CISCO SYSTEMS

®

Route Processor (RP) Installation and Configuration

Product Numbers: RP, RP=, RP-64MB=, RP-64MB-U

Introduction

This configuration note contains instructions for replacing, upgrading, and configuring the Route Processor (RP) in Cisco 7000 series routers.

Contents

This configuration note includes information on the following topics:

Product Description

The RP contains the central processing unit (CPU), the system software, and most of the memory components that are used in Cisco 7000 series routers. The system software resides on eight electronically erasable read-only memory (EPROM) components, which are also called *system ROMs* or *boot ROMs*. Although these ROMs are replaceable, most system software upgrades are distributed on floppy disk. This enables you to download and boot from upgraded software images remotely, without having to remove the RP and replace the ROMs.

1

The RP is available with either 16 MB or 64 MB of dynamic random-access memory (DRAM). DRAM, which resides on four single in-line memory modules (SIMMs), is the system operating memory that stores routing tables, protocols, and network accounting applications. Support for 64 MB of DRAM (four 16-MB SIMMs) with was introduced with Software Release 9.17(8).

Note If your RP supports 16-MB SIMMs, you can upgrade the DRAM from 16 MB to 64 MB. Otherwise, you must replace the entire RP to increase the amount of DRAM. Most RPs that shipped from the factory with maintenance Release 9.17(7) or earlier in ROM do *not* support 16 MB SIMMs. To determine whether or not your RP supports 64 MB, see the "Compatibility Requirements" section on page 7.

The RP, which is shown in Figure 1, is the main system processor in Cisco 7000 series routers. The RP contains the system CPU, the system software, and most of the system memory components, and it maintains and executes the management functions that control the system. The RP contains the following components:

- 25-megahertz (MHz) Motorola MC68040 CPU for processing key functions that are not time-critical

- System hardware configuration register for setting default boot instructions

- Bank of hardware (Media Access Control [MAC]–layer) addresses for the interface ports

- Most of the memory components used by the system, including the eight EPROM components that contain the default system software. (Although these components actually are EPROMs, they are commonly referred to as the software or boot ROMs.)

- If the router is running Cisco Internetworking Operating System (Cisco IOS) Release 11.0(0), the RP contains an 8 or 16-megabyte (MB), Intel Series 2+ Flash memory card in the slot on the faceplate. (The card is optional for other systems.)

In addition to the system software, the RP contains and executes the following management functions that control the system:

- Sending and receiving routing protocol updates

- Managing tables and caches

- Monitoring interface and environmental status

- Providing Simple Network Management Protocol (SNMP) management and the console/Telnet interface

Memory Components

Figure 1 shows the various types of memory on the RP, and Table 1 lists the functions of each type.

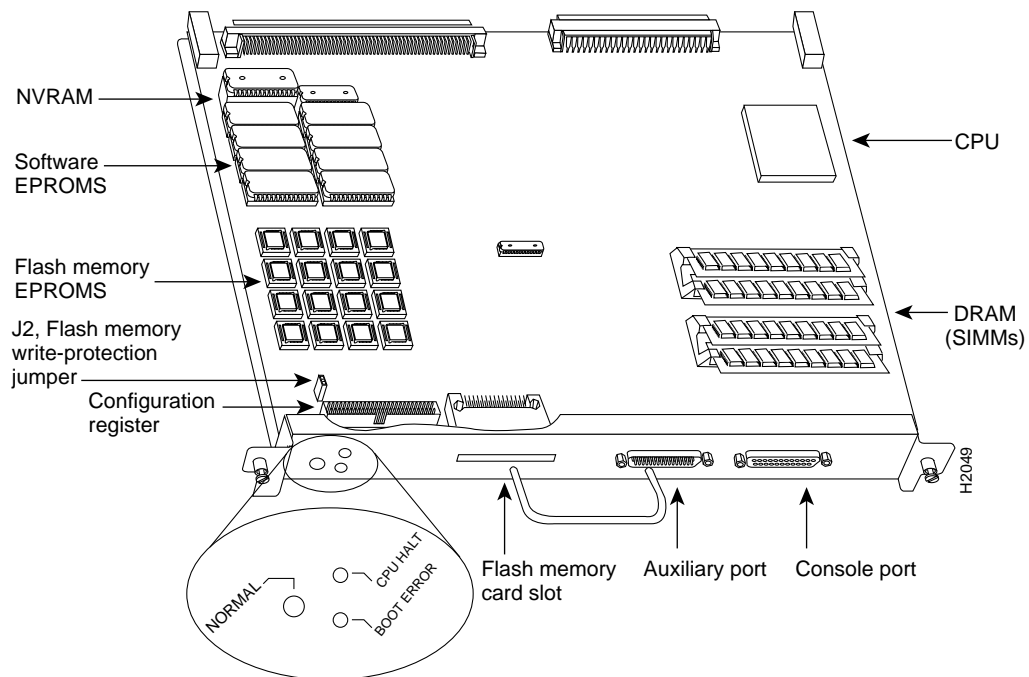**Figure 1   Cisco 7000 Series Route Processor**

Table 1   RP Memory Components

Memory Type	Size	Quantity	Description	Location
EPROM	4 MB[1]	8	4-megabit (Mb) EPROMs	ROM1–ROM8
DRAM	16 MB or 64 MB	4 4	4-MB SIMMs 16-MB SIMMs	SIMM sockets U35, U36, U58, U59
NVRAM[2]	128 KB	1	128 kilobyte (KB)	U120
EEPROM[3]	–	1	Board-specific information, address allocator	U108
Onboard Flash memory	4 MB	16	256-KB Flash components	U14–U17, U27–U30, U45–U48, U60–63
Flash memory card[4]	8 or 16 MB	1	PCMCIA Flash memory card	Flash memory card slot on faceplate

1. The size (capacity) of the software ROMs changes as needed to accommodate the size of the system software image. Maintenance Releases 9.17(6) and earlier reside on 2 megabit (Mb) ROMs, Maintenance Release 9.17(7) and later resides on 4 Mb ROMs, and the size of future releases is likely to increase.
2. NVRAM = nonvolatile read-only memory.
3. EEPROM = electrically erasable programmable read-only memory.
4. Required for systems running Cisco IOS Release 11.0(1). Optional for other systems.

System Software or Boot ROMs

Cisco 7000 series routers support downloadable system software and microcode for most upgrades, which enables you to remotely download, store, and boot from a new image. ROM replacement is seldom necessary.

Eight EPROMs contain the default and bootstrap system software. ROMs for Maintenance Release 9.17(7) and later also contain the latest microcode version, in compressed form, for each interface processor. At system startup, an internal system utility scans for compatibility problems between the installed interface processor types and the bundled microcode images, then decompresses the images into running memory (RAM). The bundled microcode images then function the same as images loaded from the microcode ROMs.

DRAM

DRAM stores routing tables, protocols, and network accounting applications. The standard RP configuration is 16 MB of DRAM, and an RP with 64 MB is available as an option or an upgrade.

Effective with Maintenance Release 9.17(8) and Maintenance Release 9.21(3), the following memory options are available:

- The RP in new systems is available with 16 MB of DRAM, which is the default, or with 64 MB of DRAM (RP-64MB-OPT).

- RP spares are available with the default 16 MB (RP=) or with 64 MB (RP-64MB=) of DRAM.

- An upgrade (RP-64MB-U) provides an RP-64MB= as a replacement for earlier RP versions that do not support 16-MB SIMMs. The upgrade requires that you return your existing RP to the factory and offers a significant cost savings over the RP-64MB= spare.

If your RP supports 16-MB SIMMs, you can upgrade the DRAM from 16 MB to 64 MB. (Because 8 MB x 9 SIMMs are not available, 32 MB is not an option.) Otherwise, you must replace the entire RP to increase the amount of DRAM. To determine whether or not your RP supports 16-MB SIMMs, see the "Compatibility Requirements" section on page 7.

NVRAM

The system configuration, software configuration register settings, and environmental monitoring logs, are backed up with built-in lithium batteries that retain the contents for a minimum of five years. When replacing an RP, be sure to back up your configuration to a remote server so that you can retrieve it later. (See the Timesaver note that follows.)

Timesaver   Before you replace an RP, back up the running configuration to a Trivial File Transfer Protocol (TFTP) file server so you can retrieve it later. If the configuration is not saved, the entire configuration will be lost—inside the NVRAM on the removed RP—and you will have to reenter the entire configuration manually. Refer to the "Saving and Retrieving the Configuration File" section on page 11 for instructions on how to save the configuration file. This procedure is not necessary if you are temporarily removing an RP you will reinstall; lithium batteries retain the configuration in memory until you replace the RP in the system.

Flash Memory

The RP contains onboard Flash memory and may also contain a Flash memory card. The Flash memory card is required for downloading software images larger than 4MB (compressed). The Enterprise and the Enterprise and APPN images of Cisco IOS Release 11.0 and later will require a Flash memory card.

Flash memory allows you to remotely load and store multiple system software and microcode images. You can download a new image over the network or from a local server and then add the new image to Flash or replace the existing files. You can then boot routers either manually or automatically from any of the stored images. Flash memory also functions as a TFTP server to allow other servers to remotely boot from stored images or to copy them into their own Flash memory. For security, jumper J2, which is adjacent to the embedded Flash components (see Figure 1), provides Flash write protection. (See the "Jumpers" section that follows.)

The Flash memory card installs in the card slot on the RP faceplate. This card is an 8 or 16-MB, Intel Series 2+ Flash memory card, which conforms with the Personal Computer Memory Card International Association (PCMCIA) format. For more information, see the "Using a Flash Memory Card" section on page 29.

EEPROM

An EEPROM on the RP (and on the SP [or SSP] and each interface processor) stores board-specific information such as the board serial number, part number, controller type, hardware revision, and other details that are unique to each processor. In addition to this standard information, the RP EEPROM also contains an address allocator, which is a bank of 40 hardware or MAC-level addresses, one for each possible port in the system. For an explanation of the hardware addressing function refer to the "MAC Address Allocator" section on page 6.

Jumpers

The hardware configuration register is a 50-pin jumper block located near the left front of the processor. (See Figure 1.)

Note If you are running Internetworking Operating System (IOS) Release 10.0 or later, *and* you have IOS Release 10.0 (or later) boot ROMs installed on the RP, the hardware configuration register is ignored by the system. The software configuration register is recognized instead.

By installing jumpers on specific pins you can define system boot instructions, set broadcast addresses and console baud rates, instruct the router to perform factory diagnostics at startup, and recover from a lost password.

Jumper J2, which is located near the configuration register, provides write protection for onboard Flash memory. (See Figure 1.) The jumper is installed on J2 by default, which allows you to write to Flash memory. When the jumper is removed, Flash is read-only; you cannot write to Flash or erase the contents until you replace the jumper.

For detailed descriptions of the configuration register, the Flash protection jumper, and all system jumpers and their settings refer to the "Hardware Configuration Register" section on page 47.

Jumpers J3 and J4 are set according to the size of the eight system software EPROMs. You need to reset these jumpers *only* if you replace the system software EPROMs with EPROMs of a different size (capacity). Do not reset these jumpers when you download new software into Flash memory, regardless of the size of the new image.

LEDs

The three LEDs on the RP indicate the system and RP status. The normal LED is on when the system is operational. During normal operation, the CPU halt and boot error LEDs on the RP should be off. When the system is turned on or restarted, the boot error LED goes on for one or two seconds, then goes off. The CPU halt LED, which goes on only if the system detects a processor hardware failure, should never be on. The Cisco 7000 model provides a redundant normal LED on the faceplate. The RP controls both LEDs and turns both on in parallel to indicate that the system is operational.

Serial Ports

Two asynchronous serial ports on the RP, the console and auxiliary ports, allow you to connect external devices to monitor and manage the system. The console port is an Electronics Industries Association/Telecommunications Industry Association (EIA/TIA)-232 receptacle that provides a data circuit-terminating equipment (DCE) interface for connecting a console terminal. (Prior to the acceptance of the EIA/TIA standard by the ANSI committee, it was referred to as a recommended standard called RS-232.) The auxiliary port is an EIA/TIA-232 plug that provides a data terminal equipment (DTE) interface; the auxiliary port supports flow control and is often used to connect a modem, a channel service unit (CSU), or other optional equipment for Telnet management.

MAC Address Allocator

All local-area network (LAN) connections (ports) require a unique *MAC-layer address*, which is also known as a *physical* or *hardware* address. Typically, the MAC address of an interface is stored on a component that resides directly on the interface circuitry, as it does on earlier Cisco router platforms (for example, on individual appliques). Every interface on the earlier platforms contains a programmable read-only memory (PROM) component with that interface's unique MAC address. The router system code reads the PROM for each interface in the system, learns the MAC addresses, and can then initialize appropriate hardware and data structures.

The Cisco 7000 series, however, requires a different method of handling the MAC addresses because of the online insertion and removal (OIR) feature. OIR allows you to remove an interface processor and replace it with another identically-configured one. If the new interfaces match the current configuration (that of the interfaces you removed), the system immediately brings them on line.

In order to allow OIR, an address allocator with 40 unique MAC addresses is stored in an EEPROM on the RP. (Because the RP supports both the seven-slot and five-slot platforms, the address bank must contain addresses for the maximum possible configuration: 40 possible interfaces [5 interface processor slots x 8 ports] in the seven-slot model. The five-slot model uses only the first 24 addresses [3 interface processor slots x 8 ports] in the MAC allocator.) Each address is assigned to a specific slot/port in the router regardless of whether or not an interface resides in that port. The MAC addresses are assigned to the ports in sequence; the first address is assigned to port 0/0, the 20th to port 2/4, and the last (40th) to port 4/8. This address scheme allows you to remove interface processors and insert them into other chassis without causing the MAC addresses to move around the network or be assigned to multiple devices.

