Doc. No. 78-2883-04

Upgrading the Boot ROM on the RSP2 and Initializing the HSA Feature

Product Number RSP2-ROMMON=

This configuration note discusses the procedures required to replace the boot read-only memory (ROM) device on the Route Switch Processor (RSP2) in Cisco 7507 and Cisco 7513 routers and to initialize the high system availability (HSA) feature.

The HSA feature allows two RSP2s to be used simultaneously in a Cisco 7507 or Cisco 7513 router. One RSP2 operates as system *master* and the other RSP2 operates as the system *slave*, which takes over if the master RSP2 fails.

The boot ROM device for the RSP2 is an erasable programmable read-only memory (EPROM) device located in socket U30 on the RSP2, and is a dual in-line package (DIP).

Caution Changing the boot ROM device on the RSP2 will make your current configuration file stored in nonvolatile random-access memory (NVRAM) unreadable and unusable. If you *do not* save the system configuration file before changing the boot ROM, you must then use the **configure** command or the **setup** command facility to reenter the configuration information after the RSP2 is reinstalled. We recommend that you save the system configuration file to a Trivial File Transfer Protocol (TFTP) server or a Flash memory card *before* you replace the boot ROM. Refer to the section "Saving and Retrieving the Configuration File" on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure.

Important Note The newer boot ROM (also called the *system bootstrap*) version uses a different memory size for its configuration. If you are upgrading to the newer boot ROM (system bootstrap) version that uses a different memory size for its configuration, you may lose the environment variable settings.

We recommend that you make a note of your current environment settings, then reset them after restarting the system. Use the **show boot** command to display these settings.

If you want to boot a different Cisco IOS image after the boot ROM upgrade (as in the case of the HSA upgrade), disable any automatic system booting function if you have one enabled.

Note *Specific instruction for complete HSA configuration is beyond the scope of this publication.*

If you want to configure the HSA feature, refer to the configuration note *Route Switch Processor (RSP2) Installation and Configuration* (Document Number 78-2026-06 or later), or to the Cisco IOS release notes and *Configuration Fundamentals Configuration Guide* and *Configuration Fundamentals Command Reference* publications for your HSA-compatible Cisco IOS version. All publications are available on the Cisco Connection Documentation, Enterprise Series CD-ROM, Cisco's online library of product information, or as printed copies.

Order of Procedures for the Boot ROM Upgrade and HSA Initialization

Following is the recommended order for the procedures you need to perform to replace the boot ROM device and then initialize the HSA feature:

1. Ensure you have what you need to upgrade the boot ROM device, then review electrostatic discharge prevention requirements. Refer to the sections "Tools and Parts Required" and "Preventing Electrostatic Discharge Damage" on page 3.
2. Ensure that you understand all of the requirements for the boot ROM upgrade and HSA initialization. Refer to the section "Software and Hardware Prerequisites" on page 4.
3. Verify which Cisco IOS release is currently installed (must be Cisco IOS Release 11.1[4] or later) and the system bootstrap version currently installed on your RSP2s (must be System Bootstrap Version 11.1[2] or later). Refer to the section "Determining Your Current Cisco IOS Release and System Bootstrap Version" on page 5.

Note You will boot the RSP2 in the even-numbered slot with HSA-compatible Cisco IOS image.

4. Save the configuration file on the RSP2 on which you want to install the new boot ROM (system bootstrap) version; save the configuration file to a TFTP server. Use the appropriate procedure in the section "Saving and Retrieving the Configuration File," which begins on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure.
5. Upgrade the boot ROM device (RSP2-ROMMON) on all RSP2s as required, and reinstall the RSP2s. Refer to the section "Upgrading the Boot ROM Device" on page 9.
6. Restart the router and initialize the HSA feature. Refer to the section "Restarting the System and Initializing the HSA Feature" on page 17.
7. Verify that the HSA feature is properly initialized. Refer to the section "Verifying that the HSA Feature is Properly Initialized" on page 22.
8. Restore (retrieve) the saved configuration files from the TFTP server. Use the appropriate procedure in the section "Saving and Retrieving the Configuration File, " which begins on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure.

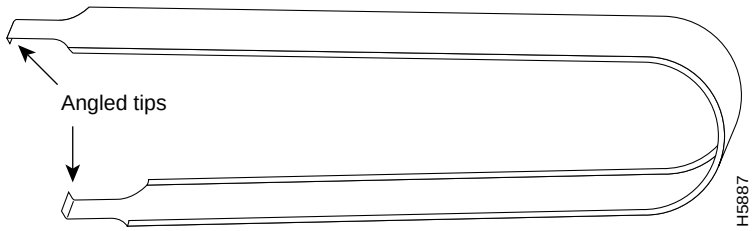
Note If you require technical assistance, refer to note at the end of the section "Cisco Connection Online" on page 34.

Tools and Parts Required

The procedures for replacing the boot ROM and initializing HSA require the following tools and parts. (Also refer to the section "Software and Hardware Prerequisites," on page 4, for specific RSP2 DRAM requirements.)

- A DIP-type integrated circuit (IC) removal tool (see Figure 1) or a small flat-blade screwdriver; to prevent damage to the boot ROM device and your RSP2 the IC removal tool is recommended.

Figure 1 IC Removal Tool



- Antistatic foam or an antistatic mat on which to lay the removed RSP2 while you replace the boot ROM device
- A number 2 Phillips screwdriver and a 3/16-inch flat-blade screwdriver
- Small needlenose pliers
- At least one terminal for connection to the master RSP2's console port

Note A console connection is required for HSA initialization because the boot ROM replacement procedure causes the configuration to be lost.

- An HSA-compatible Cisco IOS release (Refer to the section "Software and Hardware Prerequisites," on page 4, for specific requirements.)
- A boot ROM (RSP2-ROMMON=) version compatible with the Cisco IOS release currently running on your router or that is compatible with the Cisco IOS release that supports HSA. (Refer to the section "Software and Hardware Prerequisites," on page 4, for specific requirements.)

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It occurs when electronic components are improperly handled and can result in intermittent or complete failures. Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. To safely channel unwanted ESD voltages to ground, connect the clip to an unpainted surface of the chassis frame. If no wrist strap is available, ground yourself to the metal chassis.

Caution For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohms.

Software and Hardware Prerequisites

For the high system availability (HSA) feature to operate properly, the following prerequisites must be observed:

- You must have Cisco IOS Release 11.1(4), or later, installed.

Note For HSA compatibility, you need a Cisco IOS subset image that has a "v" in it. For example, *rsp-jv-mz rsp-ajv-mz*, and *rsp-pv-mz* are all HSA-compatible Cisco IOS subset images. Cisco IOS subset images are available from Cisco Connection Online; refer to the section "Cisco Connection Online" on page 34.

- You must have RSP2 boot ROM (system bootstrap) Version 11.1(2), or later, installed on each RSP2 in the router.
- Both RSP2s require the same boot-ROM version and the same DRAM configuration (24-MB DRAM at a minimum)
- Versatile Interface Processors (VIPs) and second-generation Versatile Interface Processors (VIP2s) can be used in Cisco 7507 and Cisco 7513 routers configured for HSA, if the Cisco 7507 or Cisco 7513 routers are running Cisco IOS Release 11.1(6)CA or later.
- For the initial release of the HSA feature, online insertion and removal (OIR) of the slave RSP2 is not recommended.

Note The master RSP2 must *never* be removed while the system is operating. The are no specific code requirements for the boot image (rsp-boot-xxx.x) and the HSA feature.

Caution Replacing the boot ROM on your RSP2 will make your current configuration file stored in NVRAM unreadable and unusable. Before removing the RSP2 and installing the new boot ROM, you must save your configuration file to a TFTP server or a Flash memory card on your RSP2, and then retrieve it after the new boot ROM is installed. Refer to the section "Saving and Retrieving the Configuration File" on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure.

Important Note The newer boot ROM (system bootstrap) version uses a different memory size for its configuration. If you are upgrading to the newer boot ROM (system bootstrap) version that uses a different memory size for its configuration, you may lose the environment variable settings.

We recommend that you make a note of your current environment settings, then reset them after restarting the system. Use the **show boot** command to display these settings.

If you want to boot a different Cisco IOS image after the boot ROM upgrade (as in the case of the HSA upgrade), disable any automatic system booting function if you have one enabled.

With HSA operation, the following items are important to note:

- An RSP2 card that acts as the slave runs a different Cisco IOS software version than it does when it acts as the master. The slave mode software is a subset of the master mode software; both are bundled with the Cisco IOS software.
- The two RSP2 cards do not have to run the same master software image and configuration file. When the slave reboots the system and becomes the new master, it uses its own system image and configuration file to reboot the router.
- When enabled, automatic synchronization mode (slave auto-sync config) automatically ensures that the master and slave RSP2 card have the same configuration file and is the default condition. This synchronization occurs when you issue the **copy running-config startup-config** or **write memory** commands.
- The default system master slot is the even-numbered RSP slot: slot 2 in the Cisco 7507 and slot 6 in the Cisco 7513.
- The master RSP2 has access to read or write the slave's Flash memory devices.

