Release Notes: Version 07.5.04 Operating System

for the HP ProCurve Routing Switch 9304M, 9308M, and 9315M
with Redundant Management (MII and MIV)

Software release 07.5.04 supersedes earlier software releases in the 07.x software branch. (For more on software branches, see “Software Branches” on page 1.)

Minimum S/W Version:	HP ProCurve Series 9300 Routing Switch Modules:
07.1.10	These Redundant Management Modules: • 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)
07.1.19	These Redundant Management Modules: • All of the modules listed for release 7.1.10. • J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module (8-port, MIV)

These release notes:

- Provide useful procedures, information, and notes for routing switch operation and management.
- *Summarize* the new operating system enhancements available in software release 07.5.04.
- *Summarize* earlier software operating problems fixed in software release 07.5.04.

Descriptions of the enhancements in release 07.5.04 are included in the manuals for the 07.5.*x* release. If you purchased a Redundant Management module with software version 07.5.04 or greater installed, then the CD shipped with the module includes these manuals. Otherwise, you can download PDF versions of the latest manuals. (Refer to “Downloading the Latest Software and Documentation” on page 5.)

NOTES:

Mini-GBIC ports: Hewlett-Packard offers and supports only mini-GBICs having an HP label (with product number J4858A, J4859A, or J4860A) for use with the J4856A HP ProCurve 9300 Mini-GBIC Module and the J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module. 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 “Software Image Files” on page 2.

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.

SSH: Release 7.5.04, HP supports Secure Shell (SSH) version 1.

Devices Without Redundant Management: For information on upgrading the software on the 9304M and 9308M routing switches WITHOUT redundant management, refer to the latest 6.6.x release notes. (Refer to “Downloading the Latest Software and Documentation” on page 5.)

Publication Number

5990-3049
Edition 1
July 2002

Applicable Products

HP ProCurve 9304M Routing Switch (J4139A)
HP ProCurve 9308M Routing Switch (J4138A)
HP ProCurve 9315M Routing Switch (J4874A)

HP ProCurve 9300 10/100 Module (J4140A)
HP ProCurve 9300 100Base FX Module (J4142A)
HP ProCurve 9300 1000Base-T Module (J4842A)
HP ProCurve 9300 Mini-GBIC Module (J4856A)
HP ProCurve 9300 Mini-GBIC Redundant Management Module (J4857A)

HP ProCurve Gigabit-SX-LC Mini-GBIC (J4858A)
HP ProCurve Gigabit-LX-LC Mini-GBIC (J4859A)
HP ProCurve Gigabit-LH-LC Mini-GBIC (J4860A)

Trademark Credits

Ethernet is a registered trademark of Xerox Corporation. Microsoft Windows NT is a registered trademark of Microsoft Corporation. SuperSpan is a registered trademark of Foundry Networks, Inc. Cisco is a trademark of Cisco Systems, Inc. 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.

Hewlett-Packard Company
8000 Foothills Blvd.
Roseville, CA 95747-5551
USA
http://www.hp.com/go/hpprocurve

Contents

This page is intentionally unused.

Software Branches

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

Software Version:	Typically Include:	Operate On:
06.6.28 and later 06.*x* releases	Bug Fixes	• 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 Greater 07.1.x Releases	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M and 9308M routing switches WITH redundant management (MII or higher modules)
07.5.04 and Greater 07.x Releases	New Features, Enhancements to Existing Features, and Bug Fixes	HP 9304M, 9308M, and 9315 routing switches WITH redundant management (MII or higher modules)

Already Using a 9304M or 9308M with Redundant Management? Here's New Information!

If you received a 9304M or 9308M before software release 07.5.04 began shipping, and you are updating the device to release 07.5.04, then you may want to examine the new product manuals that became available beginning with the 07.5.04 release. To view (and freely download) PDF versions of these manuals (whole manual, or chapter-by-chapter files). See "To Download Product Documentation:" on page 4.

Also, if you are upgrading a redundant management module to software release 07.5.04 (or greater) from a 7.1.*x* (or earlier) release, you will need to boot the routing switch from a TFTP server to perform this task. Refer to "Upgrading a Management Module to Release 07.5.0x (or Greater) for the First Time" on page 5.

Software/Device Compatibility

Table 1. Device Compatibility with Software Versions

Devices	Software Versions:				
	04791 05084	H2R07504.BIN	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 9315M (J4174A) Routing Switch with Redundant Management Modules *(MII or MIV)*	*No*	**Yes**	*No*	*No*	*No*
HP ProCurve Routing Switches *WITH Redundant Management Module(s) (MII or MIV):* • 9304M (J4139A) • 9308M (J4138A)	*No*	**Yes**	**Yes**	*No*	*No*
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *WITHOUT Redundant Management Modules (MI)*	**Yes**	*No*	*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**

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 the *Installation and Getting Started Guide* included on the CD-ROM shipped with your management module(s) and also available on the HP ProCurve website. (Refer to "Downloading the Latest Software and Documentation" on page 4.) Also, for information on how to update your routing switch software, refer to the chapter titled "Updating Software Images and Configuration Files" in the same *Installation and Getting Started Guide*.

Software Image Files

To run software release 07.5.04, you need the indicated boot and flash images listed below.

NOTE: This software release operates only with Redundant Management (MII and MIV) modules. You cannot install and run this software on non-redundant (MI) management modules.

The 9315M Routing Switch requires a minimum of one Redundant Management Module running software release 07.5.*x* or greater. This is true regardless of whether you plan to install a management module from a 9304M or 9308M that has been running an earlier release.

Due to the size of the 07.5.*x* (or greater) OS software image, you cannot directly upgrade the OS image in a Redundant Management Module if that module does not already have an 07.5.*x* (or greater) image in flash memory. Thus to upgrade a Redundant Management Module to release 07.5.*x* (or greater) for the first time (for use in the 9304M, 9308M, or the 9315M with Redundant Management), you must use the switch's BOOT MONITOR feature and initially boot the switch using 07.5.*x* (or greater) code residing in an TFTP server. To upgrade an MII or MIV management module from a release earlier than 07.5.04, refer to "Upgrading a Management Module to Release 07.5.0x (or Greater) for the First Time" on page 5.

NOTE: Release 07.5.04 includes Secure Shell (SSH) version 1 (HP 9304M, HP 9308M, and HP 9315M).

SSH is not available for the 9304M or 9308M with a 32MB management module ("Management I" module). Also, Management I modules cannot be used with the 9315M.

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 greater recommended	HPR06636.bin*
HP 9304M HP 9308M HP 9315M With any one or two of these MII or MIV modules; that is, WITH Redundant Management: • J4846A • J4845A • J4847A • J4857A	M2B07501.bin or greater recommended	H2R07504.bin
HP 6308M-SX	• M1B07108.bin or greater recommended	• HPR06636.bin*
HP 6208M-SX	• M1B07108.bin or greater recommended	• HPS06636.bin*

***Does not support Secure Shell (SSH) version 1.

NOTE: If you are adding a Gigabit Copper module to a 9304M or 9308M routing switch chassis, boot code version M2B07108.bin or later must already be installed in the routing switch.

Downloading the Latest Software and Documentation

You can download software version 07.5.04 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:

NOTE: The documentation for release 07.5.04 is included on the Product Documentation CD-ROM shipped with management modules after May, 2002.

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

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 latest manuals under the heading "**For software version 7.5.04 or greater**".

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

Upgrading the Routing Switch to a New Software Release

For easy software image management, all HP devices support the download and upload of software images between the flash modules on the devices and a Trivial File Transfer Protocol (TFTP) server on the network.

The management module contains two flash memory modules:

Primary flash — The default local storage device for image files and configuration files.

Secondary flash — A second flash storage device. You can use the secondary flash to store redundant images for additional booting reliability or to preserve one software image while testing another one.

