following commands configure global NAT parameters.

```
HP9308(config)# ip nat inside source list 1 pool outadds overload
HP9308(config)# ip nat pool outadds 204.168.2.1 204.168.2.254 netmask 255.255.255.0
```

The following commands configure the inside and outside NAT interfaces. Notice that the ACLs are applied to the inbound direction on the inside NAT interface, and are applied before NAT is enabled. In this example, ACL 1 permits all traffic to come into the inside interface from the private sub-net. ACL 2 denies traffic from a specific host from going out the interface to the private sub-net.

```
HP9308(config)# interface ethernet 1/1
HP9308(config-if-1/1)# ip address 10.10.200.1 255.255.255.0
HP9308(config-if-1/1)# ip access-group 1 in
HP9308(config-if-1/1)# ip access-group 2 out
HP9308(config-if-1/1)# ip nat inside
HP9308(config-if-1/1)# interface ethernet 2/2
HP9308(config-if-2/2)# ip address 204.168.2.78 255.255.255.0
HP9308(config-if-2/2)# ip nat outside
```

Where to Find More Information

The following topics are found in *Book 1: Installation and Reference Guide* (for software releases 6.6.x and 7.1.x). For more information, see “Downloading Software and Documentation” on page 10.

- For traffic filtering ACLs, see the “Using Access Control Lists (ACLs)“ chapter in *Book 1: Installation and Getting Started Guide*.
- For management access ACLs, see the “Securing Access to Management Functions“ chapter in *Book 1: Installation and Getting Started Guide*.
- For DoS protection features, see the “Protecting Against Denial of Service Attacks“ appendix in *Book 1: Installation and Getting Started Guide*.
- For information about IP access policies, see the “IP Access Policies“ section in the “Policies and Filters” appendix of *Book 1: Installation and Getting Started Guide*.
- For NAT configuration information, see the “Network Address Translation“ chapter in *Book 1: Installation and Getting Started Guide*.

Maximum File Sizes for Startup-Config and Running-Config Files

Each HP device has a maximum allowable 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 allowable size. If this occurs, you will not be able to save the configuration changes.

The following table lists the maximum size for the running-config and the startup-config file on HP devices.

Product type	Maximum running-config and startup-config file sizes[a]
A 9304M or 9308M using Management II or higher	256K
A 9304M or 9308M using Management I	128K
A 6308M-SX or 6208M-SX	64K

a.The running-config and startup-config file can each be the size listed. The maximum size is not the maximum combined size for the running-config and startup-config files.

To determine the size of a HP device's running-config or startup-config file, copy it 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.

- Command to copy the running-config to a TFTP server:

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

- Command to copy the startup-config file to a TFTP server:

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

Note Regarding Disabling BGP4, OSPF, or VRRP

You can easily disable a routing protocol using the CLI or Web management interface. However, be careful when you disable BGP4, OSPF, or VRRP. When you disable these protocols, the routing switch removes all the configuration information for the disabled protocol from the running-config. Moreover, when you save the configuration to the startup-config file after disabling one of these protocols, all the configuration information for the disabled protocol is removed from the startup-config file.

The CLI displays a warning message such as the following:

```
HP9300(config-bgp-router)# no router bgp
router bgp mode now disabled. All bgp config data will be lost when writing to
flash!
```

The Web management interface does not display a warning message.

If you have disabled the protocol but have not yet saved the configuration to the startup-config file, you can restore the configuration information by re-entering the command to enable the protocol (ex: **router bgp**), or by selecting the web management option to enable the protocol. If you have already saved the configuration to the startup-config file, the information is gone.

If you are testing a BGP4, OSPF, or VRRP configuration and are likely to disable and re-enable the protocol, you might want to make a backup copy of the startup-config file containing the protocol's configuration information. This way, if you remove the configuration information by saving the configuration after disabling the protocol, you can restore the configuration by copying the backup copy of the startup-config file onto the flash memory.