Caution To ensure that the slave RSP2 will operate properly with the full system configuration should the master RSP2 ever fail, the slave RSP2 should have the same DRAM configuration as that of the master RSP2.

Note The minimum required DRAM configuration for the RSP2s in your system is 24 MB.

- Both hardware and software failures can cause the master RSP2 to enter a nonfunctional state; but, the system does not indicate the type of failure.
- When using the console Y-cable, the master RSP2 is the only device viewed. To view both master and slave, a separate console terminal connection is required for each master and slave; without the Y-cable.

Caution Removing the system master RSP2 while the system is operating will cause the system to crash; however, the system *will* reload with the slave RSP2 as the new system master. To prevent any system problems, *do not* remove the system master RSP2 while the system is operating.

Determining Your Current Cisco IOS Release and System Bootstrap Version

The HSA feature requires Cisco IOS Release 11.1(4), or later, and System Bootstrap Version 11.1(2) or later. Your system might already be running System Bootstrap Version 11.1(2). Use the **show version** command to display the system bootstrap version currently running on the RSP2(s) in your Cisco 7507 or Cisco 7513.

Note Only the master RSP2 (installed in the even-numbered RSP slot) needs to be running Cisco IOS Release 11.1(4) or later. The appropriate Cisco IOS image is copied from the master to the slave; this procedure is discussed later in this configuration note.

Following is sample output of the **show version** command. (Take special note of the display lines preceded by >>. These lines indicate the Cisco IOS release and system bootstrap version currently running on your system.)

```
Router> show version

Cisco Internetwork Operating System Software
>> IOS (tm) GS Software (RSP-JV-M), Version 11.1(4) [biff 51096]
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 22-Jan-96 21:15 by biff
Image text-base: 0x600108A0, data-base: 0x607B8000
(additional displayed text omitted)

>> ROM: System Bootstrap, Version 11.1(2) [biff 2], RELEASE SOFTWARE (fc1)
ROM: GS Bootstrap Software (RSP-BOOT-M), Version 10.3(7), RELEASE SOFTWARE

Router uptime is 85 hours, 39 minutes
System restarted by reload
System image file is "slot0:rsp-jv-mz.111-4", booted via slot0

cisco RSP2 (R4600) processor with 81920K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
```

Installing the Correct Cisco IOS Release

If you determine that your Cisco IOS release is not Cisco IOS Release 11.1(4) or later, you need install the correct Cisco IOS release on the Flash memory card installed in PCMCIA slot 0. The following sections describe the procedures for copying a new Cisco IOS image to the Flash memory cards in the PCMCIA slots on your RSP2.

Copying a Cisco IOS Image from a TFTP Server to a Flash Memory Device

Following is the procedure for copying a Cisco IOS image to Flash memory. While there are several methods for copying Cisco IOS images from a TFTP server to a Flash memory device, the following method is recommended. Press **Return** after each command.

Step 1 Using the **cd** command, change directory to the Flash memory device on which you want the new Cisco IOS image to be stored, as follows:

```
Router# cd slot0:
```

Step 2 Verify that the Flash device is present and was correctly selected, as follows:

```
Router# pwd
slot0
```

Step 3 Using the **dir** command, verify that the Flash memory device has enough unused memory space for the new file, as follows:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  Jul 11 1996 19:24:12 rsp-jv-mz.111-4
2   1186     Jul 12 1996 16:56:50 myfile2
3   3591664  Jul 12 1996 18:43:42 rsp-k-mz.103-12
5   512      Jul 12 1996 19:05:50 myfile1

11784216 bytes available (8794088 bytes used)
```

Step 4 Use the **copy tftp flash** command to copy a Cisco IOS image from the TFTP server to the present Flash memory device, as follows:

```
Router# copy tftp flash slot0:
Enter source file name: rsp-jv-mz.111-4.2
Enter destination file name [rsp-jv-mz.111-4.2]:
11784088 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [255.255.255.255]? 1.1.1.1
Accessing file "rsp-jv-mz.111-4.2" on 1.1.1.1 ...FOUND
Loading rsp-jv-mz.111-4.2 from 1.1.1.1 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6193520/12386304 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

Step 5 Use the **dir** command to verify that the new Cisco IOS image is now present on the Flash memory device, as follows:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  Jul 11 1996 19:24:12 rsp-jv-mz.111-4
2   1186     Jul 12 1996 16:56:50 myfile2
3   3591664  Jul 12 1996 18:43:42 rsp-k-mz.103-12
5   512      Jul 12 1996 19:05:50 myfile1
6   6193520  Jul 14 1996 11:36:20 rsp-jv-mz.111-4.2

5590568 bytes available (14987736 bytes used)
Router#
```

Configuring the System to Boot from the Correct Cisco IOS Image

Following is the procedure for configuring the system to boot from the correct Cisco IOS image stored in the Flash memory device. For HSA compatibility, this is Cisco IOS Release 11.1(4) or later. If the file from which you want to boot is the first file on the Flash memory device in slot 0, no modification is required to boot the new file; use the command **boot system flash**. However, if the file is *not* the first file listed in the Flash memory device, or is on another Flash memory device, you need to modify the configuration file to point to the Flash memory device and to the specific Cisco IOS image filename within it. Configure the system as follows:

Step 1 Enter Configuration mode and issue the **boot system flash** command as follows:

```
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# boot system flash slot0:rsp-jv-mz.111-4.2
Ctrl-Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 2 Save this new configuration to NVRAM using the **copy running-config startup-config** (or **write memory**) command, as follows:

```
Router# copy running-config startup-config
Building configuration...
[OK]
Router#
```

Step 3 To further verify that the system is correctly configured, use the **show boot** command to view the environment settings, as follows:

```
Router# sh boot
BOOT variable = slot0:rsp-jv-mz.111-4.2,1;
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x2

Router#
```

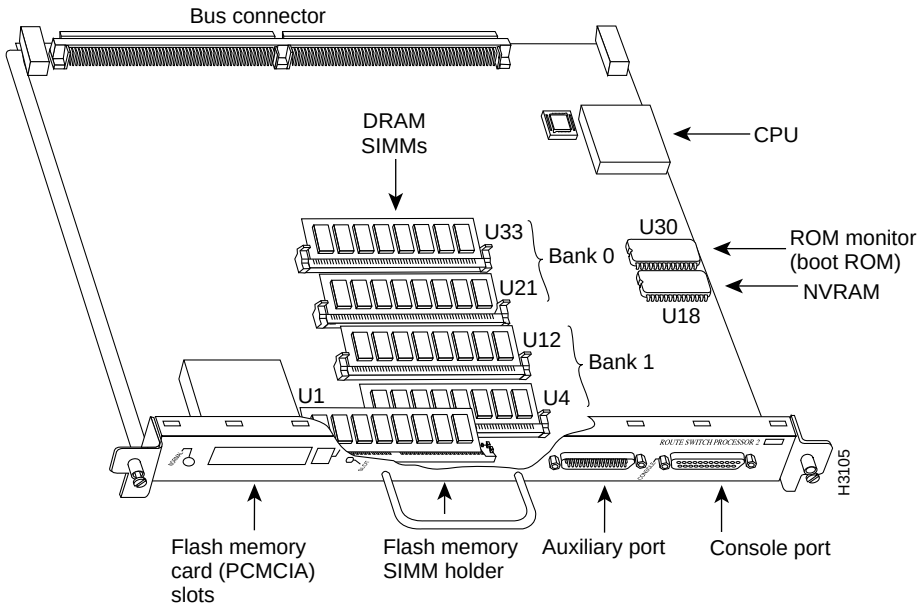
Step 4 Reload the new Cisco IOS image on the system by issuing the **reload** command.

Note Save your configuration file to a TFTP server *before* you proceed with the procedures in the following section "Upgrading the Boot ROM Device."

Upgrading the Boot ROM Device

The boot ROM device is located in socket U30 on your RSP2. (See Figure 2.) Though the RSP slots are numbered differently in the Cisco 7507 and Cisco 7513, the procedures to remove an RSP2, replace the boot ROM device, and reinstall the RSP2 are identical for each chassis. Differences between the Cisco 7507 and the Cisco 7513 are clearly noted. Upgrade both RSP2s if required.

Figure 2 Route Switch Processor (RSP2), Horizontal Orientation Shown



Caution Replacing the boot ROM on your RSP2 will make your current configuration file stored in NVRAM unreadable and unusable. Before removing the RSP2 and installing the new boot ROM, you must save your configuration file to a TFTP server or a Flash memory card on your RSP2, and then retrieve it after the new boot ROM is installed. Refer to the section "Saving and Retrieving the Configuration File" on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure. Refer to the section "Saving and Retrieving the Configuration File" on page 23.

Important Note The newer boot ROM (system bootstrap) version uses a different memory size for its configuration. If you are upgrading to the newer boot ROM (system bootstrap) version that uses a different memory size for its configuration, you may lose the environment variable settings.

We recommend that you make a note of your current environment settings, then reset them after restarting the system. Use the **show boot** command to display these settings.

If you want to boot a different Cisco IOS image after the boot ROM upgrade (as in the case of the HSA upgrade), disable any automatic system booting function if you have one enabled.