Only one flash device is active at a time. By default, the primary image will become active upon reload.

You can update the software contained on a flash module using TFTP to copy the update image from a TFTP server onto the flash module. In addition, you can copy software images and configuration files from a flash module to a TFTP server.

NOTE: The 9304M, 9308M, and 9315M routing switches are TFTP clients but not TFTP servers. You must perform the TFTP transaction from the routing switch. You cannot "put" a file onto the routing switch using the interface of your TFTP server.

The 9304M, 9308M, and 9315M TFTP client supports 8 x 3 file names. If you try to copy a file with more than eight characters and up to three characters in the extension, the interface reports that the file was not found on the TFTP server.

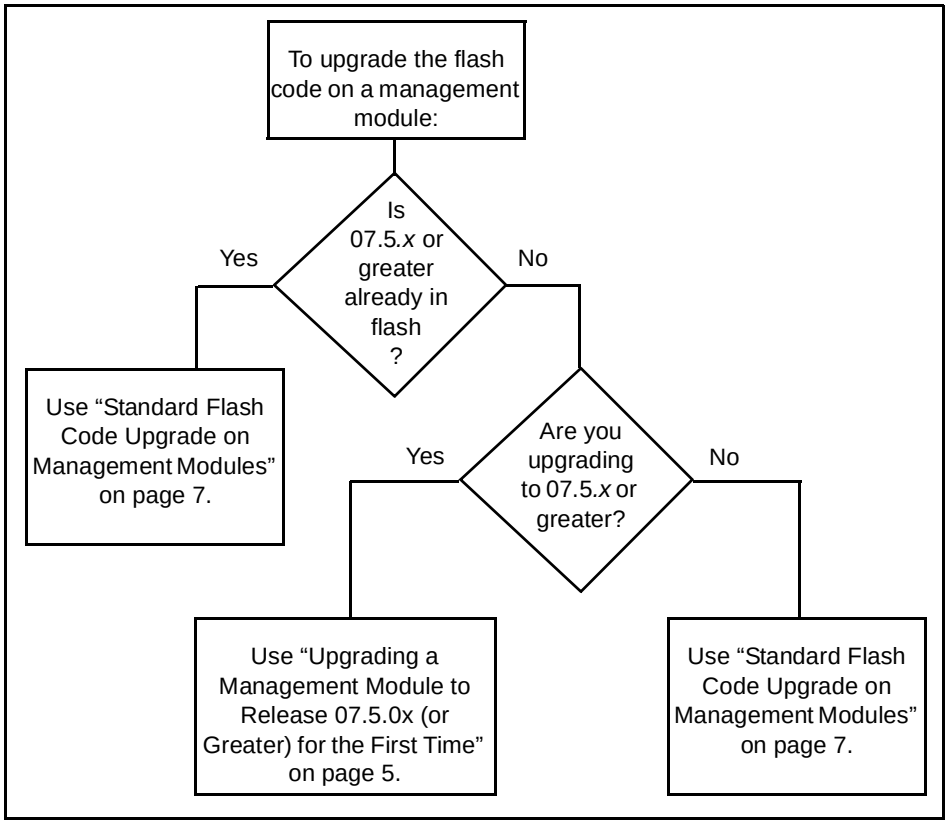
If you are upgrading redundant management modules, the flash code is automatically copied from the active management module to the standby module when you reload. However, the boot code is not automatically copied.

See the “Using Redundant Management Modules” chapter in the *Installation and Configuration Guide* included on the Documentation CD-ROM shipped with your management module(s). (For the latest version of this guide, visit **http://www.hp.com/go/hpprocurve** and click on **technical support** | **manuals**.)

Upgrading the Flash Code

Choosing the Upgrade Process

The process to use for upgrading software in a management module depends on (1) the latest version you have previously loaded into the module and (2) the version with which you want to upgrade the module. Use this flowchart to determine the upgrade process to use.



Upgrading a Management Module to Release 07.5.0*x* (or Greater) for the First Time

NOTE: The 9315M Routing Switch requires a minimum of one Redundant Management Module running software release 07.5.*x* or greater.

Due to the size of the 07.5.*x* (or greater) OS software image, you cannot directly upgrade the OS image in a Redundant Management Module if that module does not already have an 07.5.*x* (or greater) image in flash memory. Thus to upgrade a Redundant Management Module to release 07.5.*x* (or greater) for the first time (for use in the 9304M, 9308M, or the 9315M with Redundant Management), you must use the switch’s BOOT MONITOR feature and initially boot the switch using 07.5.*x* (or greater) code residing in an TFTP server.

Management modules shipped from the factory after May, 2002 include the minimum OS and boot code software required to operate a 9315M routing switch. (These modules can be installed in a 9304M, 9308M, or 9315M chassis). However, there are instances where you may be planning to use a management module with release 07.5.*x*, but that module's OS and/or boot code is earlier than release 07.5.*x*. For example:

- A module has been in prior service in a 9304M or 9308M chassis without upgrading to release 07.5.*x*.
- A module was shipped from the factory before release 07.5.*x* was released.

In these cases, it is necessary to upgrade the management module to 07.5.0*x* (or greater) OS and boot code. The following table provides a guide for this operation.

Hardware and Software Configuration	Software Upgrade Steps
MII or MIV Redundant Management Module installed in a 9304M or 9308M Chassis with: • Boot Code Earlier than 07.5.0x • OS Code Earlier than 07.5.0x **Note:** If you are using a fiber gigabit link for this operation, refer to "Known Issues" on page 33.	1. Copy the 07.5.*x* OS software to a TFTP server and note the file name and path. 2. Upgrade the boot code in the management module to release 07.5.0*x* or greater. (Refer to the chapter titled "Updating Software Images and Configuration Files" in the *Installation and Getting Started Guide for the HP ProCurve Routing Switches 9304M, 9308M, and 9315M*.) 3. Reboot the routing switch as follows. a. Execute the **reload** command. b. Immediately after executing the boot command, enter Boot Monitor mode by pressing and holding the [B] key. You will then see this prompt: **BOOT MONITOR >** c. Assign an IP address to the routing switch: **BOOT MONITOR > ip address** < *ip-address* > < *subnet-mask* > d. If necessary, assign a default gateway IP address to the routing switch: **BOOT MONITOR > ip default_gateway** < *ip-address* > 4. Boot the switch using the 07.5.*x* OS you previously copied into the TFTP server: a. **BOOT MONITOR > boot system tftp** < *server-ip-address* > < *file-name* > b. Upgrade the OS to 07.5.*x*. (Refer to the chapter titled "Updating Software Images and Configuration Files" in the *Installation and Getting Started Guide for the HP ProCurve Routing Switches 9304M, 9308M, and 9315M*.)

Hardware and Software Configuration	Software Upgrade Steps
MII or MIV Redundant Management Module installed in a 9315M chassis, and: • Boot Code 07.5.0*x* or greater. • OS Code Earlier than 07.5.0*x* **Note:** If you are using a fiber gigabit link for this operation, refer to "Known Issues" on page 33.	1. Copy the 07.5.*x* OS software to a TFTP server and note the file name and path. 2. Reboot the 9315M as follows. a. Execute the **reload** command. b. Immediately after executing the boot command, enter Boot Monitor mode by pressing and holding the B key. You will then see this prompt: **BOOT MONITOR >** c. Assign an IP address to the 9315M: **BOOT MONITOR > ip address** < *ip-address* > < *subnet-mask* > d. If necessary, assign a default gateway IP address to the 9315M: **BOOT MONITOR > ip default_gateway** < *ip-address* > 3. Boot the switch using the 07.5.*x* OS you previously copied into the TFTP server: a. **BOOT MONITOR > boot system tftp** < *server-ip-address* > < *file-name* > b. Upgrade the OS to 07.5.*x*. (Refer to the chapter titled "Updating Software Images and Configuration Files" in the *Installation and Getting Started Guide for the HP ProCurve Routing Switches 9304M, 9308M, and 9315M*.)
MII or MIV Redundant Management Module installed in a 9315M chassis, and: • Boot Code earlier than 07.5.0*x* • OS Code earlier than 07.5.0*x*	You will need assistance. Contact your HP support representative.
MII or MIV Redundant Management Module installed in a 9315M chassis, and: • Boot Code 07.5.0*x* or greater • OS Code 07.5.0*x* or greater	No upgrade necessary to use release 07.5.*x* OS and boot code. (For the latest code release, visit **http://www.hp.com/go/hpprocurve** and click on **software**.)

