

Upgrading Software and Microcode in Cisco 7000 Series Routers



Note

This document once contained information for upgrading software and microcode for Cisco 7500 series routers. For information on upgrading software and microcode in Cisco 7500 series routers, see the *Cisco IOS Configuration Fundamentals Configuration Guides* for the mainline software release that you are running.

The *Cisco IOS Configuration Fundamentals Configuration Guides* are not platform-specific; however, the information in these books also pertains to the Cisco 7500 series.

In most cases, the *Cisco IOS Configuration Fundamentals Configuration Guide* can be retrieved by clicking the following Cisco.com path:

Technical Documents (under Service & Support): **Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release** (*release number*): **Configuration Guides and Command References: Configuration Fundamentals Configuration Guide**

Cisco 7000 series routers support downloadable software and microcode for most new images; however, some exceptions require read-only memory (ROM) replacement in order for the router to boot and operate properly. This document provides instructions for upgrading with both types of media—floppy disk and ROM.

This publication describes the following tasks:

- Floppy disk or Trivial File Transfer Protocol (TFTP) server distribution—Procedures for upgrading the existing system software or microcode with new images that are distributed on floppy disk or made available for downloading from a network server using TFTP.
 - How to install a microcode upgrade or a software upgrade from 3.5-inch PC-DOS-formatted floppy disks to a personal computer (PC) or UNIX workstation configured as a TFTP server.
 - How to use TFTP to transfer a new system software image bundled (or unbundled) with microcode to Flash memory.



Note

We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility between the various interface processors in the system. The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is unbundled from the Cisco IOS bundle and shipped as a separate package on floppy disks, Flash memory cards, or is available via Cisco.com.

- How to boot the router manually or automatically from a system software image stored in Flash memory.
- ROM distribution—Upgrading the existing system software or microcode with new images that are distributed on replacement ROM components.
 - How to replace the eight system software ROMs on the Route Processor (RP).
 - How to replace the single microcode ROM on the Switch Processor (SP), Silicon Switch Processor (SSP), or any interface processor.

Routers also can netboot from a TFTP file server directly to central processing unit (CPU)—local random-access memory (RAM) regardless of whether it has Flash memory. For procedures, refer to the appropriate software configuration documentation listed in the “If You Need More Information” section on page 52. Instructions for contacting technical assistance are provided at the end of this document, in the section “Obtaining Documentation.”



Caution

SP Microcode Version 1.4 must reside in ROM; it cannot be loaded from Flash memory. During the boot process, the system accesses the SP microcode. If the SP microcode ROM contains a version earlier than 1.4 and the router contains an FSIP, the system may fail to boot properly.

Table of Contents

The information in this publication is organized within the following sections:

- Overview of Image Distribution and Upgrade Methods, page 4
- Upgrading from Floppy Disks or TFTP Servers, page 5
 - Prerequisites and Caveats, page 5
 - Procedural Overview, page 7
 - Installing the New Image onto Your TFTP Server, page 8
 - Making Network Connections, page 12
 - Loading the New Image, page 15
 - Changing the Boot Instructions, page 22
 - Configuring Microcode, page 26
 - Repeating the Installation Process, page 29
- Upgrading Software and Microcode with Replacement ROMs, page 29
 - Procedural Overview, page 29
 - Tools and Equipment, page 30
 - Removing and Replacing the RP, SP, SSP, and Interface Processors, page 31
 - Upgrading the System Software ROMs, page 39
 - Upgrading Microcode ROMs, page 46
- If You Need More Information, page 52
- Obtaining Documentation, page 53
 - World Wide Web, page 53
 - Documentation CD-ROM, page 53
 - Ordering Documentation, page 53
 - Documentation Feedback, page 53
- Obtaining Technical Assistance, page 54
 - Cisco.com, page 54
 - Technical Assistance Center, page 54

**Note**

As of Cisco IOS Release 11.0, command syntax has been updated for certain commands. Wherever command syntax appears throughout this document and the newer command syntax applies, the newer command syntax is shown in parentheses after the command.

Overview of Image Distribution and Upgrade Methods

Cisco 7000 series routers feature downloadable software and microcode for most new images. Also, microcode images are bundled with the system code, so individual microcode upgrades are no longer necessary.

**Note**

We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility between the various interface processors in the system. The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is unbundled and shipped as a separate package on floppy disks, Flash memory cards, or is available via Cisco.com.