Removing the RSP2

Following is the procedure for removing the RSP2:

Step 1 Turn OFF power to the chassis before removing an RSP2.

Note If you remove the RSP2 and do not *first* save the configuration file, you will need to use the **configure** command or the **setup** command facility to reenter all of the configuration information. We recommend that you save the current configuration file stored in NVRAM on the RSP2 to a TFTP server, before you remove the RSP2. Refer to the section "Saving and Retrieving the Configuration File" on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29.

Step 2 Attach an ESD-preventive strap between you and an unfinished chassis surface.

Step 3 Locate the RSP2 that you want to remove for the boot ROM upgrade. The RSP2 slots in the Cisco 7507 are slots 2 and 3 (see Figure 3), and in the Cisco 7513 they are slots 6 and 7. (See Figure 4 on page 11.)

Figure 3 Cisco 7507 with Two RSP2s Installed

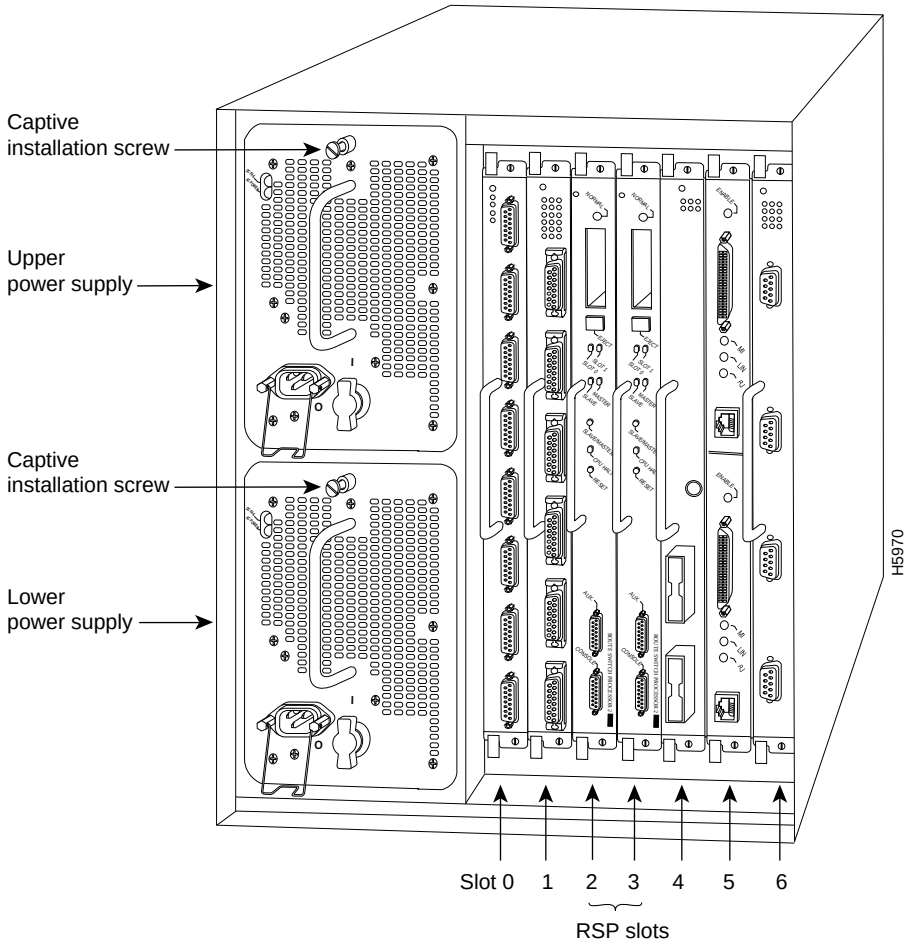
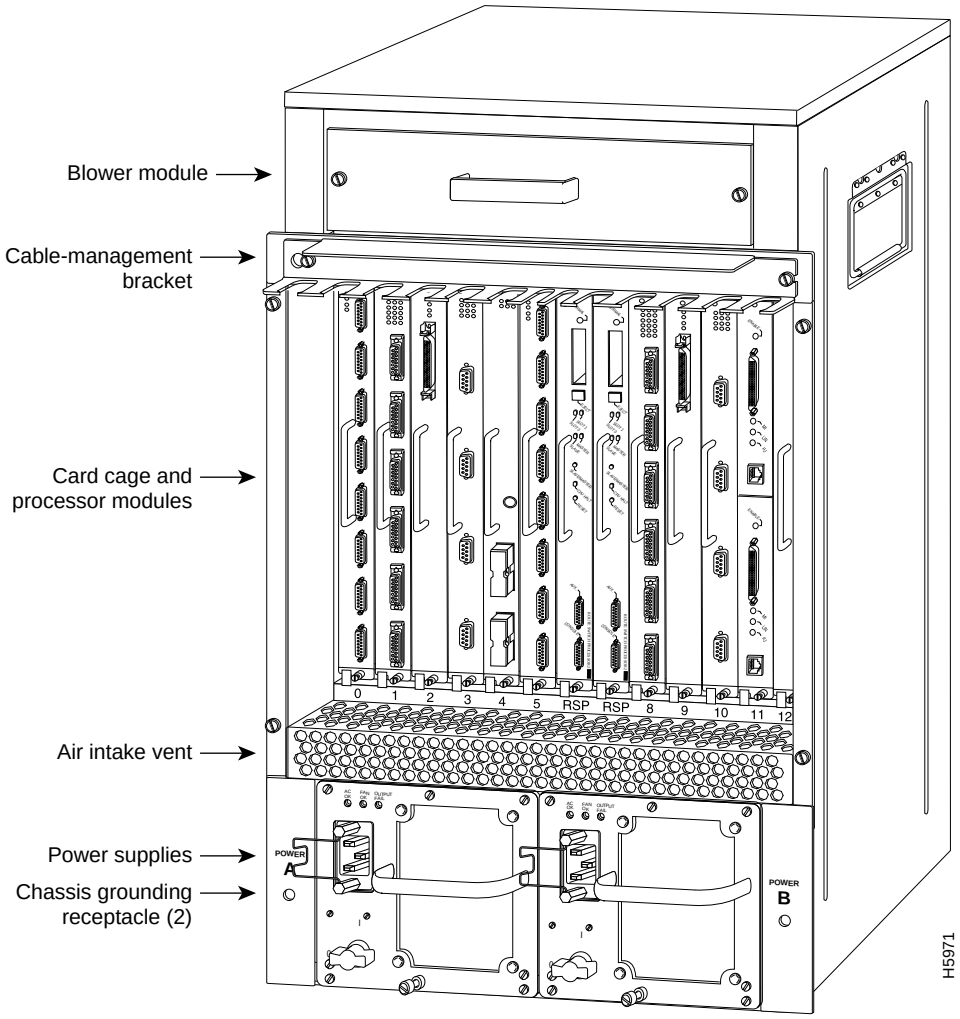


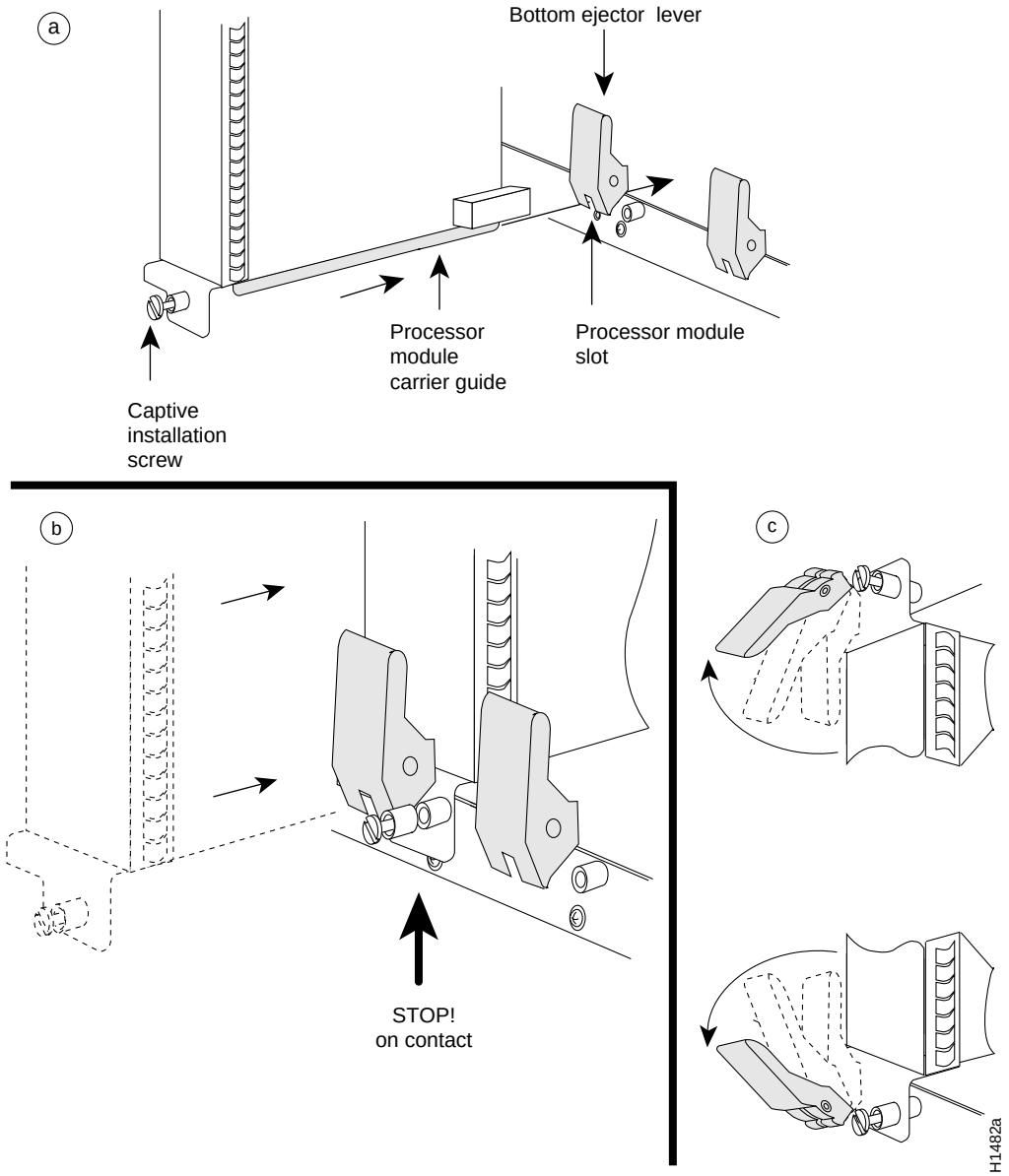
Figure 4 Cisco 7513 with Two RSP2s Installed