Standard Flash Code Upgrade on Management Modules

Use this procedure when you are ***not*** upgrading a management module from a release earlier than 07.5.*x*.

When you upgrade the flash code, you must upgrade the flash code on the management module to the same software release ***before*** you reboot.

To upgrade the flash code on a management module:

1. Place the new flash code on a TFTP server to which the routing switch has access.
2. Enter either of the following commands at the Privileged EXEC level of the CLI (example: `HP9300#`) to copy the flash code from the TFTP server into the flash memory of the management module:
   - `copy tftp flash` <ip-addr> <image-file-name> <primary | secondary>
   - `ncopy tftp` <ip-addr> <image-file-name> flash <primary | secondary>

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

   `show flash`

   The line that begins "`Compressed Pri Code size`" lists the flash code version in the primary flash, at the end of the line. Similarly, the line that begins "`Compressed Sec Code size`" lists the flash code version in the secondary flash.

4. If the flash code version is correct, go to Step 5. Otherwise, go to Step 1.

5. 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>

For information on changing the block size for TFTP transfers or using the web management interface to transfer software images, refer to *Book 1: Installation and Getting Started Guide* for the routing switches. For an electronic version of the latest release of this guide, visit **http://www.hp.com/go/hpprocurve** and click on **technical support** | **manuals**.)

Using SNMP to Upgrade Software

You can use a third-party SNMP management application such as HP OpenView to upgrade software on an HP device.

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

Use this procedure to upgrade a management II or IV module.

To upgrade flash code on the Management Processor:

1. Configure a read-write community string on the HP 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> **ro | rw**

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

2. On the HP 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 HP device, by default the HP 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 HP device.

   <hp-ip-addr> is the HP 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:

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

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

Updating Boot Code

Under certain conditions, HP support personnel may request you to update the boot code on a routing switch management module. Because the boot code is essential for the management module to operate, and because no backup copy is stored on the module, extreme caution is necessary when updating this code. Use the following steps to verify TFTP operation and to update the boot code.

1. Use the **show flash** command to verify the current boot code version. The last line in this example shows the verification output for boot code version 06.05.00:

```
HP9308> enable
HP9308# show flash
Active management module:
Code Flash Type: AMD 29F032B, Size: 64 * 65536 = 4194304, Unit: 2
Boot Flash Type: AMD 29F040, Size: 8 * 65536 = 524288
Compressed Primary Code size = 2579100, Version 07.1.10T53
Compressed Secondary Code size = 2053824, Version 06.6.16T53
Maximum Code Image Size Supported: 2817536 (0x002afe00)
Boot Image Version 06.05.00
```

2. Verify that your TFTP server interoperates properly with the routing switch. To do so, copy the software image stored in secondary flash to a TFTP server, delete the image from secondary flash, and then copy the image you saved onto the TFTP server back into secondary flash. For example, if the IP address of the TFTP server is 192.168.1.1 and the file name you will use to store the image is H2R06616.bin:

   a. Copy the software image stored in secondary flash to the TFTP server.

```
HP9308# copy flash tftp 192.168.1.1 H2R06616.bin sec
HP9308#Flash to TFTP Done.
```

   b. On the routing switch, delete the software image stored in secondary flash and verify that secondary flash is empty. (If secondary flash is empty, you will see "size = 0" in the "Compressed Secondary Code" line of the **show flash** command output.) For example:

```
HP9308# erase flash secondary
Flash Erase HP9308#------------------------------Erase flash Done.
HP9308# show flash
Active management module:
Code Flash Type: AMD 29F032B, Size: 64 * 65536 = 4194304, Unit: 2
Boot Flash Type: AMD 29F040, Size: 8 * 65536 = 524288
Compressed Primary Code size = 2579100, Version 07.1.10T53
Compressed Secondary Code size = 0, Version
Maximum Code Image Size Supported: 2817536 (0x002afe00)
Boot Image Version 06.05.00
```

   c. Copy the software image file you just saved (in step a) from the TFTP server back to secondary flash on the routing switch and verify that the code is stored in secondary flash. For example:

```
HP9308# copy tftp flash 192.168.1.1 H2R06616.bin sec
HP9308# Flash Erase ----------------------------------------
Flash Memory Write (8192 bytes per dot)
................................................................................
.................................................TFTP to Flash Done.

HP9308# show flash
```

```
Active management module:
Code Flash Type: AMD 29F032B, Size: 64 * 65536 = 4194304, Unit: 2
Boot Flash Type: AMD 29F040, Size: 8 * 65536 = 524288
Compressed Primary Code size = 2579100, Version 07.1.10T53
Compressed Secondary Code size = 2053824, Version 06.6.16T53
Maximum Code Image Size Supported: 2817536 (0x002afe00)
Boot Image Version 07.01.01
```

The “size” and “Version” values in the “Compressed Secondary Code” line, above, indicate that the software image file has been successfully reloaded into secondary flash. You have now verified that your communication with the TFTP server is working properly.

3. Download the appropriate boot code from the HP ProCurve website to your TFTP server. (Go to **http://www.hp.com/go/hpprocurve** and click on **software.**)
4. Use the (undocumented) boot command shown below to initiate the TFTP download. For example, to download the M2B07105.bin boot code from a TFTP server at 192.168.1.1.

CAUTION: It is extremely important that the TFTP download of the boot code is not interrupted. An interruption in this process can result in a non-bootable system. If for any reason the boot code download is not successful, please do not use the **reload** command in the next step. Instead, contact an HP Customer Care Center immediately. To find the HP Customer Care Center for your area, see the support and warranty booklet shipped with your routing switch product, or see the *HP ProCurve Networking Service and Support Guide* available on HP’s ProCurve website at **http://www.hp.com/go/hpprocurve**. (Click on **technical support** and then **support services**.)

```
HP9308# copy tftp flash 192.168.1.1 M2B07108.bin boot
  HP9308# Writing to flash, please wait ... Done

  HP9308# show flash
  Active management module:
  Code Flash Type: AMD 29F032B, Size: 64 * 65536 = 4194304, Unit: 2
  Boot Flash Type: AMD 29F040, Size: 8 * 65536 = 524288
  Compressed Primary Code size = 2579100, Version 07.1.10T53
  Compressed Secondary Code size = 2053824, Version 06.6.16T53
  Maximum Code Image Size Supported: 2817536 (0x002afe00)
  Boot Image Version 07.01.08
```

Note that in the preceding example, the Boot Image Version number (07.01.08) at the end of step 4, above, is a later (higher) version than the Boot Image Version number (06.05.00) at the end of step 1. This indicates a successful download of a new boot image to the `routing switch`.

5. Execute the **reload** command to ensure that the boot code operates properly:

```
HP9308# reload
```

Note Regarding Removing Chassis Modules

Before you remove a module from a chassis, 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 chassis re-initializing other modules in the chassis 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 applicable to management modules.

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

Syntax: enable module <slot-num>

For example, to re-enable a module in slot 3:

```
HP9308# enable module 3
```

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: 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.

Redundant Management on the 9304M, 9308M, and 9315M Routing Switches

Redundant Management means that the device 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.