Downloadable microcode allows you to download new images over the network, store the images in the router's Flash memory, and load images from Flash memory at system startup without having to physically access the router. Although for most upgrades you can configure the system to load newer images from Flash memory files to override the default ROM images, some exceptions require ROM replacement to ensure proper startup and operation.

All Cisco 7000 series software and microcode upgrades that were released prior to SP Microcode Version 1.4 (in September 1993) were distributed on floppy disk and could be stored in, and loaded from, Flash memory. SP Microcode Version 1.4 was the first microcode upgrade to be distributed on ROM. (Because the system software accesses the SP microcode during the boot process, SP Microcode Version 1.4 *must* reside in ROM; it cannot be stored and loaded from a Flash file.)

Bundled images include the latest system software image and the latest available microcode image for the following processor types: Asynchronous Transfer Mode (ATM) Interface Processor (AIP), Channel Interface Processor (CIP), Ethernet Interface Processor (EIP), Fiber Distributed Data Interface (FDDI) Interface Processor (FIP), Fast Ethernet Interface Processor (FEIP), Fast Serial Interface Processor (FSIP), High-Speed Serial Interface (HSSI) Interface Processor (HIP), Multichannel Interface Processor (MIP), SP, SSP, and Token Ring Interface Processor (TRIP).

The upgrade procedure for bundled images is the same as that for previous upgrades; bundled images reside either in Flash memory or in ROM. When the system boots from a bundled image, a utility scans the installed processors to determine compatibility with the new microcode, and (if there are no conflicts) loads the microcode images automatically. A new command, **show microcode**, lists all of the microcode images that are bundled with the system software image. (For a brief description of the **show microcode** command, refer to "Listing the Bundled Microcode Versions" on page 28; for a complete description, refer to the **show microcode** command reference or the appropriate chapter [in most cases, the chapter is Loading and Maintaining Software Images and Microcode] of the *Cisco IOS Configuration Fundamentals Guide*).

Depending upon the type of media in your upgrade kit, proceed as follows:

- If you received an upgrade on floppy disk, proceed to the following section, "Upgrading from Floppy Disks or TFTP Servers."
- If you received an upgrade on one or more replacement ROMs, proceed to "Upgrading Software and Microcode with Replacement ROMs" on page 29.

Review the entire section before beginning either of these procedures to ensure that you are aware of any safety considerations or system prerequisites.

**Caution**

SP Microcode Version 1.4 must reside in ROM; it cannot be loaded from Flash memory. During the boot process, the system accesses the SP microcode. If the SP microcode ROM contains a version earlier than 1.4 and the router contains an FSIP, the system may fail to boot properly.

Upgrading from Floppy Disks or TFTP Servers

This section describes the procedures for upgrading system software or microcode from a floppy disk by copying the new image to a TFTP server, then loading the new image from the TFTP server to the Flash memory on one or more routers. When ROM replacement is not required, this procedure allows you to upgrade all of the routers in your network remotely, without having to physically access the router to replace components.

Cisco 7000 series routers also can netboot from a TFTP file server directly to CPU-local RAM, which does not require storing the image in Flash memory. The procedure is described in the appropriate router software configuration documentation. If you received an upgrade kit with replacement ROMs for the system software or microcode, refer to “Upgrading Software and Microcode with Replacement ROMs” on page 29 for instructions.

Prerequisites and Caveats

To successfully upgrade the system software or microcode, you should observe the following prerequisites and caveats.

Prerequisites

- You must have Internet Protocol (IP) running to the devices you plan to upgrade on the network.
- You must have a terminal connection that enables you to issue commands to each router on the network you want to upgrade. If you do not have a direct terminal connection, you must set up a Telnet session on a device attached to the router to be upgraded.
 - If you are using TCP/IP software that permits concurrent Telnet and TFTP server connections, your terminal connection and TFTP session can be from the same PC.
 - If you are using TCP/IP software that permits only the TFTP server to run (such as PC/TCP from FTP Software, Inc.), you need two machines. Set up one for your terminal connection and the other for your TFTP server.
- A TFTP file server must be active and accessible to the router. You must copy the system software or microcode image into the TFTP server directory to download it to the router.

If the TFTP server is a PC, it must have the following minimum configuration:

- The server must be a PC or a desktop SPARC station with a 1.44-MB 3.5-inch floppy drive.
- The configuration of the computer must meet the requirements established by the TFTP software vendor. Cisco has tested the following software running on an Everex 386/33 running under DOS 5.0 (in both Ethernet and Token Ring environments):

PC/TCP from FTP Software, Inc., Version 2.0 and greater. The toll-free number for FTP Software, Inc. is 800 282-4387. The address for FTP Software, Inc. is 2 High Street, North Andover, MA 01845-2620 or 100 Brickstone Square, Andover, MA 01810.