Note that if the MAC addresses were stored on each interface processor, OIR would not function because you could never replace one interface with an identically configured one; the MAC addresses would always be different. Also, each time an interface was replaced, other devices on the network would have to update their data structures with the new address and, if they did not do so quickly enough, could cause the same MAC address to appear in more than one device at the same time. Storing the MAC addresses on the RP avoids these problems. When an interface is replaced with another interface with the same configuration, there is no need for other devices in the network to update their data structures and routing tables.

Storing the MAC addresses for every port in one central location on the RP also means that the MAC addresses stay with the RP on which they are stored. If you replace the RP, the addresses of all ports will change to those specified in the address allocator on the new RP. Because the system configuration is also stored on the RP (in NVRAM) and also stays with the RP when you remove it, you will need to reenter the configuration if you replace the RP. (See the "Saving and Retrieving the Configuration File" section on page 11.)

Installation Prerequisites

Before beginning any of these procedures, review the following sections to ensure that your equipment configuration meets the minimum requirements for the upgrade or replacement you will perform, and that you have all the parts and tools you will need. Also, review safety and ESD-prevention guidelines to help you to avoid injury or damage to the equipment.

If you are replacing the existing RP, upload your current configuration file to a remote server before you remove the RP so you can avoid having to reenter all your current configuration information manually. To upload the file, you need access to a remote server. Refer to the "Saving and Retrieving the Configuration File" section on page 11 for instructions for uploading the file and retrieving it after the new RP is installed.

Compatibility Requirements

There are no restrictions on installing an RP in a Cisco 7000 or a Cisco 7010; you can install any RP version in any Cisco 7000 series router provided that you install the RP in the RP slot.

However, before replacing SIMMs to increase the amount of DRAM available in your system, ensure that your RP supports 16-MB SIMMs.

Only RPs that meet the following prerequisites support the larger (16-MB and 64-MB) SIMMs:

- If your system contains Software Release 9.17 boot ROMs, the minimum requirements are as follows:

    — Maintenance Release 9.17(8) (or a later 9.17 image) in ROM

    — System Bootstrap Version 4.6(7.3) (or a later 4.6 bootstrap version)

    — Cisco Part Number 73-0877-06; RP Board Revision B0 or later

- If your system contains Software Release 9.21 boot ROMs, the minimum requirements are as follows:

    — Maintenance Release 9.21(3) (or a later 9.21 image) in ROM

    — System Bootstrap Version 4.7(2.1) (or a later 4.7 bootstrap version)

    — Cisco Part Number 73-0877-06; RP Board Revision B0 or later

- If your system contains Software Release 10.0 boot ROMs, the minimum requirements are as follows:

    — IOS Release 10.0(1) (or a later IOS 10.0 image) in ROM

    — System Bootstrap Version 5.0(1) (or a later 5.0 bootstrap version)

    — Cisco Part Number 73-0877-06; RP Board Revision B0 or later

- If your system contains Software Release 11.0 boot ROMs, the minimum requirements are as follows:

    — IOS Release 11.0(1) (or a later IOS 11.0 image) in ROM

    — System Bootstrap Version 11.0(1) (or a later 11.0 bootstrap version)

    — Cisco Part Number 73-0877-06; RP Board Revision B0 or later

System Bootstrap Version 4.6 is used exclusively with Software Release 9.17, and System Bootstrap Version 4.7 is used exclusively with Software Release 9.21. The revision numbers (indicated within parentheses) for each version are revised independently of other bootstrap versions. Therefore, 4.6(7) can be a later version than 4.7(2).

Maintenance Release 9.17(8), Cisco Part Number 73-0877-06 (RP Board Revision B0), and System Bootstrap Version 4.6(7.3) began shipping as the default for Cisco 7000 series systems in March 1994. Maintenance Release 9.21(3) and System Bootstrap Version 4.7(2.1) were released in May 1994.

RPs that shipped from the factory with Maintenance Release 9.17(7) or earlier in ROM do *not* support 16-MB SIMMs. To verify that your RP supports the larger SIMMs, issue the following commands:

- Use the **show version** command to display the system bootstrap version.

```
7000# show version
GS Software (GS7), Version 9.17(8)
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Fri 04-Feb-94
System Bootstrap, Version 4.6(7.3)
```

    If the display indicates that the system bootstrap version is an earlier version of 4.6 than 4.6(7.3), or an earlier version of 4.7 than 4.7(2.1), your RP will not support 16-MB SIMMs. Contact a service representative for information about the RP upgrade.

- Use the **show diag** *slot* command to display current hardware and diagnostic information about the processor installed in the slot you specify. Because the RP always resides in the same (RP) slot, specify slot 6 for a Cisco 7000 chassis or slot 4 for a Cisco 7010 chassis. The third line of the display shows the current hardware (HW) and board revisions. (Do not confuse the HW revision with the board revision; you need to verify that the *board* revision is B0, or later, and that the Cisco part number is 73-0877-06 at a minimum.)

```
7000# show diag 6
Slot 6:
        EEPROM format version 1
        Route Processor, HW rev 1.1, board revision B0
        Serial number: 00809933  Part number: 73-0877-06
```

    If the display indicates that the part number is something other than 73-0877-06 and the RP board revision is earlier than B0, your RP will not support 16-MB SIMMs. Contact a service representative for information about the RP upgrade.

- The SIMMs must meet the following requirements:

    — SIMMs must be the nine-module type, 16 MB x 9

    — Minimum speed is 70 nanosecond (ns)

    — Maximum height of one inch

All four SIMM sockets must be filled, and all must contain SIMMs of the same capacity and speed. The RP supports only 4 MB x 9 SIMMs (for a total of 16 MB) or 16 MB x 9 SIMMs (for a total of 64 MB). The RP does not support 32-MB of DRAM because 8-MB x 9 SIMMs are not available.

Note   To use the software configuration register feature that is available with IOS Release 10.0 or later), you *must* have boot ROMs that contain IOS Release 10.0 (or later) installed on your RP. If you are running IOS Release 10.0 (or later) from Flash memory and you do not have IOS Release 10.0 boot ROMs installed on the RP, then the software configuration register feature will not be available and the hardware configuration register located on the RP card (see Figure 1) will be used (recognized by the system) by default.

Tools and Parts Required

You need some or all of the following tools and parts to remove and replace an RP. If you need additional equipment, contact a service representative for ordering information.

- Number 2 Phillips or one-quarter-inch flat-blade screwdriver for the captive installation screws that secure the RP in its slot. (The carriers now use slotted screws instead of the Phillips screws that were used when the Cisco 7000 was introduced, so your chassis could have both types.)

- ESD-prevention equipment or the disposable wrist strap included with all spares and upgrade kits.

- Antistatic mat, foam pad, or bag for the removed RP (place the removed RP into an antistatic bag if you plan to return it to the factory or onto an antistatic mat or foam if you are replacing components and will reinstall the RP)

If you are replacing SIMMs you will need the following additional equipment:

- Four 16 MB x 9, 70-ns SIMMs

- SIMM extraction tool manufactured by AMP, Inc. (AMP Part Number 382264-1). For calling within the U.S., the toll-free phone number for AMP product information is 800 526-5142. Call this number for information on port orders outside of the U.S as well.

Safety Guidelines

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.

- Disconnect all power and external cables before moving a chassis.

- Do not work alone when potentially hazardous conditions exist.

- Never assume that power has been disconnected from a circuit; always check.

- Do not perform any action that creates a potential hazard or makes the equipment unsafe.

- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

In addition, use the following guidelines when working with any equipment that is connected to telephone wiring or other network cabling:

- Never install telephone wiring during a lightning storm.

- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

- Use caution when installing or modifying telephone lines.

Electrostatic Discharge Prevention

Electrostatic discharge (ESD) damage, which occurs when electronic cards or components are improperly handled, can result in complete or intermittent failures. Each processor module consists of a printed circuit board that is fixed in a metal carrier. Electromagnetic interference (EMI) shielding, connectors, and a handle are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap whenever you handle the RP, SP (or SSP), or interface processors. Handle the carriers by the handles and the carrier edges only; never touch the boards or connector pins. Figure 2 shows proper handling of an interface processor during installation in a Cisco 7010 chassis. When installing interface processors in a Cisco 7000 chassis, handle the interface processor in the same manner but rotated 90 degrees clockwise.

⚠ **Caution** Always tighten the captive installation screws on RP. These screws provide proper grounding and help to ensure that the bus connectors are properly seated in the backplane.

Figure 2   Handling an RP During Installation

Captive installation screws
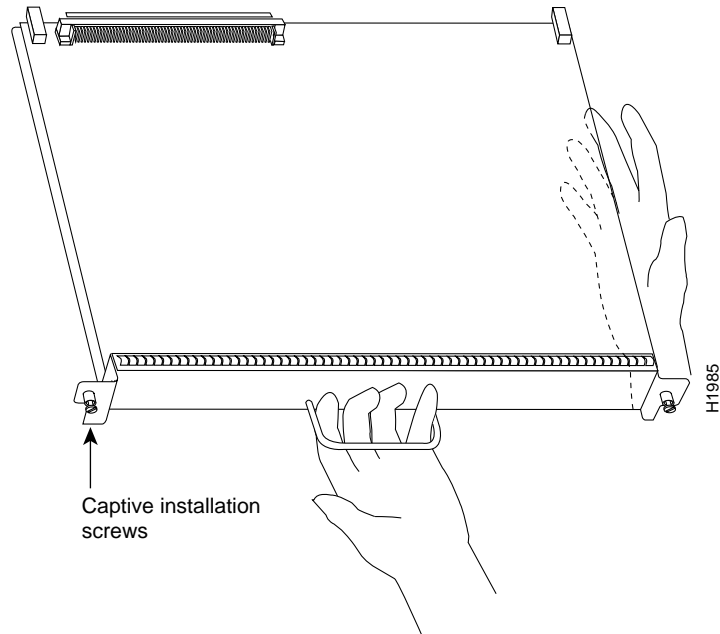
Following are guidelines for preventing ESD damage:

- Always use an antistatic wrist or ankle strap and ensure that it makes good skin contact.

- When working at the interface processor end of the chassis, connect the equipment end of the strap to a captive installation screw on an installed interface processor.

- When installing an RP, use the ejector levers to properly seat the bus connectors in the backplane, then tighten both captive installation screws. The screws prevent accidental removal, provide proper grounding, and help to ensure that the bus connectors are seated in the backplane.

- Handle processor modules by the handles and carrier edges only; avoid touching the board or any connector pins.

- Place a removed RP board side up on an antistatic surface or in a static shielding bag. If you are returning the RP to the factory, immediately place it in a static shielding bag.

- Handle SIMMs by the edges only. Avoid touching the metal contacts along the edge of the board.

- Avoid contact between the RP and clothing. Antistatic straps only protect the card from ESD voltages on the body; ESD voltages on clothing can still cause damage.

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

Installing and Replacing the RP

The following sections describe the procedures for removing and installing the RP in your chassis. If you are replacing the RP in your system, back up the current configuration to a TFTP file server before you remove the existing RP so that you can retrieve the configuration later. If you are only removing the RP temporarily (for example, to replace the DRAM SIMMs), skip the next section and proceed to the "Removing the RP" section on page 16.

Saving and Retrieving the Configuration File

This section describes the procedures for saving and retrieving the system configuration. Configuration information resides in two places when the router is operating: the default (permanent) configuration in NVRAM, and the running (temporary) memory in RAM. The default configuration always remains available; NVRAM retains the information even when the power is shut down. The current information is lost when if the system power is shut down. The current configuration contains all nondefault configuration information that you added with the **configure** command, the **setup** command facility, or by editing the configuration file. The **write memory** command adds the current configuration to the default configuration in NVRAM, so that it will also be saved when power is shut down. Whenever you make changes to the system configuration, issue the **write memory** command to ensure that the new configuration is saved.

If you replace the RP, you will also replace the entire configuration (NVRAM resides in socket U120 on the RP). If you upload (copy) the configuration file to a remote server before removing the RP, you can retrieve it later and write it into NVRAM on the new RP. If you do not upload the configuration file, you will have to use the **configure** command or the **setup** command facility to reenter the configuration information after you install the new RP. For complete descriptions of these commands and instructions for using them, refer to the appropriate software documentation.

Note   This procedure is not necessary if you are temporarily removing an RP that you will reinstall; the lithium batteries will retain the configuration in memory until you replace the RP in the system.

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 if necessary, to obtain access.

Using the EXEC Command Interpreter

Before you use the **configure** command, you must enter the privileged level of the EXEC command interpreter with the **enable** command. The system will prompt 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 user-level 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

Before you attempt to upload or retrieve a file from a remote host, ensure that the connection is good between the router and the remote server. The *packet internet groper* (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 it did not, that the server timed out while awaiting the reply. If the connection between the two devices is good, the system will display a series of exclamation points (! ! !) or [ok]. If the connection fails, the system will display 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:

```
Router# ping 131.103.11.113
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.11.113, 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:

```
Sending 5, 100-byte ICMP Echos to 131.108.11.113, 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.

Uploading (Copying) the Configuration File

Before you upload (save) 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 RP 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 privileged EXEC command **write network**. The command will prompt you for the destination host's address and a file name, then display 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 and *-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 upload (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 "Using the EXEC Command Interpreter" section on page 12, 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.")

Step 3 Issue the **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.)