Step 4 Disconnect any devices that are attached to the console or auxiliary ports. You can leave the devices attached provided that doing so will not strain the cables.

Step 5 Using a screwdriver (number 2 Phillips or 3/16-inch flat-blade), loosen the two captive installation screws on the RSP2. (See Figure 5a.)

Figure 5 Ejector Levers and Captive Installation Screw



Step 6 Place your thumbs on the ends of each of the ejector levers and simultaneously pull them both outward, away from the carrier handle (in the direction shown in Figure 5c) to release the carrier from the slot and to dislodge the RSP2 from the backplane.

Step 7 Grasp the handle of the RSP2 with one hand and pull the RSP2 straight out of the slot, keeping your other hand under the carrier to guide it. Keep the carrier at a 90-degree orientation to the backplane. Avoid touching the board or any connector pins.

Step 8 Place the removed RSP2 on an antistatic mat or foam.

This completes the RSP2 removal procedure. Proceed to the section “Changing the Boot ROM.”

Changing the Boot ROM

Following is the procedure for upgrading the boot ROM device on the RSP2.

Caution Replacing the boot ROM on your RSP2 will make your current configuration file stored in NVRAM unreadable and unusable. Before removing the RSP2 and installing the new boot ROM, you must save your configuration file to a TFTP server or a Flash memory card on your RSP2, and then retrieve it after the new boot ROM is installed. Refer to the section "Saving and Retrieving the Configuration File" on page 23. If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternative procedure. Refer to the section "Saving and Retrieving the Configuration File" on page 23.

Important Note The newer boot ROM (system bootstrap) version uses a different memory size for its configuration. If you are upgrading to the newer boot ROM (system bootstrap) version that uses a different memory size for its configuration, you may lose the environment variable settings.

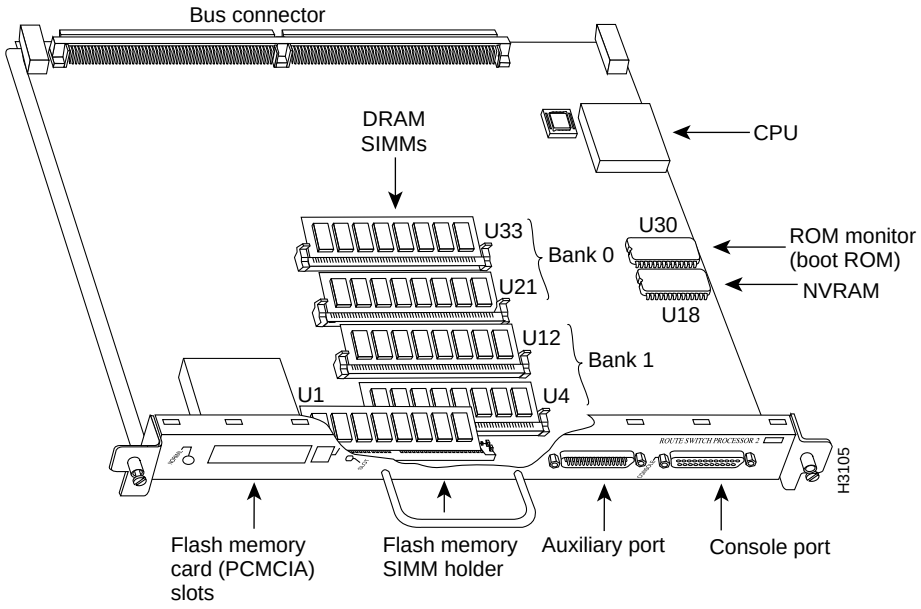
We recommend that you make a note of your current environment settings, then reset them after restarting the system. Use the **show boot** command to display these settings.

If you want to boot a different Cisco IOS image after the boot ROM upgrade (as in the case of the HSA upgrade), disable any automatic system booting function if you have one enabled.

Step 1 Attach an ESD-preventive strap between you and any unpainted chassis surface.

Step 2 With the RSP2 lying flat on an antistatic mat or foam, refer to Figure 6 and locate the boot ROM device, which is located at U30 along the right edge of the RSP2 then locate this device on your RSP2.

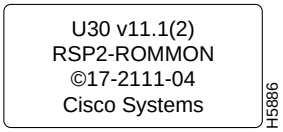
Figure 6 Boot ROM Location on RSP2



Step 3 Carefully remove the new boot ROM from its packaging and, referring to Figure 7, verify that the new boot ROM (RSP2-ROMMON, Version 11.1[2] or later) is the correct boot ROM (system bootstrap) version for this upgrade. Return the new boot ROM to its packaging.

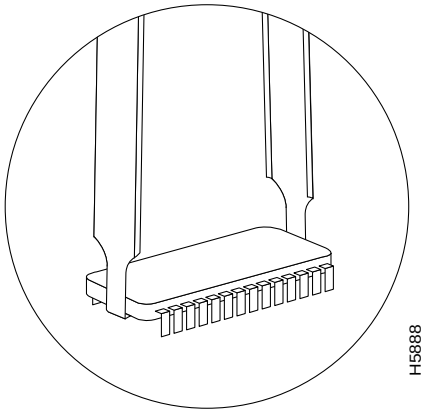
Note The boot ROM part number (17-2111-04), which is shown on the boot ROM label in Figure 7, is the minimum required version (-04) for HSA compatibility.

Figure 7 Boot ROM Label—Boot ROM Version 11.1(2) for Initial HSA Compatibility



Step 4 Place the angled tips of the IC removal tool beneath the ends of the boot ROM. (See Figure 8.)

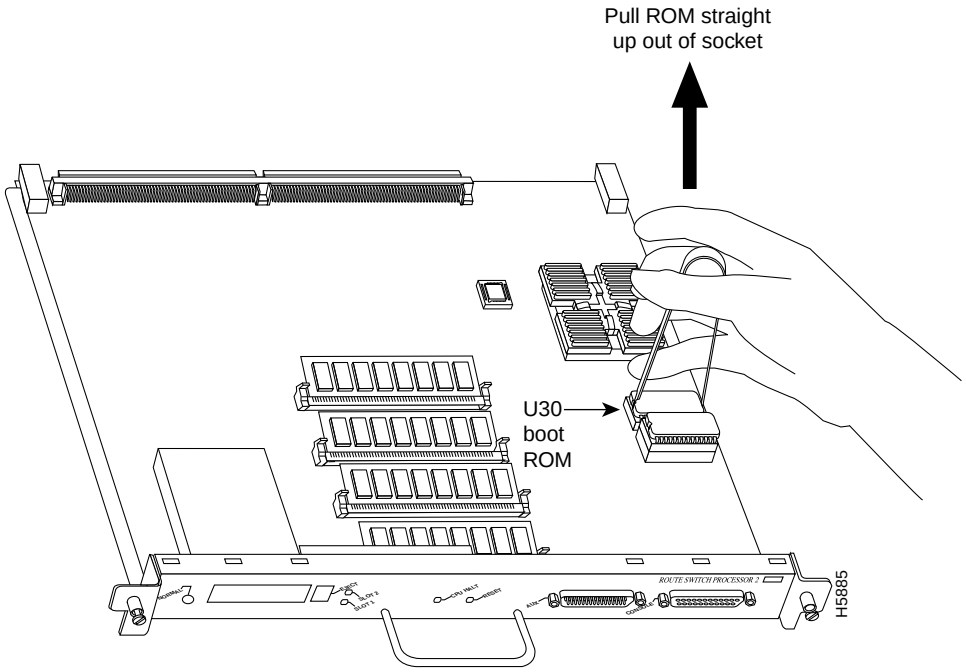
Figure 8 Enlargement of the IC Removal Tool and Boot ROM



Step 5 Squeeze the arms of the IC removal tool and gently, but firmly, pull up on the boot ROM until its pins are clear of the socket. Apply even pressure to both tips of the IC removal tool. (See Figure 9.) It might be necessary to gently rock the IC removal tool and boot ROM end to end until the boot ROM is free of the socket.