Chameleon TCP/IP for Windows from NetManage, Inc. To contact NetManage, Inc., call (408) 973-7171 or fax 408 257-6405. The address is 10725 North DeAnza Boulevard, Cupertino, CA 95014, USA.

Cisco has also tested the TFTP server provided by SunOS 4.1.x on SPARCstation platforms.

- The keywords **flash** and **rom** are reserved for the **boot system** and **microcode** configuration commands and indicate that the Flash memory or system ROMs, respectively, are to be used for booting system images. Do not use these reserved keywords for other files you might create.
- Total Flash memory capacity is 4 MB, and you cannot selectively delete files from Flash memory. If there is not sufficient free space in Flash memory to add a new image, you will have to erase the entire contents of Flash memory before you can add a new image. If there are files stored in Flash memory that you want to save, copy the files to a TFTP server before performing the upgrade. After you install the upgrade (and Flash memory is cleared of all but the new image), selectively copy the saved files back into Flash memory. (Refer to “Backing Up the Current Contents of Flash Memory” on page 15.)
- Jumper J2 on the RP is the Flash write-protect jumper. The jumper installed on J2 (the factory default) enables writing to Flash memory. Removing the jumper disables writing to Flash memory and protects the contents. You can store new images in Flash memory only if jumper J2 is installed. (For instructions, refer to “Setting the Flash Write-Protect Jumper” on page 46).
- Cisco 7000 series routers, which use the Route Processor (RP), ship with the hardware configuration register boot field jumper set to boot from ROM. If you have not yet changed this setting (if you have not installed and booted from an image in Flash), you will have to change the jumper setting. (If you are running Cisco IOS Release 10.0 or later *and* you have Cisco IOS Release 10.0 [or later] boot ROMs installed in the RP, special circumstances apply, refer to “Changing the Boot Field Jumper” on page 43.)



Note

Cisco 7000 series routers that have the 7000 Series Route Switch Processor (RSP7000) installed use the software configuration register feature exclusively. The RSP-based processor modules have no user-configurable jumpers.

Caveats

- If you have not yet installed your TCP/IP software, be aware of the following issues when installing it:
 - Use the proper driver for your network interface card and system configuration.
 - Know whether your TFTP server is using a DMA channel.
 - Some network interface cards require that you manually set the interrupt request (IRQ) value; if your network interface card requires an IRQ value, make sure it does not conflict with a value used by another PC card.
 - Some network interface cards require that you specify the card’s I/O address.
 - Obtain an IP address for the PC and identify the number of subnet bits to assign.
- If you are using Chameleon TCP/IP for Windows, make sure you click the Server On checkbox in the Server Settings dialog box before you use TFTP to transfer the system software image.
- Chameleon TCP/IP for Windows from NetManage, Inc., does not support DR DOS.
- If your PC is using a Western Digital card that was resold by SMC, you might need to use a different driver than the one supplied by NetManage.

- When you install a new image onto your TFTP server, make sure the server has at least 2 MB of disk (storage) space available. If it does not, the existing space will be filled up with an incomplete image that will not function on your routers.
- When copying a file to Flash memory, a prompt asks whether you want to erase the contents of Flash memory. Answering **yes**, or pressing the Return key without entering **yes** or **no**, erases the entire contents. (The default is to confirm the erasing process). Before starting the copy process, copy any files that you do *not* want erased to a TFTP server so that you can retrieve them later.
- If you download Cisco IOS Release 10.0 or later into Flash memory *and* wish to use the software configuration register feature, you *must* install Cisco IOS Release 10.0 or later boot ROM components on the RP card; otherwise, the hardware configuration register (located on the RP card) will be used by default. Refer to the section “Upgrading the System Software ROMs” on page 39.
- We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility between the various interface processors in the system.

Procedural Overview

This section lists the general steps required to upgrade from a new image on floppy disk. The sections that follow describe these steps in greater detail.