Step 4 Issue the **write net** command. The EXEC command interpreter will prompt 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# write net
Remote host []?
```

Step 5 Enter the name or interface processor address of the remote host. In the following example, the name of the remote server is *servername*:

```
Router# write net
Remote host []? servername
Translating "servername"...domain server (131.108.11.113) [OK]
```

Step 6 The EXEC command interpreter will prompt 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 file name. 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 131.108.11.113? [confirm]
Writing Router-confg .....
```

Step 7 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** then **Return**, and the system will begin the copy process. In the following example, the default is accepted:

```
Write file Router-confg on host 131.108.11.113? [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 8 If the display indicates that the process was successful (with the series of ! ! ! and [ok]), the upload 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.

After you upload the configuration file, proceed to the "Removing the RP" section on page 16. If you are unable to copy the configuration to a remote host successfully, contact your network administrator or refer to the end of this document for instructions on contacting technical assistance.

Downloading (Retrieving) the Configuration File

After you install the new RP, you can retrieve the saved configuration and copy it to NVRAM. To retrieve the configuration, enter configuration mode and specify that you will configure the router from the network. The system will prompt 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.

You can access the router through a console terminal attached directly to the RP console port, or you can configure an interface port before proceeding and Telnet to the router from a remote terminal.

Follow these steps to download (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 "Using the EXEC Command Interpreter" section on page 12, to enable the privileged level.

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

Step 2   Use the **ping** command to verify the connection between the router and the remote host. (See the "Using the ping Command" section on page 12.)

Step 3   At the system prompt, issue the **configure network** 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# configure network
```

Step 4   The system will ask you to select a host or network configuration file. The default is host; press **Return** to accept the default.

```
Host or network configuration file [host]?
```

Step 5   The system will prompt you for the interface processor address of the host. Enter the interface processor address or name of the remote host (the remote file server to which you uploaded the configuration file.

```
IP address of remote host [255.255.255.255]? 131.108.11.113
```

Step 6   The system will prompt you for the name of the configuration file. When uploading 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 uploaded the configuration, enter the filename; otherwise, press **Return** to accept the default.

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

Step 7   Before the system reboots with the new configuration, it displays the instructions you entered for confirmation. If the instructions are not correct, enter **n** (no) then press **Return** to cancel the process. To accept the instructions, press **Return**, or **y** then **Return**.

```
Configure using router-confg from 131.108.11.113? [confirm]
Booting router-confg from 131.108.11.113: ! ! [OK - 874/16000 bytes]
```

While the router retrieves and boots from the configuration on the remote host, the console display indicates whether or not the operation was 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 8   If the display indicates that the process was successful, 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, contact your network administrator or refer to the end of this document for instructions on contacting technical assistance.

Step 9   Issue the **write term** command to display the currently running configuration on the terminal. Review the display and ensure that the configuration information is complete and correct. If it is not, verify the filename and repeat the preceding steps to retrieve the correct file, or 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 specific configuration instructions.).

Step 10   When you have verified that the currently running configuration is correct, issue the **write memory** command to save the retrieved configuration in NVRAM. Otherwise, the new configuration will be lost if you restart the system.

This completes the downloading (retrieving) the configuration file.

Removing the RP

When you remove or install the RP, be sure to use the ejector levers. These levers help to ensure that the RP is either fully inserted in the backplane or fully dislodged from it. Any RP, SP (or SSP), or interface processor that is only partially connected to the backplane can halt the system. Figure 3 shows a detail of the ejector lever mechanism in a horizontal position that is appropriate for the Cisco 7010. For the vertical slots in the Cisco 7000, the function is the same but rotated 90 degrees clockwise. When you simultaneously push the ejector lever inward (toward the carrier handle), the levers push the RP into the slot and ensure that the board connectors are fully seated in the backplane.

Caution   You must shut down the system before removing or installing the RP or SP (or SSP), both of which are required system components. Removing an RP or SP (or SSP) while the system is operating will cause the system to shut down or crash and might damage or destroy memory files.

Figure 2 (see page 10) shows proper handling of an interface processor during installation. When installing interface processors in a Cisco 7000 chassis, handle the interface processor in the same manner but rotated 90 degrees clockwise.

Follow these steps to remove the RP:

Step 1   Optional step: If you are replacing the RP, copy (upload) the currently running configuration file to a TFTP server so you can retrieve it later. (See the "Saving and Retrieving the Configuration File" section on page 11.)

Step 2   Slip on an antistatic strap and connect the equipment end of the strap to a captive installation screw on an installed interface processor or power supply.

Step 3   If you are replacing the RP, disconnect any devices that are attached to the console or auxiliary ports. If you are removing the RP for maintenance and will reinstall the same one, you can leave the devices attached provided that doing so will not strain the cables.

Step 4   Use a screwdriver (Number 2 Phillips or one-quarter-inch flat-blade) to loosen the two captive installation screws. (See Figure 3.)

Step 5   Place your thumbs on the ends of each of the ejectors and simultaneously pull them both outward, away from the carrier handle (in the opposite direction from that shown in Figure 3c) to release the carrier from the slot and to dislodge the RP from the backplane.

Step 6   Grasp the handle with one hand and pull the RP straight out of the slot, keeping your other hand under the carrier to guide it. (See Figure 2.) Keep the carrier at a 90-degree orientation to the backplane. Avoid touching the board or any connector pins.

Step 7   Place the removed RP on an antistatic mat or foam. If you plan to return the RP to the factory, immediately place it in an antistatic bag to prevent damage from ESD.

This completes the removal procedure. If you removed the RP to change jumpers or replace SIMMs, proceed to the appropriate section. Otherwise, if you are replacing the RP, proceed to the next section to install the new RP.

Replacing the RP

Ensure that all system power is turned off before installing the RP in the chassis. The RP is keyed for installation only in the RP slot. (See Figures 1 and 2.)

Follow these steps to install an RP:

Step 1   Ensure that all power supplies are turned OFF.

Step 2   Grasp the RP handle with one hand and place your other hand under the carrier to support and guide it into the slot. (See Figure 2.) Avoid touching the board or any connectors.

Step 3   Place the back of the RP in the far right (7000) or top (7010) slot and align the notches along the edge of the carrier with the grooves in the slot. (See Figure 3.)

Figure 3 **Ejector Levers and Captive Installation Screw**

Interface processor
card slot

Ejector
lever

Interface processor card
carrier guide (black)

a

b

Captive
installation
screw

c

H1984
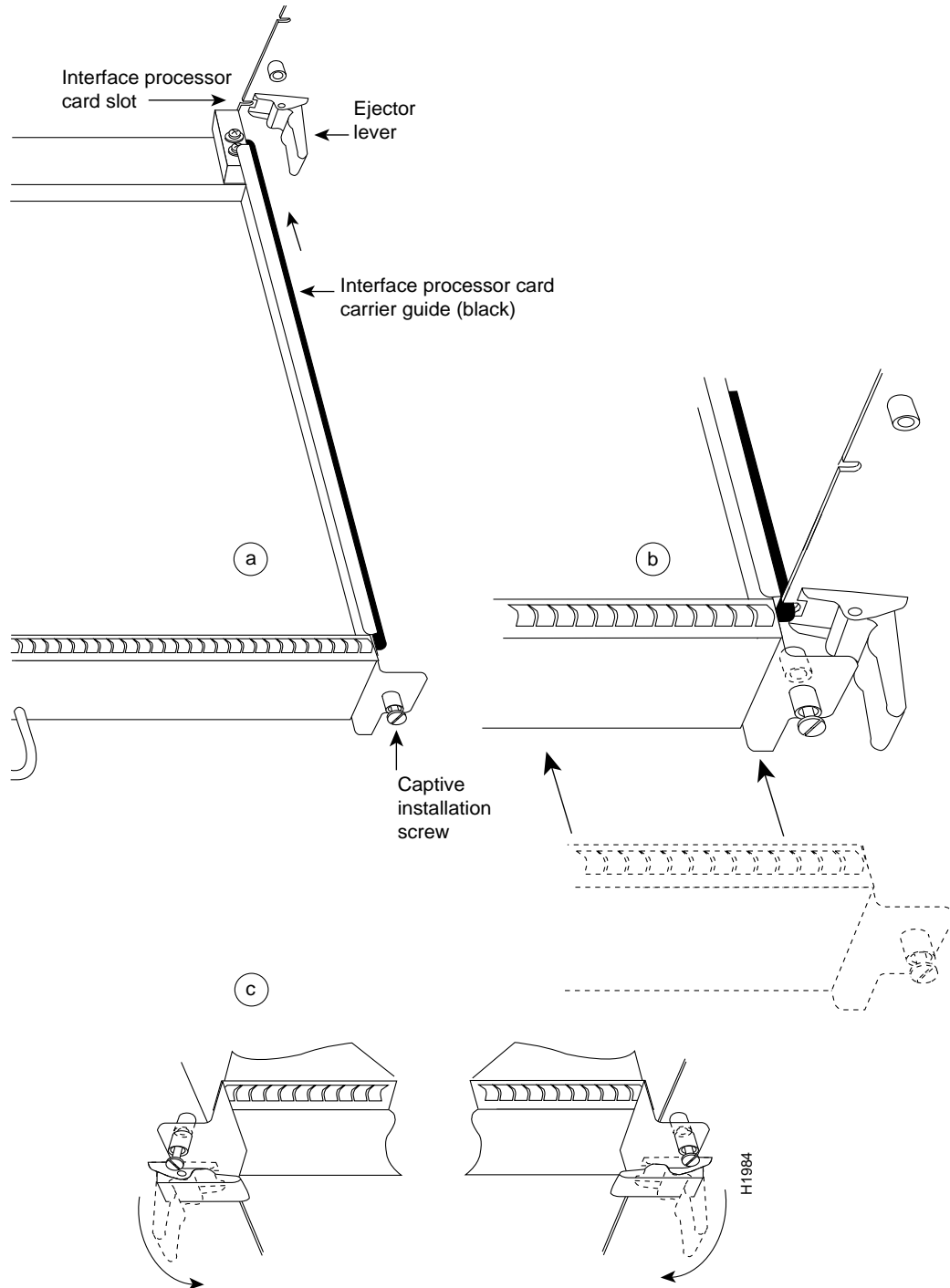
Caution You must install the RP in the far right (7000) or top (7010) slot. The slots are keyed for correct installation. Forcing the RP into a different slot can damage the backplane and the RP.

Step 4 While keeping the RP at a 90-degree orientation to the backplane, carefully slide the carrier into the slot until the RP faceplate makes contact with the ejector levers, then *stop*. (See Figure 3.)

Step 5 Using the thumb and forefinger of each hand to pinch each ejector, simultaneously push both ejectors inward (toward the handle) until they are at a full 90-degree orientation to the faceplate. (See Figure 3.)

Step 6 Use a screwdriver (Number 2 Phillips or one-quarter-inch flat-blade) to tighten the captive installation screws on the top and bottom of the RP. (See Figure 3.)

Step 7 Use a screwdriver to tighten the two captive screws on the RP faceplate to prevent the RP from becoming partially dislodged from the backplane and to ensure proper EMI shielding. (These screws must be tightened to meet EMI specifications.)

Step 8 If you disconnected the console terminal to remove the RP, or if you are installing a new RP, connect the console terminal to the console port.

Step 9 Ensure that the console terminal is turned on.

Step 10 Turn the system power back ON, and proceed to the next section to check the installation.

Restarting the System

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 from 16 to 64 MB, expect that it will take the system about four times longer to complete the memory initialization portion of the boot sequence with the larger SIMMs. (See the "System Startup Sequence" section on page 22.)

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

Step 1 Check the RP connections to make sure they are secure:

- The RP is inserted all the way into its slot, and both of the captive installation screws are tightened.

- The console terminal is turned on and is connected to the console port.

Step 2 Observe the RP LEDs. While the system initializes, the yellow boot error LED on the RP stays on, then goes off when the boot is complete. As the RP initializes each interface processor, the status LEDs on each interface processor go on and off in irregular sequence.

Step 3 Verify that the console terminal displays the system banner and startup screen as the system restarts. The display should look similar to the following:

```
GS Software (GS7), Version 9.17(8), SOFTWARE
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Thu 16-Dec-93

System Bootstrap, Version 4.6(7.3)

Current date and time is Sat 1-22-1994 21:38:35
Boot date and time is Tue 2-23-1994 15:32:28
[displayed text omitted from this example]
```

Step 4   After the system boots the software 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 RP LEDs are in the following states:

- RP normal LED is on

- CPU halt LED is off

- Boot error LED is off

Step 5   Verify that all the enabled LEDs (on the SP [or SSP] and all interface processors) are on.

When you have verified all the conditions in steps 2 through 5, the installation is complete.

If you replaced the RP and saved your configuration file to a remote server before doing so, proceed to the "Downloading (Retrieving) the Configuration File" section on page 14. If you replaced the RP and did not save the configuration, use the **configure** command or the **setup** command facility to reenter the configuration information. Refer to the appropriate software documentation for command descriptions and instructions for using them.

An error condition exists if no LEDs go on at power up or after initialization, or if the boot error or CPU halt LEDs go on and remain on. If this happens, proceed to the "Troubleshooting the Installation" section to try to isolate the problem.

Troubleshooting the Installation

This section contains procedures to follow if the system does not restart and boot as expected. Review the descriptions that follow so you can anticipate the expected system startup sequence. Then restart the system and try to isolate the problem by observing the LEDs as the system attempts to boot the software and initialize the SP (or SSP) and each interface processor.

Verifying LEDs

Following are functional descriptions of the LEDs on the power supplies and processor modules, and the behavior you should observe at system startup.

System Power LEDs

Both Cisco 7000 series models have a system power LED that should go on and stay on when the system power is turned on. If the LED does not go on or stay on, there is most likely a problem with the input power or one of the internal DC lines. However, jumpers J3 and J4, if set incorrectly, can cause the same symptom (it appears that the RP is not receiving power). If you are restarting after replacing the software (boot) ROMs, check the settings of jumpers J3 and J4. If the new ROMs are a different size from those you replaced, you will need to reset one or both of the jumpers.