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

NOTE: *MI management modules do not operate in the 9315M routing switch*.

Also, if you are using a management module without redundant management in a 9304M or 9308M, only one management module can be installed in the routing switch.

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, a 9304M or 9308M does not operate if an MII or MIV redundant management module is installed while an MI management module is also installed. Also, as noted above, MI management modules do not operate in a 9315M routing switch.

For more information, see the chapter titled "Using Redundant Management Modules" in the *Installation and Getting Started Guide* that is included on the *Documentation CD-ROM* shipped with your management module, and also downloadable from the HP ProCurve website. (Refer to "To Download Product Documentation:" on page 4.)

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 14.

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 9315 using Management II or higher	256K
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 an 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>

Configuration Considerations for the 15-Slot Chassis (9315M)

Use the following considerations when configuring your 15-slot Chassis device.

Upgrading from Earlier Software

The 15-slot chassis requires software release 07.5.04 or higher. This is true regardless of whether you plan to install a management module from a 4-slot or 8-slot chassis that has been running an earlier software release.

To upgrade a management module from a release earlier than 07.5.04, refer to "Upgrading a Management Module to Release 07.5.0x (or Greater) for the First Time" on page 5.)

Removing a Module from an Active Chassis

To remove a module from a chassis, disable the module first before removing the module from the chassis. Refer to “Note Regarding Removing Chassis Modules” on page 10.

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

Slot Locations for Redundant Management Modules

The 15 slots in the chassis 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, HP 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, HP recommends that you place the other management module in slot 6, 7, or 8.

Change to the Maximum Number of VLANs and Virtual Interfaces on 128M Devices

To support added features in software release 07.5.04 and greater, the maximum number of VLANs and virtual interfaces (VEs) that you can configure on 128M management modules is changed in software release 07.5.4 and greater.

Table 1 lists the default and configurable maximum numbers of VLANs and virtual interfaces for routing switches in software release 07.5.04 and later. Unless otherwise noted, the values apply to both types of switches.

Table 1: VLAN and Virtual Interface Support

Product	VLANs		Virtual Interfaces	
	Default Maximum	Configurable Maximum	Default Maximum	Configurable Maximum
M4 management module with 256MB	32	4095	255	4095
M2 management module with 128MB management module	16	512 (routing switch code)	255	512

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 chapter titled "Protecting Against Denial of Service Attacks"in the *Advanced Configuration and Management Guide* included on the Documentation CD-ROM shipped with your management module(s). Also, the latest version of this guide is available on the HP ProCurve website. (Refer to "Downloading the Latest Software and Documentation" on page 4.)