Caution To prevent bent pins, pull the boot ROM straight up and out of its socket.

Figure 9 Using the IC Removal Tool to Remove the Boot ROM



Step 6 Set the old boot ROM aside (preferably in an antistatic bag), and remove the new boot ROM device from its packaging.

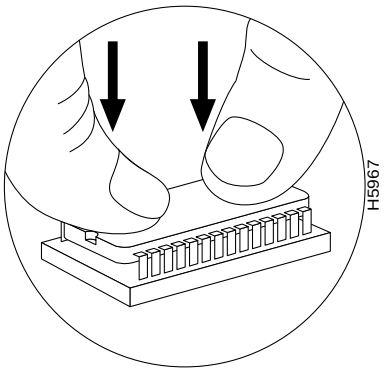
Step 7 Align the new boot ROM with the U30 socket, and note the notch at the end of the socket and boot ROM. Match the notch at the end of the boot ROM with the notch on the socket.

Caution If the boot ROM notch is not aligned with the socket notch, the boot ROM will be destroyed when power is turned on.

Step 8 Applying pressure evenly, gently press the boot ROM's pins into the holes in the U30 socket. (See Figure 10.) Take care not to bend any pins. You can straighten bent pins using a small needlenose pliers; however, a broken pin means that the boot ROM is unusable, and you must order a new one.

Caution To prevent bent pins, push the boot ROM straight down into its socket, applying pressure evenly.

Figure 10 Inserting the Boot ROM into the U30 Socket



Step 9 When you have inserted the new boot ROM all the way into its socket, check around the boot ROM for any bent pins.

Step 10 Repeat Step2 1 through 9 for the second RSP2 as required.

If any pins are bent, remove the boot ROM, use the needlenose pliers to straighten the pins, and reinsert the boot ROM using steps 7 through 9. Note that a broken pin means that the boot ROM is unusable, and you must order a new one.

If all pins are inserted correctly and the boot ROM notch is aligned with the socket notch, the boot ROM is properly installed. Proceed to the section "Replacing the RSP2."

Replacing the RSP2

The RSP2 is keyed for installation only in an RSP2 slot. (See Figure 3 for the Cisco 7507 or Figure 4 for the Cisco 7513.) By default, the system master is the RSP2 that occupies the first RSP slot in the chassis—slot 2 in the Cisco 7507, and slot 6 in the Cisco 7513. Install both RSP2s in the chassis as required.

Follow these steps to install an RSP2:

Step 1 Grasp the RSP2 handle with one hand and place your other hand under the carrier edge to support and guide it into the slot. Avoid touching the board or any connectors.

Step 2 Place the back of the RSP2 in the appropriate RSP slot and align the notches along the edge of the carrier with the grooves in the slot. (See Figure 5a.)

Caution To prevent damage to the backplane, you must install the RSP2 in one of the two RSP slots on the chassis. The slots are keyed for correct installation. Forcing the RSP2 into a different slot can damage the backplane and the RSP2. (For the locations of the RSP2 slots on the Cisco 7507, refer to Figure 3; for the location of the RSP2 slots on the Cisco 7513, refer to Figure 4.)

Step 3 While keeping the RSP2 parallel to the backplane, carefully slide the carrier into the slot until the RSP2 faceplate makes contact with the ejector levers, then *stop*. (See Figure 5b.)

Step 4 Using the thumb and forefinger of each hand to pinch each ejector, simultaneously push both ejectors inward (toward the handle) until they are parallel to the faceplate. (See Figure 5c.)

Step 5 Use a screwdriver to tighten the two captive screws on the RSP2 faceplate (see Figure 5a) to prevent the RSP2 from becoming partially dislodged from the backplane and to ensure proper EMI shielding. (These screws must be tightened to meet EMI specifications.)

Step 6 If you disconnected the console terminal to remove the RSP2, connect the console terminal to the console port.

Step 7 Repeat Steps 1 through 6 for the second RSP2, if required.

Step 8 Ensure that the console terminal is turned on.

Step 9 Turn the system power back ON, and proceed to the next section to check the installation.

Restarting the System and Initializing the HSA Feature

When you turn the system power back on, verify that the system boots and resumes normal operation. If you are restarting the system after upgrading the DRAM, expect that it will take the system longer to complete the memory initialization portion of the boot sequence with more DRAM.

Note For HSA compatibility, you need a Cisco IOS subset image that has a "v" in it. For example, *rsp-jv-mz rsp-ajv-mz*, and *rsp-pv-mz* are all HSA-compatible Cisco IOS subset images. Cisco IOS subset images are available from Cisco Connection Online; refer to the section "Cisco Connection Online" on page 34.

Follow these steps to verify that the RSP2 is installed and functioning properly:

Step 1 Ensure that both RSP2s are properly installed in the chassis.

Step 2 Install a Y-cable (CAB-RSP2CON); attach the combined end to your console terminal and each single en to the console connection of each RSP2.

As an alternative, you can install a separate console cable to each RSP2. The master console controls both the master and slave; you can view the slave through the master console connection, but you cannot view the master console from the slave console connection. The following steps are directed to the master RSP2 only.

Step 3 Check all RSP2 connections to make sure they are secure:

- The RSP2s are inserted all the way into their slots, and both the captive installation screws are tightened on each RSP2.
- The console terminal is turned on and is connected to the console port.

Step 4 Observe the RSP2 LEDs on system startup. While the system initializes, the yellow CPU halt LED on each RSP2 will blink when power is applied. The normal LED on the master RSP2 in slot 6 should be on and the normal LED on the slave RSP2 in slot 7 should be on. The master LED on the RSP2 in slot2 or slot 6 will be on and the slave LED on the RSP2 in slot 3 or slot 7 will be on. As each interface processor initializes, their status LEDs go on and off in irregular sequence.

Note If you did not install a boot ROM device correctly, the corresponding RSP2 is placed in a "nonparticipant" mode and *both* of its slave and master LEDs will be on. This can be caused by a bent boot ROM pin, a misaligned boot ROM, or a misprogrammed boot ROM. If this condition occurs, power down the system and verify that the boot ROM device is installed. If the boot ROM device was installed backwards, severe damage may have resulted rendering the boot ROM device unusable. You will have to install a new boot ROM device.

Step 5 Verify that the master console terminal displays the correct system banner and startup screen as the system restarts. For a Cisco 7513, the master console display should look similar to the following (note the RSP2 slots preceded by >> in this example):

```
(additional displayed text omitted from this example)

Warning: monitor nvram area is corrupt ... using default values
>> SLOT 6 RSP2 is system master
>> SLOT 7 RSP2 is system slave
RSP2 processor with 81920 Kbytes of main memory

rommon 1 >
```

For a Cisco 7507, the master console display should look similar to the following (note the RSP2 slots indicated):

```
(additional displayed text omitted from this example)

Warning: monitor nvram area is corrupt ... using default values
>> SLOT 2 RSP2 is system master
>> SLOT 3 RSP2 is system slave
RSP2 processor with 81920 Kbytes of main memory

rommon 1 >
```

Note The warning message in each of the preceding displays appears whenever the boot ROM device is replaced and is to be expected.

Step 6 At the ROM monitor prompt, issue the **sync** boot ROM command to write the ROM monitor environment to NVRAM, as follows:

```
rommon 1 > sync
```

Step 7 Verify that the correct HSA-compatible Cisco IOS image resides in Flash memory by issuing the **dir** *device:* command, where *device:* can be bootflash:, slot0:, or slot1:. An example follows:

```
rommon 1 > dir slot0:
         File size            Checksum      File name
   5200084 bytes (0x4f58d4)   0x827a9ae5    rsp-jv-mz.111-4
      1176 bytes (0x498)      0xc9ea46ce    myfile1 (deleted)
      1215 bytes (0x4bf)      0x4b30dc00    myfile1
   6176844 bytes (0x5e404c)   0x66180376    rsp-jv-mz.111-472
rommon 2 >
```

Note Files marked as deleted are not bootable files. You can undelete a file when the system in running a Cisco IOS image or a boot image.

Step 8 Boot the appropriate HSA-compatible Cisco IOS subset image using the **boot slot0:***filename* command., as follows:

```
rommon 2 > boot slot0:rsp-jv-mz.111-4
```

The system will boot up and automatically enable the HSA defaults.

Step 9 After the system boots the Cisco IOS image and initializes the interface processors (approximately 30 seconds for systems with 16 MB of DRAM, and approximately 2 minutes for systems with 64 MB of DRAM), verify that the RSP2 LEDs are in the following states:

- RSP2 normal LEDs are on
- CPU halt LEDs are off
- Slot 2 or 6 master RSP2 LED is on
- Slot 3 or 7 slave RSP2 LED is on

You should see the following screen banner displayed:

```
Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-JV-M), Version 11.1(4) RELEASE SOFTWARE
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 17-Jun-96 21:15 by biff
Image text-base: 0x600108A0, data-base: 0x60864000

[additional displayed text omitted from this example]
```

Note When the router first boots, the slave will be in a halted mode. This will change immediately after the system completes the boot process.