On the Cisco 7010, the system power LED is located on the lower right of the interface processor end of the chassis and is labeled DC OK. The rocker-type power switch turns the power supply on and starts the system.

On the Cisco 7000, which operates with either one or two power supplies, the system power LEDs are labeled are located on the individual power supplies. Each supply contains AC power and DC fail LEDs and a power switch. (See Figure 4.). When you turn on a power supply, the green AC power LED should go on. The yellow DC fail LED should remain off. The AC power LED will not go on if the power supply switch is not fully in the on (|) position, or if the power supply is not properly seated in the bay.

In both models, the power LED will not go on or will go off if the power supply reaches an out-of-tolerance temperature or voltage condition. It is unlikely that the power supply will shut down during startup because of an overtemperature condition; it can, however, shut down if it detects an over- or under-voltage condition during startup. For descriptions of environmental monitoring functions, refer to the *Cisco 7000 Hardware Installation and Maintenance* or the *Cisco 7010 Hardware Installation and Maintenance* publications.

Figure 4   Cisco 7000 Power Supply LEDs
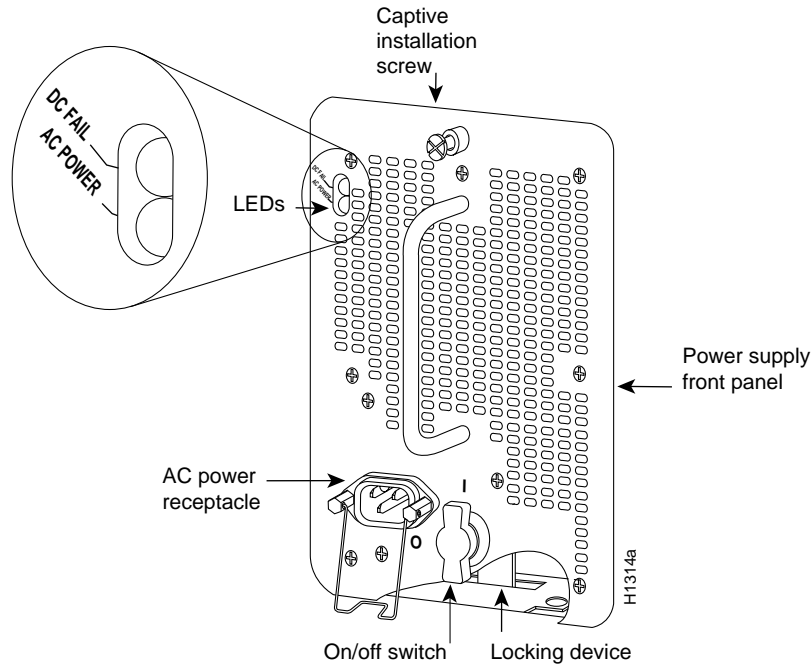
RP LEDs

Figure 5 shows the LEDs on the RP faceplate. The three LEDs on the RP indicate the system and RP status. When the system is turned on or restarted, the boot error LED goes on for one or two seconds, then goes off. The CPU halt LED, which goes on only if the system detects a processor hardware failure, should remain off. If the boot error LED stays on for more than five seconds, the system is unable to boot and should be restarted. A successful boot is indicated when the boot error LED goes off; however, this does not necessarily mean that the system has reached normal operation. During normal operation, the CPU halt and boot error LEDs should be off, and the normal LED should be on.

Figure 5   **RP LEDs (Partial Front-Panel View, Horizontal Orientation Shown)**
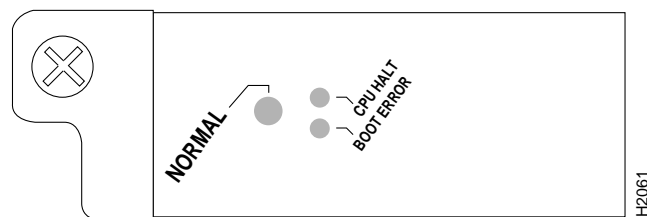
SP, SSP, and Interface Processor LEDs

The SP (or SSP) and each interface processor contain an enabled LED. The enabled LED goes on to indicate that the SP (or SSP) or interface processor is operational and that it is powered up. It does not necessarily mean that the interface ports on the interface processors are functional or enabled. When the boot sequence is complete, all of the enabled LEDs (on the SP [or SSP] and all interface processors) should go on. If any do not, one of the following errors is indicated:

- The SP (or SSP) or interface processor is not installed correctly (it is not fully seated in the backplane connector).

- The microcode and software that are loading at startup not compatible.

- The SP (or SSP) or interface processor has failed.

System Startup Sequence

By checking the state of the LEDs, you can determine when and where the system failed in the startup sequence. (The Cisco 7000 features redundant LEDs on the front of the chassis for the RP normal system status LED and the AC power LEDs on the power supplies. However, because the states reported by these LEDs are also indicated at the interface processor end of the chassis, these LEDs are ignored in the following procedure.) Because you turn on the system power with the on/off switches on each power supply, it is easiest to observe the startup behavior from the rear of the chassis. Use the following descriptions of the normal startup sequence to isolate the problem, then use the troubleshooting procedures wherever the system fails to operate as expected. If you are able to isolate the problem to a faulty hardware component, or if you are unable to successfully restart the system, refer to the end of this document for instructions on contacting a service representative.

Note   The time required for the system to initialize (boot) varies with different router configurations and the amount of memory that must be initialized. During the system startup sequence, the time required to initialize the memory (not necessarily the entire boot sequence) in a system that contains 64 MB of DRAM will be roughly four times longer than in a system that contains 16 MB of DRAM.

During the boot sequence, the system banner display pauses while it initializes the memory. If your router has 64 MB of DRAM, you may notice a significant increase in the amount of time required to initialize the memory. The pause in the banner display occurs after the copyright line, and before the system displays the list of installed hardware, as shown in the following display:

```
%SYS-5-RELOAD: Reload requested
System Bootstrap, Version 4.6(7.3)
Copyright (c) 1986-1994 by cisco Systems, Inc.

[System initializes memory at this point in the display]

RP1 processor with
```

Note The procedures in this section are based on the assumption that your system was operating correctly until you removed (or replaced) the RP. If the following sequence indicates a new problem with the power subsystem or one of the interface processors, refer to the *Cisco 7000 Hardware Installation and Maintenance* or the *Cisco 7010 Hardware Installation and Maintenance* publications for system startup troubleshooting procedures.

When you restart up the system, the system power LEDs (DC OK on the Cisco 7010, and AC power on the Cisco 7000) should indicate the following:

1 The DC OK 9 (Cisco 7010) or AC power (Cisco 7000) LED should go on. The DC fail LED on the Cisco 7000 power supply should remain off.

— If all of the system power LEDs remain off, the RP is probably not fully inserted and connected to the backplane. Loosen the captive installation screws on the RP, then use the ejector levers to release the RP and reseat it in the backplane. Refer to the "Removing the RP" section on page 16, for a description and illustration of the ejector levers.) Tighten both captive installation screws.

— Cisco 7000 only: If LEDs on only one power supply fail to go on, the power supply is probably not fully inserted into the bay. Turn the power switch off (90 degrees counterclockwise to *O*), pull the power supply out of the bay about two inches, then push the power supply firmly back into the bay. Do not slam the supply into the bay; doing so can damage the connectors on the supply and the backplane. Tighten the captive installation screw before proceeding.

— If all system power LEDs go on, the AC source is good and the power supply is functional.

— If the DC fail LED goes on, or if the AC power LED remains off, suspect the power supply or the AC power source is suspect.

When the system power LEDs indicate normal operation, proceed to number 2. If the LEDs on one or both power supplies still fail to go on as expected, a power supply or AC input power failure could be the problem. Before contacting a customer service representative, refer to the *Cisco 7000 Hardware Installation and Maintenance* or the *Cisco 7010 Hardware Installation and Maintenance* publications for power subsystem troubleshooting procedures, or refer to the note at the end of this document for instructions on contacting customer service.

2 Listen for the system blower (Cisco 7000) or the fan array (Cisco 7010). You should hear it start operating immediately after you turn on the system power. If you determine that the power supplies are functioning normally and that the blower or fan array is faulty, contact a customer service representative. If the system blower or fan tray does not function properly at initial startup, you cannot make any installation adjustments.

3 When you have verified that the power supplies are functioning properly, observe the LEDs on the RP. While the system initializes, the yellow boot error LED on the RP should be on for about five seconds or less, then go off when the boot is complete.

— If the boot error LED goes on then off as expected, proceed to number 4.

— If none of the RP LEDs light, suspect that the RP is only partially connected to the backplane. Loosen the captive installation screws on the RP, then use the ejector levers to release the RP and reseat it in the backplane (refer to page 16 for a description and illustration of the ejector levers). Tighten both captive installation screws.

— If all RP LEDs still fail to go on, suspect that an improperly connected SP (or SSP) or interface processor has halted the system. Use the ejector levers to ensure that each board is seated properly. On each ejector lever pair, push the top lever down while pushing the bottom lever up until both levers are at a 90-degree orientation to the rear of the chassis. (Refer to the "Replacing the RP" section on page 17, for a description and illustration of the ejector levers.) Tighten all captive installation screws.

— If the boot error LED stays on longer than ten seconds, or if it remains on after system initialization, a boot error has occurred. Restart the system. If this does not correct the problem, suspect a system software error.

4 The CPU halt LED on the RP should always remain off. If it goes on during the startup sequence, the system has encountered a processor hardware error.

— Remove the RP and check the configuration register settings. Ensure that a jumper has not been inadvertently installed on pin 21 and that the only jumpers installed are the default settings described in the "Configuring Jumpers" section on page 48.

— If the CPU halt LED goes on during a second startup attempt, suspect a processor hardware error and contact a customer service representative.

5 During the boot process, the LEDs on most of the interfaces light in irregular sequence; this does not indicate either correct system startup or failure.

6 When the system boot is complete, the RP begins to initialize the interface processors. During this initialization, the LEDs on each interface processor behave differently (most flash on and off). The enabled LED on each interface processor goes on when initialization has been completed.

— If the enabled LED on the SP (or SSP) and all interface processors goes on, the system has booted successfully and is now functional.

— If the RP LEDs previously indicated a successful system boot, but none of the enabled LEDs on the SP (or SSP) or the interface processors go on, suspect that one of them has shifted out of its backplane connector and halted the system. Use the ejector levers to release the SP (or SSP) or interface processor and reseat it in the backplane (refer to page 16 for a description and illustration of the ejector levers). Tighten both captive installation screws.

— If the enabled LED on a single interface processor remains off, suspect that the interface processor has shifted out of its slot. Use the ejector levers to release the interface processor and reseat it in the backplane (refer to page 16 for a description and illustration of the ejector levers). Tighten both captive installation screws. After the system reinitializes the interfaces, the enabled LED on the interface processor should go on.

— If an enabled LED still fails to go on after performing these steps, suspect that the specific SP (or SSP) or interface processor has failed.

7 When the system boot is complete and the SP (or SSP) and all interface processors have been initialized, the console screen displays a script and system banner similar to the following:

```
GS Software (GS7), Version 9.17(8)
Copyright (c) 1986-1993 by Cisco Systems, Inc.
Compiled Wed 5-Feb-94 11:06
```

— If all the previous conditions are met and this banner is displayed, the system startup was successful and your installation is complete.

— If an error message is displayed on the terminal, refer to the appropriate software publication for error message definitions.

— If the console screen is blank, check the terminal and ensure that it is turned on and that the console cable is correctly connected between the terminal and the console port on the RP.

— Check the terminal settings and ensure that the terminal is set for 9600 baud, 8 data bits, no parity, and 2 stop bits.

— If the terminal is set correctly and still fails to operate, suspect that the terminal is faulty. Connect a different terminal and restart the system.

If the system still fails to start up or operate properly, or if you isolate the cause of the problem to a failed component, contact a customer service representative for further assistance. This completes the RP installation and replacement procedure. For complete command descriptions and examples, refer to the appropriate software documentation.

Upgrading DRAM

The system DRAM resides on four SIMMs on the RP. The default DRAM configuration is 16 MB (four 4-MB x 9 SIMMs). This section describes the steps for increasing the amount of DRAM from 16 to 64 MB by replacing the four 4-MB SIMMs with four 16-MB SIMMs.

Because the SIMMs on the RP are not intended to be replaced often, if at all, the SIMM sockets do not use the thumb tabs that are often used in PCs and other computer equipment. Each RP SIMM socket has two metal retaining springs, one at each end. (See Figure 6.) When a SIMM is fully seated in the socket, the retaining springs snap upward into the holes at the ends of the SIMM to lock it in the socket. You need the AMP extraction tool to remove the SIMMs from this type of socket. The extraction tool has an embossed tip specifically designed to depress the retaining spring while wedging the SIMM out of the socket.

Figure 6   RP SIMM Sockets

Metal retaining spring

H2317
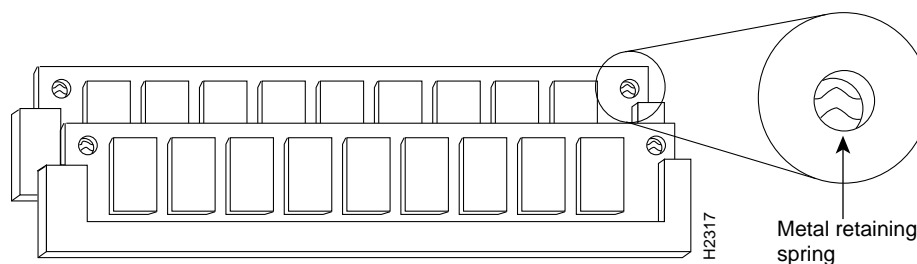
Before proceeding, ensure that you have met the following prerequisites:

• Your RP supports 16-MB SIMMs (and therefore, 64-MB SIMMs). (See the "Compatibility Requirements" section on page 7.)