Summary and Description of Enhancements Added in Software Release 06.6.32 (for the 6308M-SX, 6208M-SX, and the 9304M and 9308M Chassis without Redundant Management Modules)

This section summarizes and describes the operating system enhancements in software release 06.6.32 for the HP 9304M and 9308M WITHOUT Redundant Management modules installed.

Release 06.6.33 and release 06.6.36 do not include enhancements.

Summary of Enhancements in 06.6.32

New Hardware

Hardware	Description	See Page
New Gigabit module for 9304M and 9308M Chassis devices	The J4856A HP Procurve 9300 Mini-GBIC Module has eight slots for miniature Gigabit Interface Converters (mini-GBICs). 1000BaseSX and 1000BaseLX mini-GBICs are available and can be installed and used in any combination.	16

Security Enhancement

Enhancement	Description	See Page
The **show tech-support** command is not supported at the User EXEC level of the CLI	A user cannot display the configuration information and statistics displayed by the **show tech-support** command unless the user has successfully logged on for Enable access to the device.	17

System-Level Enhancement

Enhancement	Description	See Page
Option to suppress Telnet connection rejection messages	You can disable the message that the HP device sends to a Telnet client that is denied access to the device.	17

Description of Enhancements in 06.6.32

The enhancements for release 6.6.32 are not described elsewhere in the product documentation.

Mini-GBIC Module for the 9304M and 9308M

Software release 06.6.32 supports the J4856A HP Procurve 9300 Mini-GBIC Module, a new eight-port forwarding module for the 9304M and 9308M chassis. The J4856A contains eight slots for miniature Gigabit Interface Converters (mini-GBICs). The module provides flexibility by allowing you to install any combination of the following mini-GBICs:

- J4858A HP Procurve Gigabit-SX Mini-GBIC: 1000BaseSX port with an LC connector; supports multimode fiber cabling. Connection to a 1000BaseLX port is not supported.
- J4859A HP Procurve Gigabit-LX Mini-GBIC– 1000BaseLX port with an LC connector; supports single-mode and multi-mode fiber cabling. Connection to a 1000BaseSX port is not supported.

For more on this topic, refer to *Installing and Removing a Mini-GBIC*, provided with the mini-GBIC module and also available in the technical **support** | **manuals** area of the HP Procurve website at **http://www.hp.com/go/hpprocurve**.

Security Enhancement

Software release 06.6.32 enhances security by removing support for the **show tech-support** command when the command is entered at the User EXEC level of the CLI. In software release 06.6.32, the command is supported only at the Privileged EXEC or configuration levels of the CLI. Thus, to use the command, a user must have successfully logged in to obtain Enable access to the CLI.

Option To Suppress Telnet Connection Rejection Message

By default, if an HP device denies Telnet management access to the device, the software sends a message to the denied Telnet client. Software release 06.6.32 provides an option to suppress the rejection message. When you enable the option, a denied Telnet client does not receive a message from the HP device. Instead, the denied client simply does not gain access.

To suppress the connection rejection message, use the following CLI method.

USING THE CLI

To suppress the connection rejection message sent by the device to a denied Telnet client, enter the following command at the global CONFIG level of the CLI:

```
HP9300(config)# telnet server suppress-reject-message
```

Syntax: [no] telnet server suppress-reject-message

USING THE WEB MANAGEMENT INTERFACE

You cannot configure this option using the Web management interface.

Software Fixes

NOTE: Software releases sometimes apply only to specific products. Check the list of products supported by the release to make sure the release applies to your product. Each set of release notes lists the products to which the release applies.