Step 10 Enable EXEC command mode by using the **enable** command and your enable secret password.

Note If the configuration was removed, no password prompt will appear.

Step 11 If you have a second RSP2 installed, use the **show version** command to verify that the slave RSP2 is recognized by the system. Following is a sample from a Cisco 7513. (Take special note of the line preceded by >>.)

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-JV-M), Version 11.1(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 17-Jun-96 16:14 by biff
Image text-base: 0x600108A0, data-base: 0x60864000

ROM: System Bootstrap, Version 11.1(2) [biff 2], RELEASE SOFTWARE (fc1)

Router uptime is 6 minutes
System restarted by reload
System image file is "slot0:rsp-jv-mz.111-4", booted via

cisco RSP2 (R4600) processor with 81920K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
Last reset from power-on
G.703/E1 software, Version 1.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
Chassis Interface.

[additional displayed text omitted from this example]

123K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

>> Slave in slot 7 is running Cisco Internetwork Operating System Software
IOS (tm) GS Software (RSP-DW-M), Version 11.1(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 17-Jun-96 16:15 by biff
Loaded from system

Configuration register is 0x100
```

An error condition exists if no LEDS go on at power up or after initialization, or if both slave and master LEDS on an RSP2 stay on.

Step 12 The boot ROM replacement automatically changes the configuration register setting to 0x100. To operate correctly, you must change the configuration register setting to 0x102, so you can boot a Cisco IOS image from a Flash memory device (slot0: or slot1:). Change the configuration register setting using the **config-register** command as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# config-register 0x102
Ctrl-Z
Router#
```

You can verify that the configuration register will change to 0x102 on the next router reload by viewing the last line of the output from the **show version** command, which appears as follows:

```
Configuration register is 0x100 (will be 0x102 at next reload)
```

Step 13 Restore your saved configuration file to NVRAM. Refer to the appropriate procedure in the section “Saving and Retrieving the Configuration File” on page 23. If you saved your configuration file on a Flash memory card, refer to the section “Copying a Configuration File from a Flash Memory Card to RSP2 NVRAM” page 31. Then proceed to the section “Verifying that the HSA Feature is Properly Initialized” on page 22.

Amend the configuration file to boot the HSA-compatible Cisco IOS image on the slave RSP2 by copying the HSA-compatible Cisco IOS image to the Flash memory device on the slave RSP2. (The Flash memory device can be **bootflash:**, **slot0:**, or **slot1:**, but **slot0:** is used in the following examples.) Proceed as follows:

Step 1 Verify whether or not the HSA-compatible Cisco IOS image file exists on the slave’s Flash memory card in PCMCIA slot 0 using the **dir slaveslot0:** command as follows:

```
Router# dir slaveslot0:
-#- -length- -----date/time------ name
1   2132     May 16 1996 13:38:12 matt-confg
2   6176844  Jul 01 1996 14:05:49 rsp-jv-mz.111-472
3   3591664  Jul 11 1996 15:49:23 rsp-k-mz.103-12
4   887      Jul 11 1996 18:17:03 myfile
5   5200084  Jul 11 1996 19:45:47 rsp-j-mz.111-1

1411748 bytes available (14972252 bytes used)
Router#
```

If the file does not exist *and* you do not have enough space available on the slave’s Flash memory card, delete a file, using the delete command, then remove the file marked for deletion using the **squeeze** command as follows. (For descriptions of the **delete** and **squeeze** commands, and other Flash memory commands, refer to the section “Additional Flash Memory Commands” on page 32.)

```
RSP-6# del slaveslot0:rsp-j-mz.111-1
RSP-6# squeeze slaveslot0:
All deleted files will be removed, proceed? [confirm]
Squeeze operation may take a while, proceed? [confirm]

(a few minutes might pass before the following prompt reappears)
Router#
```

If the file does exist, but is not the first file listed in the Flash memory card in PCMCIA slot 0, modify the configuration using the **boot system flash** *device***:***filename* command to specify the file from which to boot the system.

If your slave RSP2 (in slot 7 or slot 3) has the HSA-compatible Cisco IOS image file in the Flash memory card in PCMCIA slot 1, and the master RSP2 (in slot 6 or slot 2) has this file in the Flash memory card in PCMCIA slot 0, you need to modify the configuration using the **boot system flash slot0:***filename* and **boot system flash slot1:***filename* commands.

Step 2 You must now copy the HSA-compatible Cisco IOS image file to the slave’s Flash memory card in slot 0 using the **copy slot0:***filename* **slaveslot0:** command as follows:

```
Router# copy slot0:rsp-jv-mz.111-4 slaveslot0:
6611832 bytes available on device slaveslot0, proceed? [confirm]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCcccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
```

Step 3 When the copy process is complete, use the **dir slave***device***:** command to verify it is in the slave's Flash memory card in PCMCIA slot 0, as follows:

```
Router# dir slaveslot0:
-#- -length- -----date/time------ name
1   2132     May 16 1996 13:38:12 matt-confg
2   6176844  Jul 01 1996 14:05:49 rsp-jv-mz.111-472
3   3591664  Jul 11 1996 15:49:23 rsp-k-mz.103-12
4   887      Jul 11 1996 18:17:03 myfile
5   5200084  Jul 14 1996 12:52:54 rsp-jv-mz.111-4

1411748 bytes available (14972252 bytes used)
Router#
```

Verifying that the HSA Feature is Properly Initialized

Following is the procedure for verifying HSA initialization. Verify that the HSA feature is properly initialized using the **show version** and **show boot** commands. An example from a Cisco 7513 follows. (Take special note of the lines preceded by >>.)

```
Router# show version
Cisco Internetwork Operating System Software
>> IOS (tm) GS Software (RSP-JV-M), Version 11.1(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 17-Jun-96 16:14 by biff
Image text-base: 0x600108A0, data-base: 0x60864000

>> ROM: System Bootstrap, Version 11.1(2) [biff 2], RELEASE SOFTWARE (fc1)

Router uptime is 12 minutes
System restarted by reload
System image file is "slot0:rsp-jv-mz.111-4", booted via

cisco RSP2 (R4600) processor with 81920K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
Last reset from power-on
G.703/E1 software, Version 1.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
Chassis Interface.
1 EIP controller (6 Ethernet).
1 FSIP controller (4 Serial).
PSFAIL: Power supply1 TRIP controller (4 Token Ring).
6 Ethernet/IEEE 802.3 interfaces.
4 Token Ring/IEEE 802.5 interfaces.
4 Serial network interfaces.
123K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

>> Slave in slot 7 is running Cisco Internetwork Operating System Software
>> IOS (tm) GS Software (RSP-DW-M), Version 11.1(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 17-Jun-96 16:15 by biff
Loaded from system

Configuration register is 0x100 (will be 0x102 at next reload)
```

Issue the **show boot** command. An example from a Cisco 7513 follows. (Take special note of the line preceded by >>.)

```
Router# sh boot
BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x100 (will be 0x102 at next reload)

Slave auto-sync config mode is on

>> Current slave is in slot 7.
slave BOOT variable =
slave CONFIG_FILE variable =
slave BOOTLDR variable =
slave Configuration register is 0x102

Router#
```

The HSA feature is now initialized. Refer to the section "Reference Information" for information on specific HSA configuration documentation.

Reference Information

If you need additional troubleshooting information for your Cisco 7507 or Cisco 7513, refer to the *Cisco 7507 Hardware Installation and Maintenance* or *Cisco 7513 Hardware Installation and Maintenance* publications.

If you need to configure the HSA feature for your RSP2, refer to the following publications:

- *Configuration Fundamentals Configuration Guide*
- *Configuration Fundamentals Command Reference*
- *Route Switch Processor (RSP2) Installation and Configuration* (Document Number 78-2026-xx)

All publications are available on the Cisco Connection Documentation, Enterprise Series CD-ROM, Cisco's online library of product information, or as printed copies.

The following sections include information on saving a configuration file to a server, retrieving the configuration file from a TFTP server, copying configuration files between your RSP2's NVRAM and a Flash memory card, and contacting Cisco Systems for additional information or assistance.

Saving and Retrieving the Configuration File

This section describes the procedures for saving (copying) and retrieving the system configuration using a Trivial File Transfer Protocol (TFTP) server.

Note If you do not have access to a TFTP server, refer to the section "Copying Files Between RSP2 NVRAM and a Flash Memory Card," on page 29, for an alternate procedure.

Configuration information resides in two places when the router is operating: the default startup (permanent) configuration in NVRAM, and the running (temporary) configuration in DRAM. The startup configuration always remains available; NVRAM retains the information even when the power is shut down.

The running configuration is lost if the system power is shut down. The startup configuration (in NVRAM) contains all nondefault configuration information that you added with the **configure** command, the **setup** command facility, or by editing the configuration file.

The **copy running-config startup-config** command saves the running configuration to the startup configuration file in NVRAM, so that it will also be saved when power is shut down. Whenever you make changes to the system configuration file, issue the **copy running-config startup-config** command to ensure that the new configuration information is saved.