• You have the proper tools and ESD-prevention equipment available. In particular, you need a SIMM extraction tool. (See "Tools and Parts Required" section on page 9.)

• You have four 16-MB SIMMs of the same type and speed. (See "Compatibility Requirements" section on page 7.)

Caution   All four SIMM sockets must be filled, and all must contain SIMMs of the same size (capacity) and speed. You cannot mix SIMMs of different sizes or speeds in the four sockets.

Removing DRAM SIMMs

To remove the SIMMs you need a SIMM extraction tool, which is manufactured by AMP, Inc. (See the "Tools and Parts Required" section on page 9.) Place removed SIMMs on an antistatic mat and store them in an antistatic bag. You can use the 4-MB SIMMs that you remove in compatible equipment.

Caution   Handle SIMMs by the card edges only. SIMMs are sensitive components that can be shorted by mishandling.

Follow these steps to remove the existing 4-MB SIMMs:

Step 1   Turn OFF the system power and follow the steps in the "Removing the RP" section on page 16.

Step 2   Place the RP on an antistatic mat or pad, and ensure that you are wearing an antistatic device, such as a wrist strap. Position the RP so that the backplane edge is closest to you, and the handle is away from you. The RP should be rotated 180 degrees from the orientation shown in Figure 1.

Step 3   Locate SIMMs in sockets U35, U36, U58, and U59. You will remove the SIMM from the socket closest to you first, then work backward to remove the remaining SIMMs. (See Figure 1.)

Step 4   While holding the extraction tool at the handle (at the top of the T), insert the embossed tip into the hole in the right side of the SIMM. (See Figure 7a.)

Figure 7   **Using the SIMM Extraction Tool**
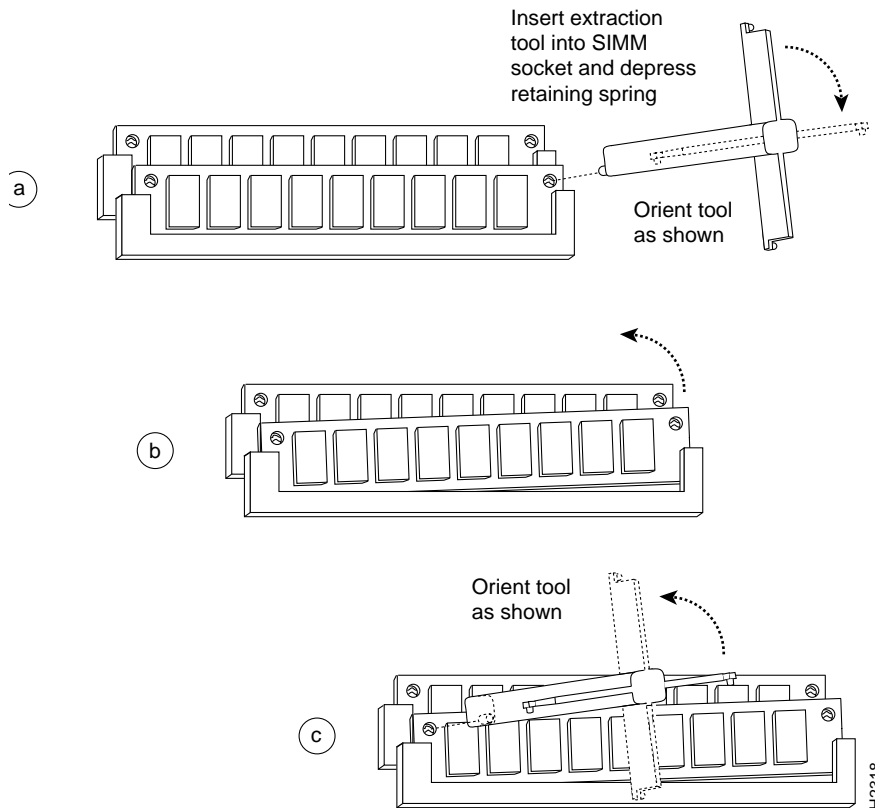
Step 5   While pressing the tool downward (to keep the retainer spring depressed), rotate the tool clockwise until the right side of the SIMM is partially released from the socket. (See Figure 7b.)

Step 6   Remove the tool from the right side, and insert the embossed tip into the hole in the left side of the same SIMM.

Step 7   While pressing the tool downward, rotate the tool counterclockwise until the left side of the SIMM is released from the socket. (See Figure 7c.)

Step 8   When both ends of the SIMM are released from the socket, grasp the ends of the SIMM with your thumb and forefinger and pull the SIMM completely out of the socket. Handle the edges of the SIMM only; avoid touching the memory module or pins, and the metal traces, or fingers, along the socket edge.

Step 9   Place the SIMM in an antistatic bag to protect it from ESD damage.

Step 10   Repeat steps 4 through 9 for the remaining SIMMs.

This completes the SIMM removal procedure. Proceed to the next section to install the new SIMMs.

Installing New DRAM SIMMs

SIMMs are sensitive components that are susceptible to ESD damage. Handle SIMMs by the edges only; avoid touching the memory modules, pins, or traces (the metal *fingers* along the connector edge of the SIMM). (See Figure 8.)

Figure 8   Handling a SIMM
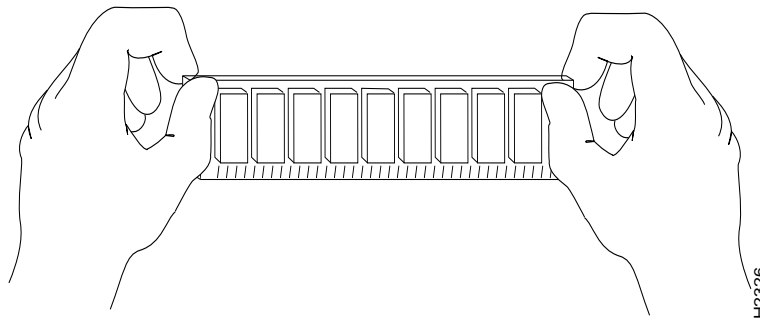
⚠ **Caution**   Handle SIMMs by the card edges only. SIMMs are sensitive components that can be shorted by mishandling.

Follow these steps to install the new SIMMs:

Step 1   With the RP in the same orientation as the previous procedure (with the backplane edge closest to you), install the first SIMM in the socket farthest from you. Then install the last SIMM in the socket closest to you.

Step 2   Remove a new SIMM from the antistatic bag.

Step 3   Hold the SIMM component side up, with the connector edge (the metal fingers) closest to you.

Step 4   Hold the sides of the SIMM between your thumb and middle finger, with your forefinger against the far edge, opposite the connector edge. (See Figure 8.)

Step 5   Tilt the SIMM to approximately the same an angle as the socket and insert the entire the connector edge into the socket.

⚠ **Caution**   When inserting SIMMs, use firm but not excessive pressure. If you damage a socket, you will have to return the RP to the factory for repair.

Step 6   Gently push the SIMM into the socket until the retaining springs snap into the holes in the SIMM. If necessary, rock the SIMM gently back and forth to seat it properly.

Step 7   Repeat steps 2 through 6 for the remaining SIMMs.

Step 8   When all four SIMMs are installed, check all eight alignment holes (two on each SIMM), and ensure that the spring retainer is visible. If it is not, the SIMM is not seated properly. If any SIMM appears misaligned, carefully remove it and reseat it in the socket. Push the SIMM firmly back into the socket until the retainer springs snap into place.

This completes the SIMM replacement procedure. To replace the RP in the chassis and restart the system for an installation check, proceed to the "Replacing the RP" section on page 17.

If the system fails to boot properly, or if the console terminal displays a checksum or memory error, check the following:

- Ensure that all four SIMMs are installed correctly. If necessary, shut down the system and remove the RP. Check the SIMMs by looking straight down on them and then at eye level. The SIMMs should all be aligned at the same angle and the same height when properly installed. If a SIMM appears to stick out, or rest in the socket at a different angle from the others, remove the SIMM and reinsert it. Then replace the RP and reboot the system for another installation check.

- All four sockets must contain SIMMs of the same size and speed or the system will not operate. The SIMMs should have the following characteristics:

    — SIMMs must be the 16 MB x 9 type. Each SIMM should contain nine small memory components, as shown in Figure 6. (The actual layout of the SIMM can be different; it is only important that there are nine components.)

    — SIMMs must be 70 ns or faster. The speed is silkscreened along one edge of the SIMM.

If after several attempts the system fails to restart properly, contact a service representative for assistance. Before you call, make note of any error messages, unusual LED states, or any other indications that might help solve the problem.

The time required for the system to initialize (boot) varies with different router configurations. Routers with 64 MB of DRAM will take longer to boot than those with 16 MB of DRAM.

Using a Flash Memory Card

This section describes installation, removal, and typical operations of the 8 or 16 MB, Intel Series 2+ Flash memory card, which installs in the PCMCIA slot on the RP faceplate.

The Flash memory card is used to store and boot Cisco Internetwork Operating System (Cisco IOS) software images and interface processor microcode images, and can be used as a server to store software and microcode images for other systems.

The spare Flash memory card is shipped blank; you *must* format it before using it. (Formatting instructions are included in this document.) The Flash memory card shipped with a spare RP or shipped with a system is already formatted.

The following sections are in a chronological order typical of many Flash memory card installations: insert the card, format the card, copy an image to the card, and make that image bootable.

Note To boot from the Flash memory card, a Cisco 7000 or Cisco 7010 router must be using Cisco IOS Release 11.0 or later boot ROMs.

Flash Memory Card Compatibility

In order to boot from the Flash memory card, the card must have been formatted on an RP board. Therefore, if you want to boot from a card formatted on an RSP board (Cisco 7500 series), you must first reformat it.

If booting is not necessary, you can still read from and write to a Flash memory card formatted on a Cisco 7500 series router.

Any Intel Series 2+ Flash memory card from a Cisco 7500 series can be used. However, the RP requires installation of the card's metal sleeve, and the router must contain Cisco IOS Release 11.0 boot ROMs. In addition, the RP can only read up to 16 MB.

Installing and Removing a Flash Memory Card

The RP has one PCMCIA slot (Slot 0) into which you can install a Flash memory card.

Note   The Flash memory card can be inserted and removed with the power on.

Following is the procedure for installing and removing a Flash memory card:

Step 1   Verify that the metal sleeve is correctly installed on the Flash memory card. (The sleeve must be installed with the connector end exposed, as shown in Figure 9.)

Note   A metal sleeve is provided with all Flash memory cards shipped as spares or with new systems. Should a replacement metal sleeve be required, consult Customer Engineering through the Technical Assistance Center (TAC) as specified on the last page of this document.

Figure 9   Installing the Metal Sleeve

Connector end →

PERFORMANCE PLUS

8 MByte Memory Card

Series 2+

FLASH

CAUTION!

FLASH FLASH FLASH

CISCO SYSTEMS

H4225
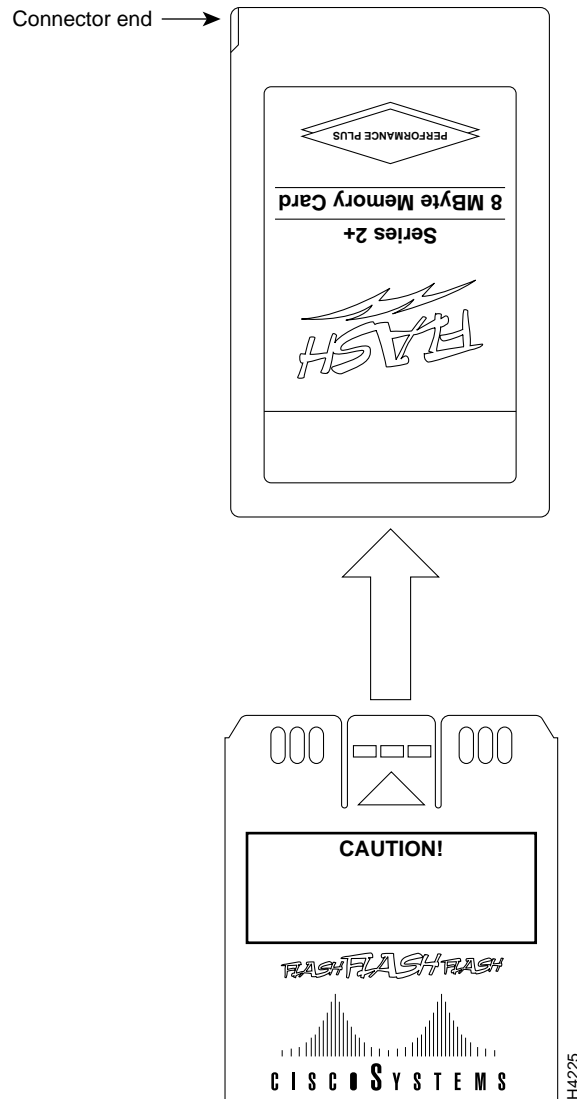
Step 2   With the RP installed in a system, hold the Flash memory card with the connector end of the card toward the RP. The product label should face to the right in a Cisco 7000 and up in a Cisco 7010. Figure 10a shows the orientation for a Cisco 7000, and Figure 11a shows the orientation for a Cisco 7010.

Note   The Flash memory card is keyed and cannot be seated the wrong way.