Fixed in 06.6.36

- **AppleTalk** – When the routing switch sent DDP packets to a particular router or AppleTalk device, the device sent them as multicast packets to the entire VLAN. This caused STP to behave incorrectly and resulted in MAC address station movements. In software release 06.6.36, the routing switch sends DDP packets as unicast packets.
- **CLI** – In some cases, entering the **show tech** command from a Telnet session, then entering any other show command that uses a paged display and ending the display using CTRL+C could cause system errors, such as hanging of the management session. The errors could occur because the **show tech** command uses a TCP buffer timer to ensure that it has enough buffers for sending the command's output to the Telnet session. If another subsystem in the software had started using the same memory location as the timer when you entered CTRL+C, CTRL+C cleared that memory location and thus could cause errors in the subsystem that was using the memory location.

  NOTE: The same type of issue, where one subsystem had started a timer but the timer was still in use when another subsystem inadvertently canceled the timer, could cause errors in other subsystems. The cause of the errors is fixed in 07.1.23.

- **DHCP** – If a DHCP client was moved from one port-based VLAN to another, the client was unable to obtain an IP address.
- **DVMRP** (9304M/9308M and 6308M-SX only) – In some configurations, if you ran DVMRP with multiple tagged trunk groups, the multicast packets were dropped when a new trunk member port was added to the trunk group.
- **DVMRP** and **PIM-DM** – In a configuration where two clients were in separate port-based VLANs that shared a tagged port, a client joining or leaving the multicast group could cause video interruption for the other client.

- **IGMP** – If a client left a multicast group, other clients in the same port-based VLAN experienced video interruption.
- **IP multicast** (chassis routing switch only) – If IP multicast routing was enabled on VLANs that shared a tagged port, and receivers were on the same VLAN as the sender and also on the other VLAN, received packets could be corrupted with 16 extra bytes of data, prepended to the original packet. This issue affected both PIM and DVMRP.
- **IPX** – If the routing switch received IPX packets whose destination MAC address was the routing switch port's MAC address, packet buffers were not freed. As a result, normal traffic forwarding stopped once the buffers became full.
- **OSPF** – In a configuration where a routing switch was configured as an Area Border Router (ABR) between a Not-So-Stubby Area (NSSA) and a backbone area, the routing switch did not pass the default route from the NSSA ASBR (the router with default-information-originate enabled) to the backbone area.
- **OSPF** – The **default-information-originate** command's **metric-type** option did not work.
- **OSPF** – In an NSSA, if the ABR received default route type 7 from the ASBR, the ABR did not translate the route into a type 5 LSA to the other area.
- **Route health injection** (routing switches only) – The feature did not work properly. When the ARP entry for a host timed out, the routing switch was not able to install the ARP reply immediately. This caused the injected route to be removed from the upstream router. Also, the **ip dont-advertise** command did not inject the network route into the upstream router, regardless of the result of the health check.
- **TCP counter** (routing switches only) – If the total time for active TCP connections to the routing switch reached a value of more than 49 days, this could cause a software reload.

Fixed in 06.6.32

- **CLI** – The **show ip bgp** command listed a route as the best route even when the route was unreachable. The show ip bgp route correctly displayed the route information.
- **DHCP relay** (6208M-SX only) – DHCP relay did not work on a port if a QoS priority was configured on the port.
- **Interface statistics** – If a Gigabit link went down, the octets counters for the port were reset to zero.
- **TACACS+** – Buffers for the TACACS+ subsystem filled to capacity, preventing further AAA operations.
- **Telnet CLI** – If you entered the **show configuration** command from a Telnet session to the CLI, the message “INFO: config data, primary copy checksum failed, try to read from backup” was displayed.
- **Virtual interfaces** – If you configured a virtual interface, then disabled it before configuring an IP address on the interface, the **enable** command did not re-enable the interface. Re-enabling the interface required removal and re-insertion of the physical link(s) for the interface.
- **Web management interface** – Selecting the Monitor->IPX->Port Counter link could cause the software to reload.

Fixed in 06.6.28

For the following devices, fixes in this section apply to the 06.6.28 software version:

- HP 9304M and 9308M routing switches using an MI management module; that is, without redundant management
- HP 6308M-SX routing switch
- HP 6208M-SX switch

For information about fixes in a software release before 06.6.28, see the release notes for that release.