Save the configuration file to a remote server before removing the RSP2. You can retrieve it later and write it back into NVRAM. If you do not copy the configuration file, you will have to use the **configure** command or the **setup** command facility to reenter the configuration information after you reinstall the RSP2. This procedure requires privileged-level access to the EXEC command interpreter, which usually requires a password. Refer to the description that follows and contact your system administrator to obtain access, if necessary.

Using the EXEC Command Interpreter

Before you use the **configure** command, you must enter the privileged level of the EXEC command interpreter using the **enable** command. The system prompts you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, enter the privileged level as follows:

Step 1 At the EXEC prompt (>), enter the **enable** command. The EXEC command interpreter prompts you for a privileged-level password, as follows:

```
Router> enable

Password:
```

Step 2 Enter the password (the password is case sensitive). For security purposes, the password is not displayed.

Step 3 When you enter the correct password, the system displays the privileged-level system prompt (#) as follows:

```
Router#
```

The pound sign (#) at the system prompt indicates that you are at the privileged level of the EXEC command interpreter; you can now execute the EXEC-level commands that are described in the following sections.

Using the ping Command to Verify Server Connectivity

Before you attempt to copy or retrieve a file from a remote host, ensure that the connection is good between the router and the remote server by using the packet internet groper (ping) program. The ping program sends a series of echo request packets to the remote device and waits for a reply. If the connection is good, the remote device echoes them back to the local device.

The console terminal displays the results of each message sent: an exclamation point (!) indicates that the local device received an echo, and a period (.) indicates that the server timed out while awaiting the reply. If the connection between the two devices is good, the system displays a series of exclamation points (! ! !) or [ok]. If the connection fails, the system displays a series of periods (. . .) or [timed out] or [failed].

To verify the connection between the router and a remote host, issue the **ping** command followed by the name or Internet Protocol (IP) address of the remote server; then press **Return**. Although the **ping** command supports configurable options, the defaults, including interface processor as the protocol, are enabled when you enter a host name or address on the same line as the **ping** command. For a description of the configurable options, refer to the appropriate software documentation. The following example shows a successful **ping** operation:

```
Router# ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms
Router#
```

The following example shows the results of a failed **ping** operation:

```
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#
```

If the connection fails, check the physical connection to the remote file server and verify that you are using the correct address or name, then ping the server again. If you are unable to establish a good connection, contact your network administrator or refer to the end of this document for instructions on contacting technical assistance.

Copying the Configuration File

Before you copy the running configuration to the TFTP file server, ensure the following:

- You have a connection to the router either with a console terminal connected to the RSP2 console port, or remotely through a Telnet session.
- The router is connected to a network supporting a file server (remote host).
- The remote host supports the TFTP application.
- You have the interface processor address or name of the remote host available.

To store information on a remote host, enter the **copy startup-config tftp** privileged EXEC command. The command prompts you for the destination host's address and a filename, then displays the instructions for confirmation. When you confirm the instructions, the router sends a copy of the currently running configuration to the remote host. The system default is to store the configuration in a file called by the name of the router with *-confg* appended. You can either accept the default filename by pressing **Return** at the prompt, or enter a different name before pressing **Return**.

Follow these steps to copy the currently running configuration to a remote host:

Step 1 The system prompt should display a pound sign (#) to indicate the privileged level of the EXEC command interpreter. If it does not, follow the steps in the section "Using the EXEC Command Interpreter" on page 24, to enable the privileged level.

Step 2 Use the **ping** command to check the connection between the router and the remote host. (See the previous section "Using the ping Command to Verify Server Connectivity.")

Step 3 Issue the **show running-config** (or **write term**) command to display the currently running configuration on the terminal, and ensure that the configuration information is complete and correct. If it is not, use the **configure** command to add or modify the existing configuration. (Refer to the appropriate software documentation for descriptions of the configuration options available for the system and individual interfaces, and for specific configuration instructions.)

Note Before you can save (copy) a file to a TFTP server, a file must first exist on the TFTP server. Use the appropriate server commands to create this file and ensure that the filename matches the filename you will copy from the router. Also, ensure that the appropriate server permissions are set so the router can copy to this file.

Step 4 Create a file on the TFTP server.

Step 5 Issue the **copy startup-config tftp** command. The EXEC command interpreter prompts you for the name or interface processor address of the remote host that is to receive the configuration file. (The prompt might include the name or address of a default file server.)

```
Router# copy startup-config tftp
Remote host []?
```

Step 6 Enter the name or interface processor address of the remote host. In the following example, the name of the remote server is *servername*:

```
Router# copy startup-config tftp
Remote host []? servername
Translating "servername"...domain server (1.1.1.1) [OK]
```

Step 7 The EXEC command interpreter prompts you for the name of the file that will contain the configuration. By default, the system appends *-confg* to the router's name to create the new filename. Press **Return** to accept the default filename, or enter a different name for the file before pressing **Return**. In the following example, the default is accepted:

```
Name of configuration file to write [Router-confg]?
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg .....
```

Step 8 Before the router executes the copy process, it displays the instructions you entered for confirmation. If the instructions are not correct, enter **n** (no), then **Return**, to abort the process. To accept the instructions, press **Return**, or **y** and then **Return**, and the system begins the copy process. In the following example, the default is accepted:

```
Write file Router-confg on host 1.1.1.1? [confirm]
Writing Router-confg: !!!! [ok]
```

While the router copies the configuration to the remote host, it displays a series of exclamation points (! ! !) or periods (. . .). The !!!! and [ok] indicate that the operation is successful. A display of . . . [timed out] or [failed] indicates a failure, which would probably be due to a network fault or the lack of a writable, readable file on the remote file server.

Step 9 If the display indicates that the process was successful (with the series of ! ! ! and [ok]), the copy process is complete. The configuration is safely stored in the temporary file on the remote file server.

If the display indicates that the process failed (with the series of . . . as shown in the following example):

```
Writing Router-confg .....
```

your configuration was not saved. Repeat the preceding steps, or select a different remote file server and repeat the preceding steps.

Step 10 To further ensure that the configuration file was copied correctly, issue the **show startup-config** command and look at the first line for the configuration file's size. Match it with the file you copied to the TFTP server. Following is an example. (Take special note the line preceded by >>.)

```
Router# show startup-config
>> Using 1186 out of 126968 bytes
!
version 11.1
hostname Router
Router#
```

After you copy the configuration file, proceed to the section "Upgrading the Boot ROM Device" on page 9. Then proceed to the following section "Retrieving the Configuration File," after you have replaced the boot ROM and reinstalled the RSP2. If you are unable to copy the configuration file to a remote host successfully, contact your network administrator or refer to the end of this document for instructions on contacting technical assistance.

Retrieving the Configuration File

After you reinstall the RSP2, you can retrieve the saved configuration and copy it back to NVRAM. To retrieve the configuration, enter configuration mode and specify that you will configure the router from the network. The system prompts you for a host name and address, the name of the configuration file stored on the host, and confirmation to reboot using the remote file.

Note You must access the router through a console terminal connected to the master RSP2's console port, as a minimum. The configuration is lost due to the boot ROM upgrade, so no remote Telnet session can be established through an interface port.

Follow these steps to retrieve the currently running configuration from a remote host:

Step 1 On the console terminal, the system prompt should display a pound sign (#) to indicate the privileged level of the EXEC command interpreter. If it does not, follow the steps in the section "Using the EXEC Command Interpreter," on page 24, to enable the privileged level.

Note Until you retrieve the previous configuration file, the router will be running from the default configuration file in NVRAM. Therefore, any passwords that were configured on the previous system will not be valid until you retrieve the configuration file.

Step 2 Configure an interface port on the router for a connection to a remote host (TFTP server).

Step 3 Use the **ping** command to verify the connection between the router and the remote host. (See the section "Using the ping Command to Verify Server Connectivity" on page 24.)

Step 4 At the system prompt, issue the **copy tftp startup-config** command and press **Return** to enter the configuration mode and specify that you will configure the system from a network device (instead of from the console terminal, which is the default).

```
Router# copy tftp startup-config
```

Step 5 The system prompts you for the IP address of the host. Enter the IP address or name of the remote host (the remote TFTP server to which you originally saved the configuration file).

```
Address of remote host [255.255.255.255]? 1.1.1.1
```

Step 6 The system prompts you to select a host or network configuration file. The default is host; press **Return** to accept the default.

```
Name of configuration file [Router-confg]? Router-confg
```

Step 7 The system prompts you for the name of the configuration file. When copying the file, the default is to use the name of the router with the suffix *-confg* (*router-confg* in the following example). If you specified a different filename when you copied the configuration, enter the filename; otherwise, press **Return** to accept the default.

```
Name of configuration file [Router-confg]?
```

Step 8 Before the system reloads the new configuration file in NVRAM, it displays the instructions you entered for confirmation. If the instructions are not correct, enter **n** (no), and then press **Return** to cancel the process. To accept the instructions, press **Return**, or **y**, and then **Return**. Output similar to the following will appear:

```
Configure using Router-confg from 1.1.1.1? [confirm]
Loading Router-confg from 1.1.1.1: ! ! [OK - 1186/126927 bytes]
Warning: distilled config is not generated
[OK]
%SYS-5-CONFIG_NV: Non-volatile store configured from Router-confg
by console tftp from 1.1.1.1
```

While the router retrieves and reloads the configuration file from the remote host, the console display indicates whether or not the operation is successful. A series of !!!! and [OK] (as shown in the preceding example) indicates that the operation was successful. A series of . . . and [timed out] or [failed] indicate a failure (which would probably be due to a network fault or an incorrect server name, address, or filename). The following is an example of a failed attempt to boot from a remote server:

```
Booting Router-confg ..... [timed out]
```

Step 9 If the display indicates that the process was successful, as shown in Step 8, proceed to the next step.