Step 3   Insert the card into the slot until the card completely seats in the connector at the back of the slot. Note that the card does not insert all the way inside the RP; a portion of the card and sleeve remains outside of the slot. *Do not attempt to force the card past this point.*

Step 4   To remove the card, grasp the card near the slot and squeeze the sleeve together to release it from the slot. Then pull the card free from the connector at the back of the slot. (See Figure 10c or Figure 11c.)

Step 5   Place the removed Flash memory card on an antistatic surface or in a static shielding bag.

Figure 10   Installing and Removing a Flash Memory Card (Cisco 7000 shown)
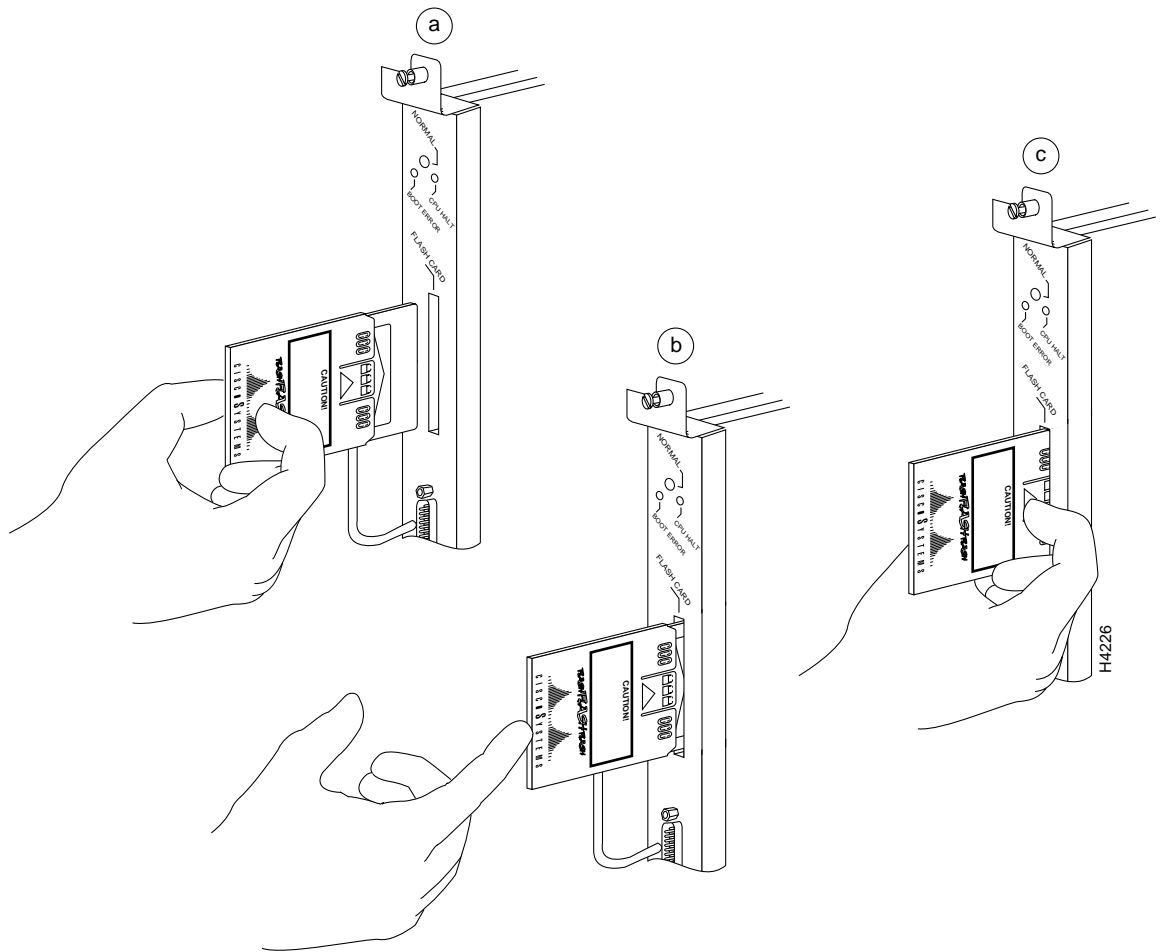
Figure 11   Installing and Removing a Flash Memory Card (RP in a Cisco 7010)
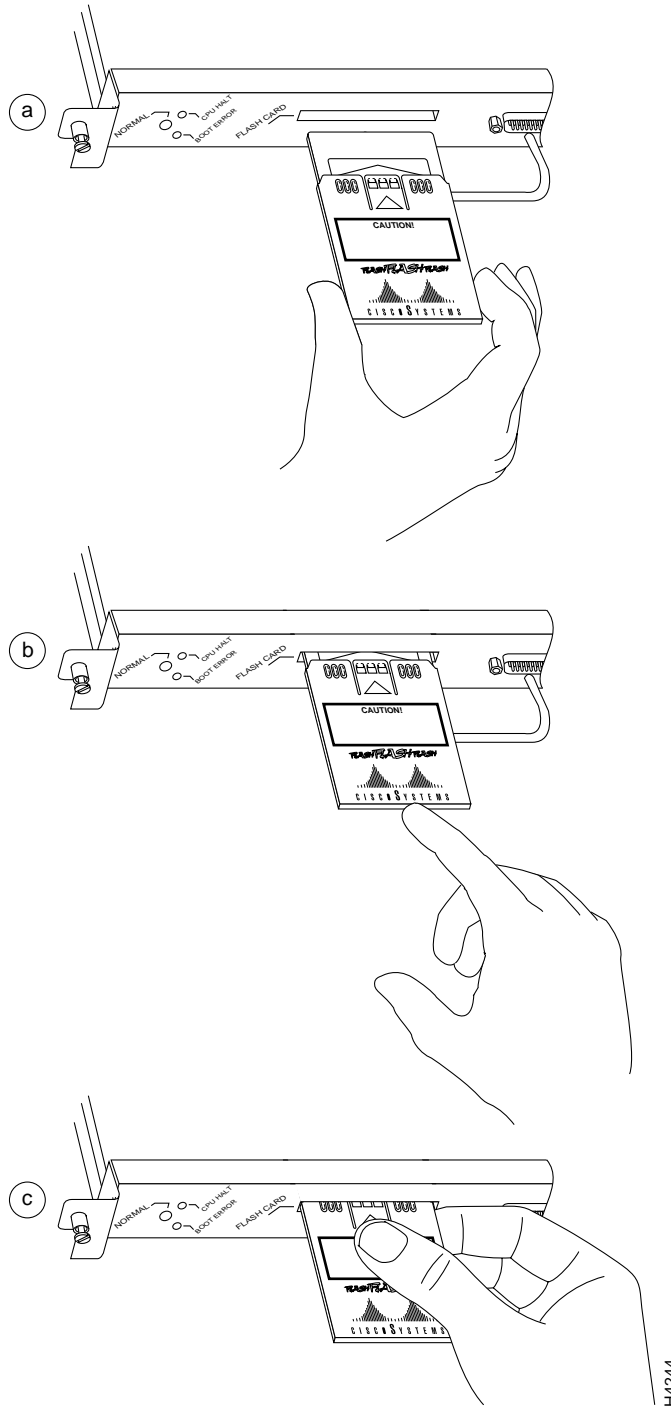
Formatting a Flash Memory Card

The Flash memory card shipped with a spare RP or shipped with a system is already formatted. However, a spare Flash memory card is shipped blank and must be reformatted before use. Also, if you plan to boot from a Flash memory card that was formatted on an RSP-based system (Cisco 7500 series), you must first reformat the card on your system.

Note The following procedure assumes you have already booted your router.

The formatting procedure erases all information on the Flash memory card. To prevent the loss of important data that might be stored on a Flash memory card, proceed carefully. If you want to save the data on a Flash memory card, copy the data to a server before you format the card.

Use the following procedure to format a new Flash memory card:

Step 1   Using the procedures in the "Installing and Removing a Flash Memory Card" section on page 30, insert the Flash memory card into the PCMCIA slot.

Step 2   To format the Flash memory card, use the **format slot0:** command as follows. (Use only Intel Series 2+ Flash memory cards.)

```
Router# format slot0:
All sectors will be erased, proceed? [confirm]
Enter volume id (up to 30 characters): MyNewCard
Formatting sector 1
Format device slot0 completed
Router#
```

Note For this example, an 8-MB Flash memory card was used, and at the line "Formatting sector," the system counted the card's sectors backwards from 64 to 1 as it formatted them. For 16-MB Flash memory cards, the system counts backwards from 128 to 1.

The new Flash memory card is now formatted and ready to use.

Note For complete command descriptions and configuration information, refer to the *Router Products Command Reference* publication and the *Router Products Configuration Guide*.

Copying a Bootable Image into a Flash Memory Card

With the Flash memory card formatted, you can now copy a bootable image into it. To copy an image, use the following procedure, which assumes the following:

- The system is running Cisco IOS Release 11.0 or later.

- The bootable image you want to copy to the Flash memory card exists on a TFTP server to which you have access (meaning you know its name and have connectivity to it), and at least one interface is available over which you can access this server.

Note To assure access to a TFTP sever, you will need to configure at least one interface using the **setup** command facility. For instructions on using this procedure, refer to the *Router Products Configuration Guide* or *Router Products Getting Started Guide* publications.

- You know the filename of the image you want to copy into the Flash memory card.

Following is the procedure for copying a bootable file (called *new.image*) into the Flash memory card:

Step 1 If the Flash memory card is unformatted or has been formatted on a Cisco 7500 series system, format it using the procedure in the "Formatting a Flash Memory Card" section on page 34.

Note If you have already formatted a Flash memory card, you can use it instead; however, you cannot boot from a Flash memory card formatted on another type of system. You must reformat it to use it as a boot source.

Step 2 To copy the image *new.image* to the Flash memory card, use the following series of commands:

```
Router> en
Password:
Router# copy tftp:new.image slot0:new.image
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]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

Note In the preceding example, the exclamation points (!!!) appear as the file is downloaded and the "C" characters signify calculation of the checksum, which is a verification that the file has been correctly downloaded to the Flash memory card.

Step 3   To make this image the default boot image and reboot the router, use the following series of commands. Note that, since the configuration register must be set to 0x2102, the **config-register** command is part of the sequence.

```
Router# config terminal
Router(config)# no boot system
Router(config)# boot system flash slot0:new.image
Router(config)# config-register 0x2102
Router(config)# ^z
Router# copy running-config startup-config
Router# reload
```

When the system reloads it will boot the image *new.image* from the Flash memory card in Slot 0 (RP Flash memory card slot).

For complete information about the **boot system flash** command used in Step 3, see the following section.

Enabling Booting from a Flash Memory Card

To enable booting from Flash memory, set configuration register bits 3, 2, 1, and 0 to a value between 2 and 15 in conjunction with the **boot system flash** *[filename]* configuration command.

Following are definitions of the various Flash memory-related **boot** commands:

boot system flash—Boots the first file in onboard Flash memory

boot system flash flash:—Boots the first file in onboard Flash memory

boot system flash *herfile*—Boots the file named "herfile" on onboard Flash memory

boot system flash slot0:—Boots the first file on the Flash memory card in the PCMCIA slot

boot system flash flash:*hisfile* —Boots the file named "hisfile" on onboard Flash memory

boot system flash slot0:*myfile* —Boots the file named "myfile" on the Flash memory card in the PCMCIA slot

To enter configuration mode and specify a Flash memory filename in the PCMCIA slot from which to boot, enter the **configure terminal** command at the enable prompt, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CTRL-Z.
Router(config)# boot system flash slot0:myfile
```

To disable Break and enable the **boot system flash slot0:** command, enter the **config-register** command with the value shown in the following example:

```
Router(config)# config-reg 0x2102

To exit configuration mode, enter Cntl-Z as follows:
Router(config)# ^Z
Router#
```

To save the new configuration to memory, use the **copy running-config startup-config** command as follows:

```
Router# copy running-config startup-config
```

When you enter **boot** commands, pay attention to the use of the space bar, which influences the way the router interprets the command. For example, notice the difference in the following commands:

```
Router(config)# boot system flash slot0:myfile (correct command)
Router(config)# boot system flash slot0: myfile (incorrect command)
```

In the first case, the router boots the file specified (*myfile*). In the second case, the router finds the *filename* field blank, and boots the first file on the Flash memory card.

Copying to a Flash Memory Card

Copying to the Flash memory card might be required whenever a new image or maintenance release becomes available.

Use the command **copy tftp:***filename* [**bootflash** | **slot0**]:*filename* for the copy procedure where **tftp:***filename* is the source of the file and [**bootflash** | **slot0**]:*filename* is the destination in onboard Flash memory or on either of the Flash memory cards.

An example of the **copy tftp:***filename* command follows:

```
Router# copy tftp:myfile1 slot0:myfile1
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]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Router#
```

Note In the preceding example, the exclamation points (!!!) appear as the file is downloaded, and the "C" characters signify calculation of the checksum, which is a verification that the file has been correctly downloaded to the Flash memory card.

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 to recover from locked blocks will cause existing data to be lost.

Note For complete command descriptions and configuration information, refer to the *Router Products Command Reference* publication and the *Router Products Configuration Guide*.

Software Configuration Register

This section describes the software (virtual) configuration register that is used with the RP in a system running Internetworking Operating System (IOS) Release 10.0 or later.

Following is the information included in this section:

- Software configuration register settings

- Explanation of boot field

- Changing configuration register settings

- Software configuration register bit meanings

- Default boot filenames

- Software configuration register settings for broadcast address destination

- System console terminal baud-rate settings

- Enabling booting from Flash

- Copying to Flash

Software Configuration Register Settings

Settings for the 16-bit software configuration register are written into the NVRAM. Following are some reasons for changing the software configuration register settings:

- Set and display the configuration register value

- Force the system into the bootstrap program

- Select a boot source and default boot filename

- Enable or disable the Break function

- Control broadcast addresses

- Set the console terminal baud rate

- Load operating software from ROM

- Enable booting from a Trivial File Transfer Protocol (TFTP) server

Table 2 lists the meaning of each of the software configuration memory bits, and Table 3 defines the boot field.