- **10/100 ports** (9304M and 9308M only) – When a 10/100 port was disabled, the link LED did not go dark and the port on the other end of the link did not indicate that the link was down.
- **ACLs** – When an ACL was applied to an interface, the data buffer containing a packet denied by the ACL

could be freed twice.

- **ACLs** – If you used an external configuration file to load ACLs and an access-list command in the file had a blank space in front of the command, the system reset when you loaded the configuration file. This occurred if you loaded the file from a TFTP server or a flash card.
- **ACLs** – An extended ACL for IP protocol TCP or UDP did not take effect. The CLI allowed the ACL to be entered, but the ACL did not take effect and was not displayed in the running-config or in the **show ip acl** display.
- **ARP** – In configurations that use the IP follow feature, which allows multiple port-based VLANs to share the same IP sub-net address, ARP entries entered the Invalid state and remained in this state until the ARP entries were cleared. This problem prevented the device from responding to IP pings.
- **BGP4** – If a route map without **set** commands for matched routes was used for filtering neighbor outbound routes, the route map could cause reference count errors for the BGP attributes. As a result, attributes learned from a neighbor might not be cleared from memory even when the attributes were no longer being used. This could cause the memory for attributes to become full.
- **BGP4** – The first time BGP4 was enabled on a device, the BGP4 timer was not properly initialized. This required you to save the configuration and reload the software to initialize the timer. Now, you do not need to reload the software to initialize the timer. The timer is properly initialized as soon as you enable BGP4.
- **BGP4** – In a configuration where AS-path filters were in use and the routing switch received a route containing a very large number of AS numbers (50) in one path attribute, the software could reset.
- **CLI** – If you entered a very long string when prompted for a Telnet password, then pressed Enter before the software timed out the access attempt, the device reset.
- **CLI** (6208M-SX switch only) – The interface erroneously stated that the software supported Secure Shell (SSH).
- **CLI** – The CLI limited the number of VRRP VRIDs that could be displayed.
- **CLI** – When the skip-page mode was enabled, the last page of a **show vlan** display was missing a few lines of data. In addition, if the command was entered repeatedly, the CLI displayed the message “all 13 display buffers are busy, please try later” and did not display the VLAN data.
- **CLI** – If you entered the ip pim ttl-threshold <num> command, after you saved the configuration change to the startup-config file, the file contained two instances of the command. Moreover, after you reloaded the software, the show ip pim int <portnum> command showed the wrong TTL threshold value.
- **IGMP** (routing switch only) – The software did not save the **ip igmp query-interval** or **ip igmp max-response-time** command in the startup-config file, and thus did not reinstate the commands following a software reload.

NOTE: Make sure IP multicast routing is enabled before you configure IGMP parameters on a routing switch.

- **IP** – Momentary high CPU utilization could occur if the device had active IP static routes and was waiting for an ARP response from the next-hop gateway used by the static routes.
- **MAC filters** – A MAC filter applied as Ethernet type 0800 and equal to 0806 did not work.
- **OSPF** – Removing a static default route caused the system to reset.
- **OSPF** – OSPF permit redistribute did not work properly.
- **OSPF** – In configurations with two or more equal-cost Area Border Routers (ABRs), the routing switch could fail to remove the corresponding route path for external routes or inter-area summary routes when the link to one of these ABRs went down.
- **OSPF** – In a configuration where there was more than one route to a stub network, if the best route (the route with the lowest cost) became unavailable, the software did not use another, available route to the stub network.