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 of 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 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 a 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-e1000-1/1)# ip address 10.10.200.1 255.255.255.0
HP9308(config-if-e1000-1/1)# ip access-group 1 in
HP9308(config-if-e1000-1/1)# ip access-group 2 out
HP9308(config-if-e1000-1/1)# ip nat inside
HP9308(config-if-e1000-1/1)# interface ethernet 2/2
HP9308(config-if-e1000-2/2)# ip address 204.168.2.78 255.255.255.0
HP9308(config-if-e1000-2/2)# ip nat outside
```

Where to Find More Information

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

Where To Find Documentation: All of the above manuals are included on the *Documentation CD-ROM* shipped with your management module(s). Also, the latest version of these guides are available on the HP ProCurve website. (Refer to “Downloading the Latest Software and Documentation” on page 4.)

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.

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 *Advanced Configuration and Management Guide provided for software release 07.5.x (or greater)*.

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/9315 (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.

Table 2 lists how HP devices load share traffic across the ports in a trunk group on a 9304M, 9308M, or 9315M.

Table 2: HP Trunk Group Load Sharing – 9304M/9308M/9315M

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

NOTE: The 6308M-SX and 6208M-SX use the 06.*x* software branch (page 1) and are no longer offered by Hewlett-Packard.

Table 3: 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

Recovering from a Lost Password

By default, the CLI does not require passwords. However, if someone has configured a password for the HP device but the password has been lost, you can regain super-user access to the device using the following procedure.

NOTE: Recovery from a lost password requires direct access to the serial port and a system reset.

To recover from a lost password:

1. Start a CLI session over the serial interface to the device.
2. Reboot the device.
3. While the system is booting, before the initial system prompt appears, enter **b** to enter the boot monitor mode.
4. Enter **no password** at the prompt. (You cannot abbreviate this command.) This command causes the device to bypass the system password check.
5. Enter **boot system flash primary** at the prompt.
6. After the console prompt reappears, assign a new password.

Summary of Enhancements in 07.5.04

This section summarizes the operating system enhancements in software release 7.5.04. These enhancements are described in the product documentation for software release 07.5.04 or greater, included on the *Documentation CD-ROM* shipped with management modules after May, 2002. The latest version of this documentation is also available on the HP ProCurve website. (Refer to "Downloading the Latest Software and Documentation" on page 4.)

New Hardware Support

Software release 07.5.04 provides the following new hardware support.

Enhancement	Description
New SNMP objects for Gigabit Interface Converters (GBIC) and mini-GBIC ports	You can use SNMP to determine what type of mini-GBIC a port has.

Layer 3 Enhancements in 07.5.04

Enhancement	Description
New command, to enforce use of an EBGP neighbor's AS as the first AS in the path	The **bgp enforce-first-as** command causes the device to accept an AS path update from an EBGP neighbor only if the neighbor's AS is also the first AS in the AS_SEQUENCE field in the Update. If the ASs do not match, the device sends a Notification to the neighbor and closes the session.
Support for using an IP address as a BGP4 cluster ID	The **bgp cluster-id** command allows you to enter an IP address for the cluster ID, as an alternative to entering a number. Previous releases support entering a number only.
New interface options for the BGP4 neighbor update source	The **neighbor** command's **update-source** parameter now allows you to specify a physical port, a virtual routing interface, or an IP interface as the source for receiving BGP4 updates from a neighbor. Previous releases support specifying a loopback interface only.
New command, to change the BGP4 next-hop update timer	The **update-time** command changes the timer value for updating the BGP4 next-hop tables.
New commands, to change the BGP4 best path comparison	The following commands disable or enable specific comparisons used during selection of the best route path to a given destination: • **as-path-ignore** – disables or re-enables comparison of otherwise equal paths based on the length of the AS-Path. • **compare-routerid** – enables or disables comparison of otherwise equal paths based on the router ID of the neighbor that sent the path. **Note**: Comparison of router IDs is applicable only when BGP4 load sharing is disabled.

Enhancement	Description
New command, to change the path types for which BGP4 load sharing is supported	The **multi-path** command lets you do the following: • Change load sharing support to apply to IBGP route paths only or to EBGP route paths only. By default, load sharing applies to both types of paths. • Enable load sharing among paths learned from different neighboring ASs. By default, load sharing applies only to paths that come from the same neighboring AS.
Static multicast groups	You can manually add a port to a multicast group. This is useful when a host is unable to use IGMP to advertise its group membership.
Unicast high-performance mode is enabled by default	The unicast high-performance mode, which enables the IP forwarding cache to contain more unique host route entries for unicast traffic, is enabled by default. In previous releases, the feature is disabled by default.
Increased route table capacity	You can configure the IP route table on a management module with 256M or higher to hold up to 400,000 entries. Previous releases support up to 256,000 routes. The default is still 128,000.
Support for configuring the ARP age on an individual interface	You can enter the **ip arp-age** command at the individual interface level to set ARP age for the interface. The interface's ARP age overrides the globally configured ARP age.
Support for enabling or disabling ICMP redirect messages on an individual interface	You can enter the **ip icmp redirect** command at the individual interface level to enable or disable ICMP redirect messages. **Note**: The port forwards misdirected traffic to the appropriate router, even if you disable the redirect messages.
Changes to BGP4 Multi-Exit Discriminator (MED) comparison	This release contains the following MED changes: • Deterministic MED is always on and cannot be disabled. Deterministic MED compares MEDs ***if and only if*** the routes were learned from the same neighboring AS. • A new command, **med-missing-as-worst**, makes the routing switch regard a BGP route with a missing MED attribute as the least favorable route, when comparing the MEDs of the routes.
Cooperative BGP4 route filtering	You can configure the routing switch to send IP prefix lists to a BGP4 neighbor and ask the neighbor to use the prefix lists to filter routes sent from the neighbor to the routing switch.
New command to unsuppress a neighbor's routes	You can use the **neighbor** <ip-addr> | <peer-group-name> **unsuppress-map** <map-name> command to selectively unsuppress a route that has been suppressed due to aggregation, and enable advertisement of that route to a neighbor or peer group.
New command to use the IP default route as a valid next hop for a BGP4 route	You can use the **next-hop-enable-default** command to enable the device to use the IP default route to resolve the BGP4 next hop for a BGP4 route. By default, the default route is not used to resolve the BGP4 next hop.
Named IP community and AS-path ACLs	The CLI syntax for configuring IP community ACLs and AS-path ACLs is changed to accept a text string instead of a number as the ACL ID.

Enhancement	Description
New BGP4 route-map options	This release provides the following new route-map options for BGP4 routes: • **match ip route-source** <acl> | **prefix** <name> – Matches based on the source of a route (the IP address of the neighbor from which the HP device learned the route) • **match community** <acl> **exact-match** – Matches a route only if the route's community attributes field contains the same community numbers specified in the match statement • **set metric-type internal** – When advertising a BGP4 route to an EBGP neighbor, sets a route's MED to the same value as the IGP metric of the BGP4 next-hop route • **set ip next-hop peer-address** – Sets the BGP4 next hop for a route to a neighbor address (inbound filtering) or the local IP address of the BGP4 session (outbound filtering) • **set comm-list** <acl> **delete** – Deletes the specified communities from a route's communities attribute
Support for using regular expressions in BGP4 community ACLs	You can use a regular expression in a community ACL. Previous releases support regular expressions only in an AS-path ACL or filter.
New option to display the last packet from a BGP4 neighbor that contained an error	You can use the **last-packet-with-error** option with the **show ip bgp neighbor** <ip-addr> command to display the last packet from the neighbor that contained an error. The packet's contents are displayed in decoded format.
Support for OSPF RFC 2328 Appendix E	The routing switch generates separate type-5 link-state advertisements (LSAs) for external networks that are the same network but have different network masks. Previous releases do not generate separate LSAs.
New IP interface options for OSPF	You can configure an IP interface to be ignored by OSPF or to be advertised in OSPF without the interface forming OSPF router adjacencies. By default, an IP interface on a port enabled for OSPF is advertised and forms OSPF adjacencies.
Dynamic memory allocation for IP multicast groups	The software dynamically allocates memory for up to 1024 PIM group memberships and 1024 DVMRP group memberships.
Support for PIM Sparse Mode (SM) on loopback interfaces	You can configure a PIM SM Bootstrap Router (BSR) or Rendezvous Point (RP) on a loopback interface. Previous releases support configuring BSRs and RPs on physical ports or virtual interfaces only.
Multi-protocol Border Gateway Protocol (MBGP) support	You can use MBGP to configure BGP4 routing features for exchanging IP multicast route information with other IP multicast routers.
Option to disregard OSPF MTU field	You can disable comparison of the MTU field when forming OSPF adjacencies.
Enhancement to OSPF route learning	If a new area is configured after the routing switch comes up, OSPF routers in the new area learn routes in other areas.
Disabling BGP4 removes the entire BGP4 configuration	In software releases earlier than 07.5.04, disabling BGP4 does not actually remove the configuration information for the protocol. ***In software release 07.5.04, disabling BGP4 removes all the running configuration information for the protocol.***