⚠ **Caution** To avoid confusion and possibly halting the router, remember that valid configuration register settings might be combinations of settings and not just the individual settings listed in Table 2. For example, the factory default value of 0x0101 is a combination of settings.

Table 2   **Software Configuration Register Bit Meanings**

Bit No.[1]	Hexadecimal	Meaning
00 to 03	0x0000 to 0x000F	Boot field (see Table 3)
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	OEM bit enabled[2]
08	0x0100	Break disabled
09	0x0200	Use secondary bootstrap
10	0x0400	IP broadcast with all zeros
11 to 12	0x0800 to 0x1000	Console line speed (default is 9,600 baud)
13	0x2000	Boot default ROM software if network boot fails
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore NVRAM contents

1. The factory default value for the configuration register is 0x0101. This value is a combination of the following: bit 8 = 0x0100 and bits 00 through 03 = 0x0001 (see Table 3).
2. OEM = original equipment manufacturer.

Table 3   **Explanation of Boot Field (Configuration Register Bits 00 to 03)**

Boot Field	Meaning
00	Stays at the system bootstrap prompt
01	Boots system image in system ROM
02 to 0F	Specifies a default netboot filename Enables boot system commands that override the default netboot filename

Changing Settings

Some common reasons to modify the value of the software configuration register are as follows:

- Recover a lost password.
- Change the console baud rate.
- Enable or disable Break.

- Allow you to manually boot the operating system using the **b** command at the bootstrap program (ROM monitor) prompt.

- Force the router to boot automatically from the system bootstrap software (boot ROM image) or from its system image in Flash memory, and read any **boot system** commands that are stored in the configuration file in NVRAM. If the router finds no **boot system** commands, it uses the configuration register value to form a filename from which to netboot a default system image stored on a network server. (See Table 4.)

To change the configuration register while running the system software, follow these steps:

Step 1   Enter the **enable** command and your password to enter privileged level, as follows:

```
Router> enable
Password:
router#
```

Step 2   At the privileged-level system prompt (router #), enter the command **configure terminal.** You will be prompted as shown in the following example:

```
Router# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
```

Step 3   To set the contents of the configuration register, enter the **config-register** *value* configuration command where *value* is a hexadecimal number preceded by 0x (see Table 2), as in the following:

```
config-register 0xvalue
```

Step 4   Exit the configuration mode by entering **Ctrl-z**. The new value settings will be saved to memory; however, the new settings do not take effect until the system software is reloaded by rebooting the router.

Step 5   To display the configuration register value currently in effect and the value that will be used at the next reload, enter the **show version** EXEC command. The value will be displayed on the last line of the screen display, as in the example following:

```
Configuration register is 0x141 (will be 0x101 at next reload)
```

Step 6   Reboot the router. The new value takes effect. Configuration register changes take effect only when the server restarts, such as when you switch the power off and on or when you issue a **reload** command from the console.

If the boot ROMs do not support the software configuration register (not IOS Release 10.0 or later), the following message will be displayed:

```
 Boot ROMs do not support software configuration register.
 Value not written to NVRAM.
```

Bit Meanings

The lowest four bits of the software configuration register (bits 3, 2, 1, and 0) form the *boot field.* (See Table 3.) The boot field specifies a number in binary form. If you set the boot field value to 0, you must boot the operating system manually by entering the **b** command at the bootstrap prompt as follows:

```
> b [tftp] flash filename
```

Definitions of the various **b** command options follow:

- **b**—Boots the default system software from ROM

- **b flash**—Boots the first file in Flash memory

- **b slot0:** *filename*—Boots the file *filename* from the Flash memory card in the PCMCIA Slot on the faceplate

- **b** *filename [host]*—Netboots using TFTP

- **b flash** *[filename]*—Boots the file *filename* from Flash *memory*

For more information about the **b** [**tftp**] **flash** *filename* command, refer to the *Router Products Command Reference* publication and the *Router Products Configuration Guide*.

If you set the boot field value to *0x2* through *0xF*, and there is a valid system boot command stored in the configuration file, then the router boots the system software as directed by that value. If you set the boot field to any other bit pattern, the router uses the resulting number to form a default boot filename for netbooting. (See Table 4.)

In the following example, the software configuration register is set to boot the router from Flash memory and to ignore Break at the next reboot of the router:

```
Router# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-register 0x102
boot system flash [filename]
^z
Router#
```

The server creates a default boot filename as part of the automatic configuration processes. To form the boot filename, the server starts with the name cisco and adds the octal equivalent of the boot field number, a hyphen, and the processor-type name. Table 4 lists the default boot filenames or actions for the processor.

Note A **boot system** configuration command in the router configuration in NVRAM overrides the default netboot filename.

Table 4   Default Boot Filenames

Action/File Name	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
ROM software	0	0	0	1
cisco2-igs	0	0	1	0
cisco3-igs	0	0	1	1
cisco4-igs	0	1	0	0
cisco5-igs	0	1	0	1
cisco6-igs	0	1	1	0
cisco7-igs	0	1	1	1
cisco10-igs	1	0	0	0
cisco11-igs	1	0	0	1
cisco12-igs	1	0	1	0
cisco13-igs	1	0	1	1
cisco14-igs	1	1	0	0
cisco15-igs	1	1	0	1
cisco16-igs	1	1	1	0
cisco17-igs	1	1	1	1

Bit 8 controls the console Break key. Setting bit 8 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 causes the processor to interpret the Break key as a command to force the system into the bootstrap monitor, thereby halting normal operation. A break can be sent in the first 60 seconds while the system reboots, regardless of the configuration settings.

Bit 9 controls the secondary bootstrap program function. Setting bit 9 causes the system to use the secondary bootstrap; clearing bit 9 causes the system to ignore the secondary bootstrap. The secondary bootstrap program is used for system debugging and diagnostics.

Bit 10 controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the broadcast address. Table 5 shows the combined effect of bits 10 and 14.

Table 5   Configuration Register Settings for Broadcast Address Destination

Bit 14	Bit 10	Address (<net> <host>)
Off	Off	<ones> <ones>
Off	On	<zeros> <zeros>
On	On	<net> <zeros>
On	Off	<net> <ones>

Bits 11 and 12 in the configuration register determine the baud rate of the console terminal. Table 6 shows the bit settings for the four available baud rates. (The factory-set default baud rate is 9,600.)

Table 6   System Console Terminal Baud Rate Settings

Baud	Bit 12	Bit 11
9,600	0	0
4,800	0	1
1,200	1	0
2,400	1	1

Bit 13 determines the server response to a bootload failure. Setting bit 13 causes the server to load operating software from ROM after five unsuccessful attempts to load a boot file from the network. Clearing bit 13 causes the server to continue attempting to load a boot file from the network indefinitely. By factory default, bit 13 is cleared to 0.

Enabling Booting from Onboard Flash

To enable booting from onboard Flash, set configuration register bits 3, 2, 1, and 0 to a value between 2 and 15 in conjunction with the **boot system flash** *[filename]* configuration command.

To enter configuration mode while in the system software image and specify a Flash filename from which to boot, enter the **configure terminal** command at the enable prompt, as follows:

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
boot system flash [filename]
```

To disable Break and enable the **boot system flash** command, enter the **config-register** command with the value shown in the following example:

```
config-reg 0x2102
^Z
router#
```

Copying to Onboard Flash

Copying a new image to onboard Flash might be required whenever a new image or maintenance release becomes available. To copy a new image into Flash (write to Flash), you must first reboot from ROM and then copy the new image into Flash. You *cannot* copy a new image into Flash while the system is running from Flash. Use the **copy tftp flash** command for the copy procedure.

Following is the sample output for reloading the router and then copying a file (called IJ09140Z) to Flash from a TFTP server (called server1):

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-reg 0x2101
^Z
```

The configuration register setting 0x0101 tells the system to boot from ROM, but does *not* reset the Break disable or checking for a default netboot filename.

```
Router# reload
...
router(boot)# copy tftp flash
IP address or name of remote host [255.255.255.255]? server1
Name of tftp filename to copy into flash []? IJ09140Z
copy IJ09140Z from 131.131.101.101 into flash memory? [confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm] <Return>
Clearing and initializing flash memory (please wait)####...
Loading from 101.2.13.110: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!... [OK - 324572/524212 bytes]
Verifying checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv...
Flash verification successful. Length = 1204637, checksum = 0x95D9

router(boot)# config term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
config-reg 0x2102
^Z
```

The configuration register setting 0x2102 tells the system to boot from ROM if netboot fails, disable Break, and check for a default netboot filename.

```
Router(boot)# reload
...
```

The system is now ready to be configured to boot from the new image you copied to Flash. For more information on the **copy tftp flash** command, and other related commands, refer to the set of router products configuration publications.

Recovering a Lost Password

An overview of recovering a lost password follows:

- Enter the **show version** command to note the existing software configuration register value.

- Break to the bootstrap program prompt (ROM monitor).

- Change the configuration register to 0x0141 (ignore Break; ignore NVRAM; boot from ROM).

Note A key to recovering a lost password is to set the configuration register so that the contents of NVRAM are ignored (0x0040), allowing you to see your password.

- Enter privileged level in the system bootstrap program.

- Enter the **show configuration** command to display the enable password.

- Change the configuration register value back to its original setting.

Note To recover a lost password if Break is disabled on the router, you must have physical access to the router.

To recover a lost password, follow these procedures.

Step 1   Attach an ASCII terminal to the router console port, which is located on the rear panel.

Step 2   Configure the terminal to operate at 9600 baud, 8 data bits, no parity, 2 stop bits (or to whatever settings the router is set).

Step 3   Enter the **show version** command to display the existing configuration register value. Note this value for later use in step 14.

Step 4   If Break is disabled, power cycle the router. (Turn the router OFF, wait five seconds, and then turn it ON again.) If Break is enabled on the router, press the Break key or send a break and then proceed to step 5.

Step 5   Within 60 seconds of turning on the router, press the Break key. This action causes the terminal to display the bootstrap program prompt (>).

Step 6   To reset the configuration register to boot from the boot ROMs and ignore NVRAM, enter **o/r** at the bootstrap prompt as follows:

```
> o/r
```

> **Note** If the boot ROMs do not support the software configuration register (that is, they are not IOS Release 10.0 or later), this command will not be recognized and the current hardware configuration register value will display.

Step 7 Initialize the router by entering the **i** command as follows:

```
> i
```

The router will power cycle, the configuration register will be set to 0x141, and the router will boot the boot ROM system image and prompt you with the system configuration dialog as follows:

```
--- System Configuration Dialog ---
```

Step 8 Enter **no** in response to the system configuration dialog prompts until the following system message is displayed:

```
Press RETURN to get started!
```

Step 9 Press **Return**. After some interface information, the boot ROM prompt appears as follows:

```
Router(boot)>
```

Step 10 Enter the **enable** command to enter the EXEC mode in the boot ROM image. The prompt changes to the following:

```
Router(boot)#
```

Step 11 Enter the **show configuration** EXEC command to display the enable password in the configuration file and to display any **boot system** commands.

Step 12 Enter the **configure terminal** command at the EXEC prompt. You are prompted as follows:

```
Router(boot)# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
```

Step 13 Enter **no** in response to any **boot system** command in the configuration file.

Step 14 Using the **config-register** 0x<*value*> command, change the configuration register value back to its original value (noted from step 3) or change it to a value of 0x0101 (factory default).

Step 15 Exit configuration mode by entering **Ctrl-z**.

Step 16 Reboot the router and enable it using the recovered password.

Hardware Configuration Register

The RP contains the hardware configuration register, which is used in systems running Software Release 9.17 or later or Software Release 9.21 or later. Systems running Software Release 10.0 or later use the software configuration register, which is described in the "Software Configuration Register" section on page 38.

The RP also contains the Flash memory write-protect jumper and two jumpers that define the size of the system software ROMs. (See Figure 12.) Jumpers installed on the hardware configuration register define boot instructions and set broadcast addresses and console baud rates. Jumper J2, when removed, protects the contents of Flash memory by preventing any information being written to Flash.

Jumpers J3 and J4 (see Figure 12) are set according to the size of the eight software EPROMs on the RP, and are described in the "Configuring Jumpers" section on page 48. These jumpers correspond to the EPROMs only; you do not need to reset the jumpers when loading a larger image into Flash memory.

Figure 12   RP Jumper Locations
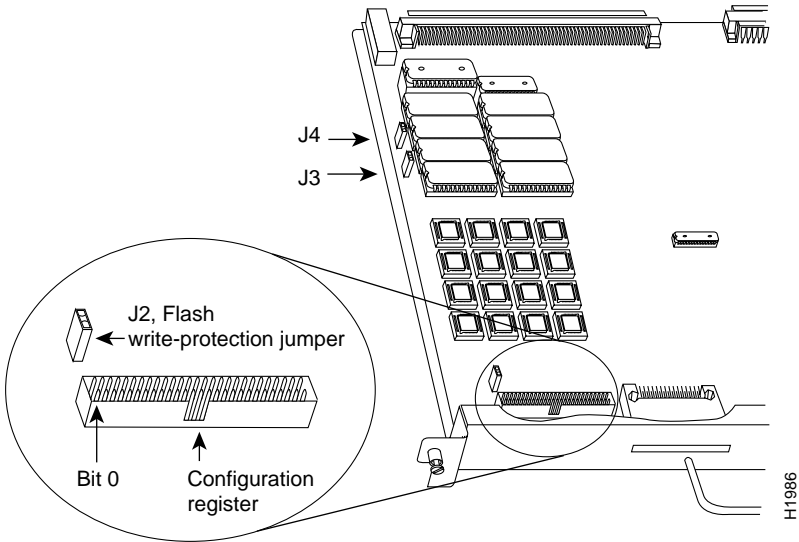
Configuring Jumpers

The configuration register consists of 32 pins of the 50-pin jumper block located behind the Flash card port on the RP. (See Figure 12.) With the RP in the orientation shown in Figure 12, the 32 left-most pins are the configuration register. You can define boot instructions, set broadcast addresses and console baud rates, or perform factory diagnostics at startup by installing jumpers on specific pins. Jumper bit (position) 0 is the left-most pair of pins (these are the two *top* pins when the RP is installed in a Cisco 7000).