- **OSPF** – This problem affected only configurations where two ASBRs each advertised a static route (redistributed into OSPF on the ASBRs) to the same external network, and where the advertisements resulted in other OSPF routers having two equal-cost paths to the external network. If the static route referred to an interface on one of the ASBRs as its next hop, and that interface flapped (went down and then came back up), one of the equal-cost paths was missing in the routers that received the static route advertisement from the ASBRs.
- **OSPF** – In configurations where there was more than one route to a stub network and the routes were though different next-hop routers, the software did not always choose the route with the shorter path. When this occurred, it was usually when the route with the shorter path flapped (went down and came back up).
- **PIM and VLANs** – Outbound multicast packets on a tagged PIM interface were sent with the VLAN ID 0.
- **PIM Dense** – On a VLAN containing tagged ports, the group reports received on a tagged port were not processed correctly. As a result, the tagged ports could be omitted from the forwarding entry, which could result in incorrect forwarding of multicast traffic.
- **PIM Sparse** – A memory management issue could cause the routing switch to drop IP multicast packets.
- **PIM Sparse** – The timer entries were not scheduled correctly, which could result in timer-related PIM Sparse events and messages to occur at times other than when expected.
- **RADIUS** – RADIUS authentication stopped working after 256 authentications. As part of standard RADIUS operation, the RADIUS 8-bit sequence number rolls back to 0 after 255. However, the HP device was using a 16-bit counter for the authentications and thus expected 256 (0x1ff), whereas the sequence number received from the RADIUS server was 0 (which was correct).
- **Spanning Tree** – If you enabled single STP, saved the configuration, then reloaded, STP was disabled on the device following the reload.
- **SRP** – In configurations where IP clients used SNAP encapsulation instead of Ethernet II encapsulation, the clients could ping the real IP address of the backed up gateway but could not ping the virtual IP address of the backed up gateway.
- **SRP** – On random occasions, when the active routing switch (primary) was powered down, then powered back up, network connectivity was lost to the hosts connected to the primary routing switch for approximately one minute.
- **Telnet** – In a configuration where two routing switches were directly attached by the same physical link but each side of the link was on a separate network, and each of the routing switches was configured with a static route that pointed to the other routing switch, the devices could not establish Telnet connections with one another even though they could respond to IP pings from one another.
- **Trunk groups** – In configurations where SRP, trunk groups, and Spanning Tree all were configured, ports did not properly learn the MAC address for the new root bridge following a topology change. As a result, loops could occur in the network.
- **VRRP** – If a device running VRRP in the backup state received a packet with the destination MAC of the VRID, the device tried to route the packet instead of forwarding it at Layer 2 to the VRRP master.
- **VRRP** – If you deleted an IP address from an interface on which multiple VRIDs were configured, the software removed all the VRIDs in addition to the one that matched the deleted IP address.
- **Web management interface** – If you were using the NetScape browser and enabled the front panel display, the browser would hang and not download all the required files.
- **Web management interface** – The interface did not allow creation of an AppleTalk protocol VLAN. The appropriate radio button could be selected, but selecting Add after selecting the radio button resulted in an error message.

Known Issues in Release 06.6.36

- **Syslog** – If the link state changes for a port in a trunk group and the port is not the primary port for the group, the software does not send a link state change message to the Syslog buffer.
- **CLI** – If the device is configured to authenticate user access, after a user enters a password to start a CLI session, the system name in the command prompt appears twice in each prompt (for example, `HP9300 RouterHP9300 Router>`). This is a cosmetic issue only and does not affect the device's operation or performance. This issue is also present on the 6208M-SX and 6308M-SX devices.
- **CLI** – The **show cpu** command sometimes displays incorrect statistics.
- **CLI** (6208M-SX and 6308M-SX only) – If a Gigabit port is configured for Auto-Gigabit (auto-negotiation) in software release 06.6.16 or later, the device does not retain the change following a software reload. The running-config file contains a Negotiation-Off setting for the port and the port at the other end of the link does not come up.
- **Interface-Based Static Routes** – If you replace an interface-based static route with one that has a longer network mask, the interface-based static route with the longer network mask does not correctly supersede the existing interface-based static route with the shorter network mask.

HP Part Number: 5969-2391
Edition 1, September 2001