Enhancement	Description
Changes to how BGP4 compares route paths	The default method for comparing paths based on the Multi-Exit Discriminator is changed.
New option for BGP4 neighbors	You can specify a maximum number of network prefixes to learn from a given BGP4 neighbor, and optionally terminate the session with that neighbor if the maximum is exceeded.
Soft reconfiguration of BGP4 neighbor sessions	You can configure the routing switch to retain all route updates from a neighbor or peer group, and use those updates to change the BGP4 route table after you change route policies. This method avoids requesting the neighbor's entire BGP4 route table again or resetting the session with the neighbor.
Changes to route maps are retroactively implemented	If you change a route map that is used by the BGP4 **network** command or a BGP4 redistribution command, the software updates the routes to retroactively place the change into effect. You do not need to clear routes manually.
Easier method for deleting route maps	You can remove an entire route map using a single command. Previous software releases require you to delete each entry in the route map separately.
New display option for **show ip route** command	The new **none-bgp** option displays the most specific route (the route with the longest matching prefix) that was not learned from BGP4.
New command for clearing and re-installing BGP4 routes in the IP route table	The **clear ip bgp routes** [<ip-addr>/<prefix-length>] command clears BGP4 routes from the IP route table and re-installs routes.
Enhanced **show ip bgp summary** display	The display lists how many routes have been filtered out and thus not placed in the BGP4 route table.
Enhanced display of summary route information	All show commands that display BGP4 route information in summary format have been enhanced to show the AS-path of the Network Layer Reachability Information (NLRI).
Option to display summary route information for all BGP4 neighbors	You can enter a single command, **show ip bgp neighbor route-summary**, to display summary route information for all BGP4 neighbors. Previous releases allow you to display the summary information for individual neighbors only.
Enhancement to route information shown when you specify a prefix	When you specify an IP address with a **show ip bgp routes** <ip-addr> or **show ip bgp** <ip-addr> command, the output now lists information about the paths installed in the IP route table and the neighbors to which the routes will be advertised.

Enhancement	Description
Enhancements to **show ip bgp routes** command	The **show ip bgp routes** command has the following enhancements: • A new option, **nexthop**, for displaying the routes for a given next-hop IP address. • A new option, **no-best**, to display the BGP4 routes for which none of the routes to a given prefix were selected as the best route. • A new option, **age** <secs>, to display only the routes that have been received or updated more recently than the number of seconds you specify. • A new option, **route-map** <map-name>, to display only routes that match the match conditions in the route map. • Two new fields and enhanced display format for the **detail** option.
New command for displaying peer group information	The **show ip bgp peer-group** [<group-name>] command displays configuration information for the specified peer group or for all peer groups.
Enhanced **show ip bgp neighbors** <ip-addr> display	The display now lists the values for all the configurable parameters for the neighbor.
Option to display error packet information for all neighbors	You can enter a single command, **show ip bgp neighbor last-packet-with-error**, to display error packet information for all BGP4 neighbors. Previous releases allow you to display the information for individual neighbors only.
Route map support for OSPF redistribution	You can use route maps to more tightly control route redistribution into OSPF.
Configurable reference bandwidth for OSPF interface cost	You can change the basis (reference bandwidth) on which the software calculates the OSPF cost of an interface.
OSPF Link State Advertisement (LSA) filters	You can filter out type 3 LSAs from a given area and address range.
Graceful migration for OSPF authentication changes	The software supports both new and old (changed) authentication information for a brief, configurable interval to prevent disruption to adjacencies with neighbors.
Changes to the ACLs in distribution lists are implemented automatically	If you change an ACL that is used by an OSPF distribution list, the software automatically implements the change. Previous releases require you to clear the IP route table to place a change to an OSPF distribution list into effect.
New Syslog messages for bad OSPF packets	The device generates a Syslog message if it receives a bad OSPF packet. The message provides details about the error.
New command to list routes redistributed into OSPF	The **show ip ospf redistribute route** command lists the routes that have been redistributed into OSPF and the source from which the routes were redistributed.
New option for decrypted display of OSPF link-state advertisements (LSAs)	The **extensive** option displays decrypted LSA information when you use the option with the following commands: • **show ip ospf database external-link-state** • **show ip ospf database link-state**

Enhancement	Description
New command for displaying entries in the Content Addressable Memory (CAM)	You can use the **show cam ethernet** <portnum> command to display Layer 2 CAM entries and the **show cam ip** <portnum> command to display Layer 3 CAM entries.
Support for Protocol Independent Multicast, Dense Mode (PIM DM) version 2	You can enable PIM DM V2 or V1 on a routing switch interface. Previous software releases support V1 only.
Increased number of VRRP Virtual Router IDs (VRIDs) supported on an interface	You can configure up to 16 VRRP VRIDs on an interface. Previous releases support up to 12.
Support for Network Address Translation (NAT) of global (Internet) addresses into private addresses	You can configure inside destination NAT, which translates the global addresses of traffic received from those addresses into private addresses. Previous releases support translation only of private addresses into public addresses, for traffic generated by the private addresses.
Support for optimized forwarding on the default route	You can optimize a routing switch's Content Addressable Memory (CAM) to cache multiple forwarding entries for the default route, instead of caching entries for individual destination networks.
BGP4 next-hop recursion	You can enable BGP4 to recursively look up a route's next hop until the software finds an Interior Gateway Protocol (IGP) path to the route destination. By default, the software performs only one route lookup, regardless of whether the path to the next hop is an IGP path or a BGP path. Only BGP routes with IGP paths to the next-hop gateway are eligible to be installed in the IP route table.
New command for injecting a a default route into an OSPF Not-So-Stubby Area (NSSA)	You can configure the routing switch to inject a Type-7 default route into an NSSA to provide a path out of the NSSA, when the routing switch is an Area Border Router (ABR).
New CLI command to display CPU utilization statistics	The **show process cpu** command shows the percentage of CPU processing that each Layer 3 protocol has used since startup and had used at various time intervals.
New SNMP objects for PIM Sparse Mode (SM)	You can manage PIM SM through an SNMP application by accessing new PIM SM MIB objects.
Higher maximum number of IP routes	Redundant management modules with 128MB or higher memory can have up to 256,000 IP routes. Previously, up to 200,000 routes were supported.
More control over route redistribution from OSPF into the IP route table	You can use a distribution list to deny specific OSPF routes from being eligible for insertion into the IP route table.
Change to the default value for the IGMP maximum response time	The default IGMP maximum response time is 5 seconds in software release 07.5.04. In previous software releases, the default is 10 seconds.

Layer 2 Enhancements in 07.5.04

Enhancement	Description
New command to display SuperSpan™ customer ID information	The **show super-span** [**cid** <num>] command displays the boundary interface configuration and BPDU statistics for each SuperSpan customer ID configured on the device.
SuperSpan™	You can configure HP devices as a common STP backbone for a large number of separate customer spanning trees. The SuperSpan backbone allows a very large yet manageable Layer 2 network while still minimizing interruptions caused by topology or link-state changes.
STP per VLAN group	You can configure a group of port-based VLANS to use the same instance of a spanning tree. Grouping VLANs for STP enables you to use STP in more VLANs on a device.
GARP VLAN Registration Protocol (GVRP)	GVRP enables an HP device to dynamically create 802.1Q-compliant VLANs on links with other devices that are running GVRP. **Note**: This feature is supported in the B2R, B2S, and B2P images only.
Rapid Spanning Tree (RSTP)	This feature enhances STP by immediately failing over to an alternate root port if the root port becomes unavailable.
Spanning Tree (STP)	The valid range for the STP port priority has been changed from 0 – 255 to 8 – 255.

System-Level Enhancements in 07.5.04

Enhancement	Description
STP display enhancements	This release contains the following enhancements to how STP information is displayed: • The **show span detail** command's output is condensed to show information in fewer lines. In addition, the display now shows the bridge identifier. • New options with the **show span detail** command display detailed information for a single port in a specific VLAN. • The **show span** display is more readable.
New commands, to display and clear ACL statistics	The **show ip acl-traffic** command lists the number of packets permitted and denied by ACLs. The **clear ip acl-traffic** command clears the statistics.
New command, to enable hardware filtering for packets denied by ACLs	You can use the **hw-drop-acl-denied-packet** command to enable the device to create Content Addressable Memory (CAM) entries for packets denied by ACLs. This causes the filtering to occur in hardware instead of in the CPU. By default, packets denied by ACLs are filtered by the CPU.
New command, to reload an individual ATM module	The **reload atm** <slotnum> command reloads the software on a specific module in the chassis, without also reloading the management module.
Port ranges and lists supported when disabling or re-enabling trunk ports	You can disable ro re-enable a range or list of individual ports in a trunk group. Previous releases support disabling or re-enabling either a single trunk port or all ports in the trunk group, but do not support disabling or re-enabling a range or list of ports.