To set a bit to 1, insert a jumper. To clear a bit to 0, remove the jumper.

To change configuration register settings, you must turn off the system power and remove the RP. Figure 13 shows the configuration register with the factory setting- jumpers installed on bits 0 and 8. Bit 0 instructs the system to boot from ROM; bit 8 instructs the system to ignore the Break key on the console terminal keyboard.

Figure 13   Configuration Register Factory Default Settings
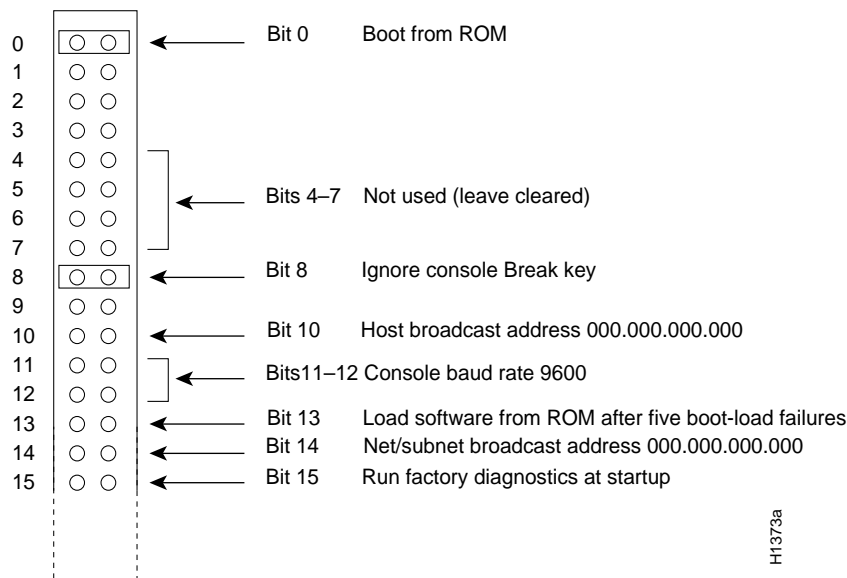
Note   Configuration register setting changes take effect when the system restarts.

The lowest four bits of the configuration register (bits 3 through 0) form the *boot field*. The boot field specifies a number in binary. When the boot field is set to either 0 or 1 (0-0-0-0 or 0-0-0-1) the system ignores any boot instructions in the configuration file. When the boot field is set to 0, you must boot the operating system manually by entering a **b** (or **boot**) command to the system bootstrap program (or *ROM monitor*). You can enter the **boot** command only, or include additional boot instructions with the command such as the name of a file stored in onboard Flash memory, a file on the Flash memory card, or a file that you specify for netbooting. If you use the **boot** command only, without specifying a file or any other boot instructions, the system boots from the ROM image.

Otherwise, you can instruct the system to boot from a specific image such as a Flash file (**boot system flash** *filename*), or to netboot by sending either broadcasting TFTP requests (**boot system** *filename*) or a direct TFTP request to a specific server (**boot system** *filename address*). When the boot field is set to 1 (the factory default), the system boots from ROM. Boot field settings of 0 and 1 both override any boot instructions in the system configuration file.

If you set the boot field to any bit pattern other than 0 or 1, the system uses the resulting number to form a file name for netbooting. To form the filename, the system starts with *cisco* and links the octal equivalent of the boot field value (jumper setting) and the processor type in the format *cisco<jumpervalue>-<processorname>*. (Table 7 lists the default boot filenames or actions for the RP.) The system uses that filename to invoke the system image from ROM or by netbooting. However, if the configuration file contains any boot instructions, the system uses those boot instructions instead of the filename it computed from the jumper settings.

Table 7   Default Boot Filenames—Boot Field Jumpers

Action/Filename	Bit 3	Bit 2	Bit 1	Bit 0
Bootstrap mode	0	0	0	0
EPROM software	0	0	0	1
cisco2-rp	0	0	1	0
cisco3-rp	0	0	1	1
cisco4-rp	0	1	0	0
cisco5-rp	0	1	0	1
cisco6-rp	0	1	1	0
cisco7-rp	0	1	1	1
cisco10-rp	1	0	0	0
cisco11-rp	1	0	0	1
cisco12-rp	1	0	1	0
cisco13-rp	1	0	1	1
cisco14-rp	1	1	0	0
cisco15-rp	1	1	0	1
cisco16-rp	1	1	1	0
cisco17-rp	1	1	1	1

Note The four bits after the boot field (bits 4 to 7) in the configuration register are not used and must be left cleared (0).

Bit 8 in the configuration register controls the console Break key. Setting bit 8 to 1 (the factory default) causes the processor to ignore the console Break key. Clearing bit 8 to 0 causes the processor to interpret Break as a command to force the system into the bootstrap monitor, thereby suspending normal operation.

Bit 9 in the configuration register controls the use of a secondary bootstrap procedure when netbooting. If a jumper is installed on bit 9, a secondary bootstrap with the filename *boot-rp* is first loaded into the system over the network. This bootstrap image then loads in the desired boot file, completing the netbooting process.

Bit 10 in the configuration register controls the host portion of the IP broadcast address. Setting bit 10 causes the processor to use all zeros; clearing bit 10 (the factory default) causes the processor to use all ones. Bit 10 interacts with bit 14, which controls the network and subnet portions of the broadcast address. Table 8 shows the combined effect of bits 10 and 14.

Table 8   Configuration Register Settings for Broadcast Address Destination

Bit 14	Bit 10	Address (<net><host>)
Out	Out	<ones><ones>
Out	In	<zeros><zeros>
In	In	<net><zeros>
In	Out	<net><ones>

Bits 11 and 12 in the configuration register determine the console port baud rate. Table 9 shows the bit settings for the four available baud rates (the factory default is 9,600).

Bit 13 in the configuration register determines the system's response to a boot-load failure. Setting bit 13 causes the system to load operating software from EPROM after five unsuccessful attempts to load a boot file from the network. Clearing bit 13 causes the system to continue attempting to load a boot file from the network indefinitely. By factory default, bit 13 is cleared to 0.

Table 9   System Console Terminal Baud Rate Settings

Baud	Bit 12	Bit 11
9,600	0	0
4,800	0	1
1,200	1	0
2,400	1	1

Bit 14 in the configuration register controls the network and subnet portions of the Internet broadcast address. Setting bit 14 causes the system to include the network and subnet portions of its address in the broadcast address. Clearing bit 14 causes the system to set the entire broadcast address to all ones or all zeros, depending on the setting of bit 10. By factory default, bit 14 is cleared to 0. See Table 8 for the combined effect of bits 10 and 14.

Bit 15 in the configuration register controls factory diagnostic mode in the system. Setting bit 15 causes the system to produce detailed CPU self-check messages, to automatically prompt for interface addresses (not look for addresses on the network), to *not* read configuration files or NVRAM, and to automatically set diagnostic tracing modes using the **debug** commands. Clearing bit 15 (the factory default) causes the system to operate normally. (For a description of the **debug** command, refer to the appropriate software documentation.)

Bits 16 through 18 are not used and should remain cleared.

Bit 19 disables the fast page-burst mode from DRAM to the MC68EC040 CPU.

Bits 20 through 23 (the four pairs of pins on the far left of the 50-pin header) are not used in normal operation; however, they can be used to invoke slave mode, external reset function, processor halt, and cache disable mode functions. (See Figure 14.)

Figure 14   Optional Configuration Register Settings
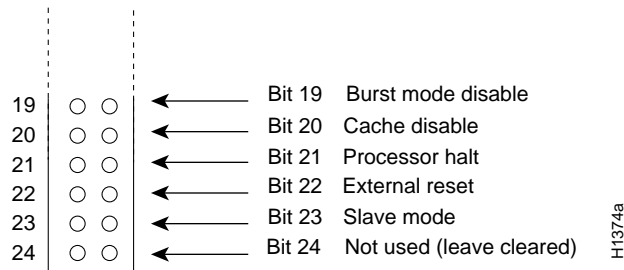
Flash Memory Write Protection

The Flash memory write-protect option protects the contents of onboard Flash memory against accidental erasure or reprogramming. The factory default, a jumper installed on J2, is to allow programming (writing) to Flash. To protect the contents, remove the jumper from J2. You can later replace the jumper to enable Flash programming. Figure 12 shows the location of J2 on the RP.

Command Descriptions and Examples

The **show version** command displays the current hardware configuration of the router, including the system software version that is currently loaded and running. The **show controllers cxbus** command lists all CxBus interfaces and includes the currently loaded and running microcode version for each. You can check the version of the default ROM image either by removing the board and checking the ROM labels or by configuring the interface or system software to boot from ROM, restarting the system, and using these same commands to check the currently running version.

In the following example of the **show controller cxbus** command, the SP (or SSP) microcode is Version 1.2 although the microcode ROM on the SP (or SSP) contains Version 1.0. (In this example, ROM Version 1.0 is assumed because you cannot determine the ROM version from screen displays unless it is the version that is running.)

```
Router# show controllers cxbus

Switch Processor 5, hardware version 11.1, microcode version 1.2
  [text omitted from example]
 FSIP 1, hardware version 1.0, microcode version 1.0
  Interface 8 - Serial1/0, electrical interface is V.35 DTE
  [text omitted from example]
  Interface 9 - Serial1/1, electrical interface is V.35 DTE
  [remainder of displayed text omitted from example]
```

Use the **show version** command to display the current system software and system bootstrap versions, and use the **show controllers cxbus** command to display the microcode version of the SP (or SSP) and each interface processor. In the following example of the **show version** command, the system is running Maintenance Release 9.17(6).

```
Router> show version

GS Software (GS7), Version 9.17(8.1), SOFTWARE
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Thu 16-Feb-94 14:46

System Bootstrap, Version 4.6(7.3) [fc2], SOFTWARE

Current date and time is Sat 2-22-1994 21:38:35
Boot date and time is Tue 12-28-1993 15:32:28
Router uptime is 8 weeks, 4 days, 6 hours, 7 minutes
System restarted by reload
System image file is "gs7-k.917-8.1", booted via tftp from 131.108.13.112

RP1 (68040) processor with 16384K bytes of memory.
X.25 software, Version 2.0, NET2 and BFE compliant.
1 Switch Processor.
1 EIP controller (6 Ethernet).
[remainder of example text omitted]
```

If the display indicates that the system software is earlier than Maintenance Release 9.17(3) or that the SP microcode is an earlier version than 1.2, check the contents of Flash memory to determine whether the required images are available on your system. (If the required images are available, you can use configuration commands to instruct the system to download the correct image before you install the new High-Speed Serial Interface [HSSI] interface processor [HIP].) The **show flash** command displays a list of all files stored in Flash memory.

The following example shows that Fiber Distributed Data Interface (FDDI) interface processor (FIP) Microcode Version 1.1 and SP Microcode Version 1.2 are stored in Flash.

```
Router# show flash
4096K bytes of flash memory on embedded flash (in RP1).

file    offset      length      name
  0     0x80        53364       fip1-1
  1     0xD134      55410       sp1-2
  [4085336/4194304 bytes free]
```

The **show interfaces serial** *slot/port* command displays statistics for the specific serial interface you specify by its slot/port address. If you use this command without the *type* and *slot/port* arguments, the system will display statistics for all interfaces in the system:

```
Router> show int hssi 1/0

Hssi 1/0 is up, line protocol is up
  Hardware is cxBus HIP
  Internet address is 131.108.38.9, subnet mask is 255.255.255.0
[display text omitted]
```

The **show configuration** command displays the contents of the system configuration file stored in NVRAM. This file should reflect all new configuration changes you made and wrote to memory with the **write terminal** command.

```
Router# show config

Using 1652 out of 130048 bytes
version 9.17
!
hostname Router
!
enable-password guessagain
!
microcode TRIP flash trip1-0
microcode reload
!
interface hssi1/0
ip address 131.108.4.67
ip route-cache cbus
no keepalive
!
interface serial2/1
ip address 131.108.22.12
[display text omitted]
```

The **show protocols** command displays the global (system-wide) and interface-specific status of any configured Level 3 protocol.

```
Router> show protocols

Global values:
  Internet Protocol routing is enabled
Hssi1/0 is up, line protocol is up
[display text omitted]
```

The **show diag** *slot* command allows you to specify a processor slot, and obtain current hardware and diagnostic information about the processor installed in that slot. Because the RP always resides in the same (RP) slot, specify slot 6 for a Cisco 7000 chassis, and slot 4 for a Cisco 7010 chassis.

```
7000# show diag 6

Slot 6:
        EEPROM format version 1
        Route Processor, HW rev 1.1, board revision B0
        Serial number: 00809933  Part number: 73-0877-06
        Test history: 0x00       RMA number: 00-00-00
```

Cisco Information Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information 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, product documentation, 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 it 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 connection rates up to 28.8 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.