If the display indicates that the process failed, verify the name or address of the remote server and the filename, and repeat the preceding steps. If you are unable to retrieve the configuration file, contact your network administrator or refer to the end of this document for instructions on contacting technical assistance.

Step 10 To ensure that the configuration file was retrieved correctly, issue the **show startup-config** command and look at the first line for the configuration file's size. Match it with the file you retrieved from the TFTP server. Following is an example:

```
Router# show startup-config
Using 1186 out of 126968 bytes
!
version 11.1
hostname Router
!
Router#
```

Step 11 Ensure that the startup configuration file stored in NVRAM is the default running configuration file used by the system, issue the **copy startup-config running-config** command as follows:

```
Router# copy startup-config running-config
Router#
%SYS-5-CONFIG_I: Configured from memory by console
Router#
```

This completes the procedure for retrieving the saved configuration file.

Copying Files Between RSP2 NVRAM and a Flash Memory Card

Copying a configuration file to a Flash memory card in PCMCIA slot 0 or slot 1, might be required if you do not have access to a TFTP server on which you can temporarily store your configuration file. You can then copy the configuration file back to NVRAM after the boot ROM replacement procedure is complete. Use the following sections to first copy the configuration file to a Flash memory card, and then to copy the configuration from the Flash memory card back to NVRAM.

Copying a Configuration File from RSP2 NVRAM to a Flash Memory Card on the RSP2

You can use the command **copy startup-config** [**slot0:** | **slot1:**]:*filename* for the copy procedure where **startup-config** is the file's source (NVRAM) and [**slot0:** | **slot1:**]:*filename* is the file's destination, in either of the Flash memory cards; however, the environmental variable CONFIG_FILE must be pointing (set) to NVRAM, which is the system default.

Use the **show boot** command to display the current setting for the environmental variable CONFIG_FILE as follows:

```
Router# show boot
(display text omitted)

CONFIG_FILE variable =
Current CONFIG_FILE variable =

(display text omitted)
```

Note The preceding example shows that the environmental variable CONFIG_FILE is set for NVRAM, by default.

Follow these steps to copy a configuration file from RSP2 NVRAM to a Flash memory card:

Step 1 Use the **copy startup-config slot0:***filename* command *as* follows:

```
Router# copy startup-config slot0:myfile2
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet1/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

Note In the preceding example, the exclamation points (!!!) appear as the file is copied. The "C" characters signify calculation of the checksum—a verification that the file has been correctly copied.

You can also copy the running configuration (located in DRAM) to a Flash memory card, as shown in the following section "Copying a Configuration from RSP2 DRAM to a Flash Memory Card on the RSP2."

Step 2 To verify the file was copied correctly, use the dir command as follows:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  Jul 11 1996 19:24:12 rsp-jv-mz.111-4
3   1215     Jul 11 1996 20:30:52 myfile1
4   6176844  Jul 11 1996 23:04:10 rsp-jv-mz.111-472
5   1186     Jul 12 1996 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

After you copy your configuration file to a Flash memory card and have verified that it was copied correctly, proceed to the section "Upgrading the Boot ROM Device" on page 9. When you have finished replacing the boot ROM and reinstalling the RSP2, refer to the following section "Copying a Configuration File from a Flash Memory Card to RSP2 NVRAM."

Copying a Configuration from RSP2 DRAM to a Flash Memory Card on the RSP2

You can use the command **copy running-config** [**slot0:** | **slot1**:]:*filename* for the copy procedure where **running-config** is the file's source (the temporary configuration in DRAM) and [**slot0:** | **slot1:**]:*filename* is the file's destination, in either of the Flash memory cards. An example of the **copy startup-config slot0:***filename* command follows:

```
Router# copy running-config slot0:myfile2
20575008 bytes available on device slot0, proceed? [confirm]
Address or name of remote host [1.1.1.1]?
Loading new.image from 1.1.1.1 (via Ethernet1/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 7799951/15599616 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

Note In the preceding example, the exclamation points (!!!) appear as the file is copied. The "C" characters signify calculation of the checksum—a verification that the file has been correctly copied.

To verify the file was copied correctly, use the **dir** command as follows:

```
Router# dir slot0:
-#- -length- -----date/time------ name
1   5200084  Jul 11 1996 19:24:12 rsp-jv-mz.111-4
3   1215     Jul 11 1996 20:30:52 myfile1
4   6176844  Jul 11 1996 23:04:10 rsp-jv-mz.111-472
5   1186     Jul 12 1996 16:56:50 myfile2

9197156 bytes available (11381148 bytes used)
Router#
```

After you copy your configuration file, proceed to the section "Upgrading the Boot ROM Device" on page 9. When you have finished replacing the boot ROM and reinstalling the RSP2, refer to the following section "Copying a Configuration File from a Flash Memory Card to RSP2 NVRAM."

Copying a Configuration File from a Flash Memory Card to RSP2 NVRAM

Following is the procedure for copying your configuration file from the Flash memory card in PCMCIA slot 0 or slot 1, back to NVRAM.

Use the command **copy** [**slot0:** | **slot1:**]:*filename* **startup-config** for this copy procedure, where [**slot0** | **slot1**]:*filename* is the source of the file (Flash memory card) and **startup-config** is the destination (NVRAM).

An example of the **copy slot0:***filename* **startup-config** command follows:

```
Router# copy slot0:myfile startup-config
[ok]
Router#
```

To ensure that the startup configuration file, now stored in NVRAM, is the default running configuration file used by the system, issue the **copy startup-config running-config** command as follows:

```
Router# copy startup-config running-config
Router#
%SYS-5-CONFIG_I: Configured from memory by console
Router#
```

Additional Flash Memory Commands

Following are additional commands related to the Flash memory in the single in-line memory module (SIMM) on the RSP2 (called *bootflash*) and in PCMCIA-based Flash memory cards. (The following example assumes you are currently in PCMCIA slot 0.) You can determine which PCMCIA slot you are accessing using the **pwd** command as follows:

```
Router# pwd
slot0
```

You can move between Flash memory media using the **cd** [**bootflash**: | **slot0**: | **slot1:**] command as follows:

```
Router# cd slot1
slot1
Router# cd slot0
Router# pwd
slot1
```

You can list the directory of any Flash memory media using the **dir** [**bootflash**: | **slot0:** | **slot1:**] command as follows:

```
Router# dir
-#- -length- -----date/time------ name
1   1        Jul 12 1996 09:54:53 fun1
```

You can delete a file from any Flash memory media using the **delete** command as follows:

```
Router# delete slot0:fun1
Router# dir
-#- -length- -----date/time------ name
```

Note Files that are deleted are simply marked as deleted, but still occupy space in Flash memory. To remove them, use the **squeeze** command.

The **squeeze** command permanently removes files, which are marked as deleted, and pushes all other undeleted files together to eliminate spaces between them.

Following is the syntax of the squeeze command:

```
Router# squeeze slot0:
All deleted files will be removed, proceed? [confirm]
Squeeze operation may take a while, proceed? [confirm]
ebESZ
```

To prevent loss of data due to sudden power loss, the “squeezed” data is temporarily saved to another location of Flash memory, which is specially used by the system. In the preceding command display output, the character “e” means this special location has been erased (which must be performed before any write operation). The character “b” means that the data that is about to be written to this special location has been temporarily copied. The character “E” signifies that the sector which was temporarily occupied by the data has been erased. The character “S” signifies that the data was written to its permanent location in Flash memory.

The **squeeze** command operation keeps a log of which of these functions has been performed so upon sudden power failure, it can come back to the right place and continue with the process. The character “Z” means this log was erased after the successful **squeeze** command operation.

Recovering from Locked Blocks

A locked block of Flash memory occurs when power is lost or a Flash memory card is unplugged during a write or erase operation. When a block of Flash memory is locked, it cannot be written to or erased, and the operation will consistently fail at a particular block location. The only way to recover from locked blocks is by reformatting the Flash memory card with the **format** command.

Caution Formatting a Flash memory card will cause existing data to be lost.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com.
- WWW: http://www-europe.cisco.com.
- WWW: http://www-china.cisco.com.
- Telnet: cco.cisco.com.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or `tac@cisco.com`. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or `cs-rep@cisco.com`.

This document is to be used in conjunction with the *Cisco 7507 Hardware Installation and Maintenance*, *Cisco 7513 Hardware Installation and Maintenance*, and the *Route Switch Processor (RSP2) Installation and Configuration* publications. (2883romu.fm)