New command, to close a UDP port	The **port aps | bootp** command closes a UDP port. Some UDP ports are left open by default on the device. In software release 07.5.04, you can close the BootP or APS UDP port to provide additional security for the device.
New SNMP traps in the HP MIB	Traps are generated for the following conditions: • Changes to the running configuration • Changes to the start-up configuration • User login • User logout
Enhancements to SNMP version 3	SNMP Version 3, the user-based security model, has been enhanced with the following additions: • Support for SNMP version 3 packet encryption using the Data Encryption Standards (DES) encryption key. • Engine boots and engine time have been added to the SNMP version 3 packets. These parameters plus the engine ID provide replay protection of packets.
Addition of SNMP System Log Server Table	Servers where Syslog messages will be sent can be configured using the new SNMP object "snAgSysLogServerTable".
End-to-end link keepalive for trunk links	End-to-end link keepalive monitors the links between two HP devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices.

Enhancement	Description
sFlow Export MIB support	The sFlow MIB (RFC 3176) enables you to configure and manage sFlow Export through SNMP.
Simplified configuration of individual trunk ports	The **config-trunk-ind** command enables configuration of individual trunk ports. You can enable, disable, or monitor primary or secondary individual trunk ports after entering this command. The command is not required for renaming individual trunk ports.
Simplified **show statistics** and **show statistics brief** displays	The display of packet errors in the output of the **show statistics** and **show statistics brief** commands is simplified to list InErrors and OutErrors only. Detailed error information is still provided by the **show statistics** <portnum> command.
Additional parameters for the **show span detail** command	The **show span detail** command has the following new parameters: • **vlan** <num> – Specify detailed information only for the specified VLAN • <num> – Skip the display forward to display information for VLANs after the specified number of VLANS
New command, to display information about VLAN groups	The **show vlan-group** [<group-id>] command displays configuration information for VLAN groups.
The **show process cpu** command displays GARP VLAN Registration Protocol (GVRP) statistics	The **show process cpu** command now includes statistics for GVRP.
SNMP MIB objects for 10 Gigabit Ethernet modules	Objects that show the speed of incoming and outgoing traffic on interfaces that are 10 Gigabits or faster have been added to the HP MIBs.
Support for Maximum Transmission Unit (MTU) of 1920 bytes.	A new command, **jumbo**, globally sets the MTU for Ethernet interfaces to 1920 bytes. Previous releases support up to 1500 bytes.
Trunk group enhancements	This release contains the following trunk group enhancements: • New command, **trunk deploy**, to activate trunk group configuration commands without reloading the software. • Support for up to eight 10/100 or Gigabit trunk ports supported per module • New commands for naming, disabling, and re-enabling individual ports in a trunk group • Support for monitoring individual ports in a trunk group • Enhanced trunk group information display
ACL packet and flow counters	The HP device counts packets and flows matching a given ACL entry in an ACL list.
Option to add a comment to an ACL	You can optionally add comment text to describe entries in an ACL.
ACL permit logging	This release supports logging of packets that match the permit conditions of an ACL entry.

Enhancement	Description

Show command enhancements	This release contains the following enhancements to show commands:
	• You can display hardware serial numbers.
	• The **show interfaces** command displays an interface's input and output load in terms of bits per second, packets per second, and utilization percentage, averaged over a configurable interval.
	• The **show ip interface** command now displays the following IP parameters for each interface:
	  • Proxy ARP
	  • Split horizon
	  • ARP age
	  • IP ACLs applied to the interface
	• A new command, **show ip vrrp vrid** <num> [**ethernet** <num> | **ve** <num>], displays information for a specific VRP VRID and even for a specific port configured with the VRID.
	• The **show interface** [<portnum>] and **show interfaces brief** commands show a virtual interface's state as down if the interface's VLAN is down.
	• A new command, **show ptrace**, lists the ptraces that are enabled.

Support for searching and filtering output from **show** commands	You can filter CLI output from **show** commands and at the --More-- prompt.
IPv6 protocol VLAN support	You can configure protocol-based VLANs to provide Layer 3 broadcast domains for IPv6 traffic.
Support for empty VLANs	You can configure a VLAN without ports or delete all the ports from a VLAN without the VLAN being removed from the configuration. Previous releases do not allow you to configure a VLAN with no ports, and delete a VLAN entirely if you remove all the ports from the VLAN.
Change to how SSH key pairs are stored on HP devices	Starting this software release, RSA host key pairs are saved in internal memory on the HP device and, by default, do not appear in the startup-config file. You can optionally configure the HP device to hide or show the RSA host key pair in the running-config file.
Support for TFTP source interface	You can specify an IP address on the HP device to use as the source address for all TFTP packets originated by the device.
More flexible command syntax for clearing MAC addresses	The **clear mac-address** command has new parameters that allow you to specify a module, VLAN, or individual port.
Support for Telneting to a specified port	The HP device supports connecting to a Telnet server using a specified port number.
Cancelling an outbound Telnet session	If you have established a Telnet session from the console to a remote Telnet server, you can terminate the Telnet at the console.
Support for reading Cisco Discovery Protocol (CDP) packets	You can enable an HP device to capture and display the contents of a CDP packet, which contain information about the Cisco devices that send them.

Enhancement	Description
Enhanced **show span** output	The **show span detail** and **show span vlan** <vlan-id> commands are enhanced to display more information.
Enhanced **show span vlan** output	The **show span detail** command is enhanced to display more information.
New port number format in Web management interface	Chassis port numbers in the Web management interface are displayed and can be selected as a single entity. For example, port 1/1 is a single item on the pulldown menu for a panel's Port field. In previous releases, separate fields were used for slot numbers and port numbers.
Change to the SNMP community strings command	Specific views of the MIB can be assigned to community strings.
Support for SNMP v3 (RFCs 2570 and 2575)	You can use SNMP v3 for tighter security when managing an HP device.
New HP MIB objects	This release contains new HP MIB objects for the following: • CPU utilization • Memory utilization • Software loads • SNMP trap holddown
Enhancement to **ptrace snmp** command	The command now lists the SNMP portion of all incoming SNMP packets.
New HP MIB object for CPU utilization	HP MIB MIB07208.mib and later contains the snAgentCpuUtilTable object for CPU utilization.
Maximum number of local user accounts increased	You can configure up to 32 local user accounts for access authentication. Previous releases support up to 16 local user accounts.
New display options for the running-config	You can specify an interface or use the **vlan** option with the show running-config command to display configuration information specifically for the interface or for VLANs.
Displaying TCP memory usage	The **show memory tcp** command displays the amount of used and free memory for each of the four internal TCP buffers.
Displaying TCP connections	The **show ip tcp connections** command displays information about each TCP connection on the device, including the local IP address, local port number, remote IP address, remote port number and the state of the connection. In addition, the command displays the percentage of free memory for each of the internal TCP buffers.
Displaying information about individual TCP connections	The **show ip tcp status** command displays detailed information about a specified TCP connection, including the sequence and ACK numbers, window sizes, and available buffer sizes.
Displaying internal TCP buffer memory allocation	The **debug ip tcp memory** command causes messages to be displayed when memory is allocated or deallocated to the internal TCP buffers.
Options to specify ICMP message types upon which to filter in extended ACLs	You can use extended ACLs to more precisely filter ICMP traffic using new ICMP message type options.

Enhancement	Description
Support for multiple ports on a Static MAC entry	When you configure a static MAC entry, you can associate the entry with multiple ports. Previous software releases allow you to associate a static MAC entry with only a single port.
Support for multiple mirror ports	You can configure and use more than one mirror port. Each mirror port can have its own set of monitored ports. Previous releases allow only one mirror port.
Increased maximum number of VLANs on 256MB redundant management modules	You can configure up to 4095 port-based VLANs on a redundant management module with 256MB or higher memory. Previous releases allow up to 2048 VLANs.
Configurable holddown timer for SNMP traps	You can specify how many seconds SNMP waits following a software reload or device cold start, before beginning to send traps to an SNMP server. Previous software releases use a non-configurable holddown time of 60 seconds.
New MIB objects for dynamic memory utilization statistics	The HP MIB has new objects that indicate the total amount of memory on the device, the amount that is free, and the percentage that is currently being used.
Support for SSH access control using ACLs	You can more tightly control management access to a device through SSH by using ACLs.
Configurable maximum idle time for SSH sessions	The maximum idle time for SSH sessions can be set to between 0 – 240 minutes.
Encryption of RADIUS and TACACS keys	When you display the configuration of the HP device, the RADIUS and TACACS keys are encrypted. You can configure this feature using the CLI, Web management interface.
AAA security for commands pasted into a running-config file	If AAA security is enabled on the device, commands pasted into the running-config file are subject to the same AAA operations as if they were entered manually.
Ability to specify different servers for individual AAA functions	In a RADIUS or TACACS+ configuration, you can designate a server to handle a specific AAA task. You can configure this feature using the CLI, Web management interface.
Ability to enter Privileged EXEC Mode After a Telnet or SSH Login	By default, you enter User EXEC mode after a successful login through Telnet or SSH. Optionally, you can configure the device so that you enter Privileged EXEC mode after a Telnet or SSH login.
Telnet/SSH login prompt obtained from TACACS+ server	When TACACS+ authentication is configured, the HP device now obtains from the TACACS+ server the login prompt, password prompt, as well as any other prompts specified by the TACACS+ server.
Users can be prompted for Enable or Line password when TACACS+ server is unavailable	If a user attempts to login through Telnet or SSH, but none of the configured TACACS+ servers are available, the user can be prompted for the Enable or Line password if these methods are specified after TACACS+ in the authentication-method list.
Command authorization and accounting for console commands	The device now supports command authorization and command accounting for CLI commands entered at the console.
Backplane debugging commands	For debugging purposes, you can monitor information about the backplane hardware on a Chassis device.

Enhancement	Description
New RSVP diagnostic commands	RSVP diagnostic commands display information about RSVP messages sent and received on the device.
Enhancement to BGP diagnostic command	The **debug ip bgp update** command can display debugging output for a specified IP prefix list.
Dynamic link aggregation	You can enable ports for IEEE 802.3ad link aggregation, a protocol that allows ports to automatically negotiate trunk group configuration with other devices.
Private VLANs	You can configure highly secure VLANs within port-based VLANs for very tight access control between ports.
Dual mode VLAN ports	You can configure a tagged port as a ***dual-mode*** port, which allows it to accept and transmit both tagged traffic and untagged traffic at the same time.
Configurable link hold-down timer	You can specify how many milliseconds you want the software to wait before bringing up a specific port following a software reload.
Dynamic configuration loading	You can load dynamic configuration commands from a configuration file on a TFTP server into the device's running-config. **Note**: This enhancement applies only to commands that do not require a software reload to take effect.
Rate limiting for ARP packets	You can limit the number of ARP packets the HP device receives each second.
New CLI command to display detailed Spanning Tree Protocol (STP) information	The **show span detail** command displays detailed STP information for each port on the device.
Enhancement to **show vlan** command	The **show vlan** command orders the display of VLANs according to VLAN ID. In previous software releases, the command displayed the VLANs according to the order in which they were configured.
TACACS+ Exec authorization supports non-HP A-V pairs	To set a user's privilege level using a TACACS+ server, the HP device can accept either a HP-specific A-V pair or a non-HP-specific A-V pair.
Option to specify different servers for individual AAA functions	In a RADIUS or TACACS+ configuration, you can designate a server to handle a specific AAA task.
Encryption of RADIUS and TACACS keys	When you display the configuration of the HP device, the RADIUS and TACACS keys are encrypted.
New HP MIB objects for CPU utilization statistics	You can use SNMP to get average CPU utilization statistics for the latest one-second, five-second, and one-minute intervals.
Higher maximum number of VLANs allowed in a spanning tree	You can configure up to the maximum number of port-based VLANs allowed on a device to be members of a single instance of the Spanning Tree Protocol (STP). Previously, you could configure up to 128 VLANs to use the same spanning tree.
Dynamic link aggregation	You can enable ports for IEEE 802.3ad link aggregation, a protocol that allows ports to automatically negotiate trunk group configuration with other devices.
Private VLANs	You can configure highly secure VLANs within port-based VLANs for very tight access control between ports.

Enhancement	Description
Dual mode VLAN ports	You can configure a tagged port as a ***dual-mode*** port, which allows it to accept and transmit both tagged traffic and untagged traffic at the same time.
Configurable link hold-down timer	You can specify how many milliseconds you want the software to wait before bringing up a specific port following a software reload.
Dynamic configuration loading	You can load dynamic configuration commands from a configuration file on a TFTP server into the device's running-config. **Note**: This enhancement applies only to commands that do not require a software reload to take effect.
Rate limiting for ARP packets	You can limit the number of ARP packets the HP device receives each second.
New CLI command to display detailed Spanning Tree Protocol (STP) information	The **show span detail** command displays detailed STP information for each port on the device.
Enhancement to **show vlan** command	The **show vlan** command orders the display of VLANs according to VLAN ID. In previous software releases, the command displayed the VLANs according to the order in which they were configured.
TACACS+ Exec authorization supports non-HP A-V pairs	To set a user's privilege level using a TACACS+ server, the HP device can accept either a HP-specific A-V pair or a non-HP-specific A-V pair.
Option to specify different servers for individual AAA functions	In a RADIUS or TACACS+ configuration, you can designate a server to handle a specific AAA task.
Encryption of RADIUS and TACACS keys	When you display the configuration of the HP device, the RADIUS and TACACS keys are encrypted.
Enhancement to **ptrace snmp** command	The command now lists the SNMP portion of all incoming SNMP packets.

In addition, this release has a change to the CLI. The global CONFIG level of the CLI no longer lists the **perf-mode** command. This command is not used on Chassis devices.

Known Issues

Known Issues in Release 07.5.04

This software release contains the following issues.

- **Mini-GBIC ports** – Hewlett-Packard offers and supports only mini-GBICs that include an HP label (with product number J4858A, J4859A, or J4860A) for use with the J4856A HP ProCurve 9300 Mini-GBIC Module and the J4857A HP ProCurve 9300 Mini-GBIC Redundant Management Module. Use of other brands of mini-GBICs is not supported.
- **AppleTalk** – Appletalk does not work when the dual-mode VLAN feature (**dual-mode** command) is enabled on an interface.
- **Jumbo packet support** – The default MTU of Ethernet interfaces will be displayed as 1500 bytes even if jumbo support is enabled. This is a display issue only and does not affect the operation of the jumbo packet support.
- **CLI display of ACLs** – The **show access-list all** command does not display more than around 300 ACL entries. If your configuration contains more ACL entries than this, not all of the ACL entries are displayed by the command.

- **Upgrade to 07.5.x in Boot Monitor Mode** – This operation fails over a fiber gigabit interface when the routing switch port is set to (the default) 1000 full-duplex and is connected to a switch port configured for Auto. Change the switch port configuration to 1000 full-duplex. If the upgrade still fails, the problem may be due to a software feature on the switch (such as LACP or RSTP) creating latency that allows the routing switch port to time-out before the upgrade can begin. In this case, use a 10/100 link or a Gigabit copper link to perform the upgrade. For information on upgrading to release 07.5.x, refer to “Upgrading the Flash Code” on pages 5 through 8.

Single STP Issues When Migrating from 06.6.*x* to 07.5.*x* or Greater

Overview

Software releases 07.x support up to 4095 port-based VLANs in a single spanning tree. This support required a change to the position of the port-based VLAN commands in the running-config and startup-config file.

- In software release 06.6.*x*, the VLAN commands are placed before the **spanning-tree single** command.
- In the 07.*x* software releases, the **spanning-tree single** command is placed before the VLAN configuration commands.

As a result of the changed command positions, if you boot a device using software release 07.5.x but also load a startup-config file created using software release 06.6.x, the CLI parser does not find the **spanning-tree single** command before the VLAN commands. The parser therefore assumes that the single STP feature is not enabled. When the device finishes booting, the device contains a separate spanning tree for each VLAN on which STP is enabled, instead of a single spanning tree consisting of all the VLANs on which STP is enabled.

Migration Procedure

NOTE: You need to use this procedure only if you are upgrading a device running software release 06.6.x (and using single STP) to the 07.x software releases.

To migrate your single STP configuration from 06.6.*x* to 07.5.*x*:

- Make a backup copy of the startup-config file. You will need this file if you decide to revert to the 06.6.*x* release for any reason.
- Boot the device using software release 07.5.*x*.
- Disable single STP.
- Enable STP (not single STP) in each of the port-based VLANs that you want to include in the single spanning tree.
- Enable single STP.
- Save the configuration. You cannot use the configuration you saved using 06.6.*x* on a device running 07.*x*.

Saving a Backup Copy of the Service’s Startup-Config File

1. Make sure the device has IP access to a TFTP server.
2. Enter one of the following commands at the Privileged EXEC level of the CLI to copy the device’s startup-config file onto the TFTP server:
   - **copy startup-config tftp** <ip-addr> <filename>
   - **ncopy startup-config tftp** <ip-addr> <from-name>

Completing the Migration

1. Boot the device using software release 07.5.*x*.
2. Enter the following command at the global CONFIG level of the CLI to disable single STP:
   - **no spanning-tree single**
3. Enable STP within the port-based VLANs that will be members of the single spanning tree. When you re-enable single STP, all the VLANs in which you enabled STP will become members of the single spanning tree. Other VLANs (in which STP is disabled), will not become part of the single spanning tree.

To enable STP in a VLAN, enter the following command at the global CONFIG level of the CLI to exchange the CLI to the configuration level for that VLAN:

- **vlan** <vlan-id>

To enable STP within the VLAN, enter the following command:

- **spanning-tree**

4. Enable single STP. To do so, enter the **exit** command to return to the global CONFIG level of the CLI, then enter the following command to enable single STP:

   - **spanning-tree single**

5. Save the configuration changes to the startup-config file.
6. Reload the 075.*x* software.

NOTE: When you reload, use the startup-config file you saved in Step 5. If you try to use a startup-config file saved while running 06.6.*x*, the single STP configuration will not be loaded.

HP Part Number: 5990-3049
Edition 1, July 2002