-
- | | |
|----------------|--|
| Step 1 | Install the new image from the floppy disk on your PC or UNIX machine into the TFTP server directory. |
| Step 2 | Verify that the router you want to upgrade has access to the TFTP server. Ping from the TFTP server to the router and from the router to the TFTP server. |
| Step 3 | Start the TFTP server if it is not already active. |
| Step 4 | Connect a console terminal or establish a Telnet session with the router you plan to upgrade. |
| Step 5 | Back up any current system software and microcode images that are stored in Flash memory by copying them to the TFTP server. |
| Step 6 | Copy the new image from the TFTP server into Flash memory. |
| Step 7 | Ensure that the checksum listed on the bottom line of the output for the copy tftp command matches the checksum listed in the README file on the upgrade disk. If it does not, you must invoke the copy tftp command again before booting from Flash memory. |
| Step 8 | Make sure your system is configured to boot from the new image in Flash memory. |
| Step 9 | Boot the router from Flash memory. This process writes the images from Flash memory into system RAM. |
| Step 10 | Check all network connections to make sure the router with the upgraded system software is up and functioning properly. |
| Step 11 | Repeat these steps to upgrade additional routers. |

Installing the New Image onto Your TFTP Server

This section describes how to use the installation program on the disk to install the new image onto your DOS-based PC or your desktop SPARCstation. Refer to the online README file on the upgrade disk for details about the new image. The README file lists details such as the product number, image types, file sizes, and checksums of the images.

Installing New Images onto a DOS-Based PC

To copy the new image into the appropriate directory on the PC you plan to use as the TFTP server, follow this procedure. Allow five minutes to complete this procedure.

**Caution**

Do not install the system software or microcode image to the TFTP server and then install it a second time. If you do, the system appends the second image to the first image rather than writing over it, and the altered image will not function in your routers. If you want to install the image a second time, first delete the image from the destination directory on the TFTP server and then reinstall it.

**Note**

It is good practice to make a backup copy of the master upgrade disk (containing the new bundled image) and work from the backup copy. Archive the master disk.

Following is the procedure for installing new images onto a DOS-based personal computer (PC):

Step 1 Insert the master upgrade disk into your 3.5-inch disk drive.

Step 2 Type the following command and press Enter.

```
C:\> a:install
```

where *a* is the drive in which you inserted the source disk. The drive letter can be either *a* or *b*.

A screen similar to the following appears. This screen is for a 10.3(9) software image. If you are upgrading to a release other than 10.3(9), the information in the header fields (the first four lines) will be different.

```
***** 7K1000390Z.DOC *****
```

```
PRODUCT NO. SW-G7-10.3.9=
System Software Image 7K91770Z, GS7-K Version 10.3(9)
Compressed size = 1610960 bytes; Checksum=0xa0df
Copyright (c) 1995 Cisco Systems, Inc.
```

File 7K10390Z supports all software capabilities for the Cisco 7000.

```
To install this software in a PCDOS environment enter:
  A:install          (or use the appropriate drive letter)
To install this software in a UNIX environment enter:
  #mount -rt pcfs /dev/fd0 /pcfs
  #/pcfs/install.unx  (where the user has root privileges)
```

To install this software onto a router, follow the procedures in the accompanying publication, "Upgrading System Software and Microcode in the Cisco 7000."

```
*****
```

- Step 3** A prompt appears asking if you want to continue with the installation. Press the **Y** key (or **Enter**) to continue, or the **N** key to abort.
- Step 4** A prompt appears asking where the files will be installed. The default directory is C:\TFTPBOOT. To accept this directory, press **Enter**. To specify a different directory, type the full pathname, then press **Enter**.
- If the nondefault directory you specify does not already exist, a message appears asking if you want to create the directory.
- Step 5** To create the directory, press the **Y** key. If you do not want to create a new directory on your PC and want to abort this process, press the **N** key.
- The software displays a set of messages indicating the status of the installation. The copy process takes about one minute.
- Step 6** If you have multiple floppy disks, the system prompts you to insert the second disk and press **Enter**. When the process is complete, a message appears. The following example shows the 10.3(9) image—7K1000390Z.
- ```
Installation for 7K10390Z complete!
```
- Step 7** Eject the disk from the disk drive and keep it in a safe place.
- Step 8** Change to the directory in which you installed the 10.3 image. For example, if you installed it in the default directory, type the following command and press **Enter**:
- ```
C:\> cd \tftpboot
```
- Step 9** List the contents of the image in this directory. For example, if you installed the System Software Release 10.3(9), type the following command and press **Enter**:
- ```
C:\> dir 7K10390Z.*
```

The following two files should appear:

- 7K10390Z
- 7K10390Z.DOC (the README file that appears when you install the image on the server)

Proceed to “Establishing a TFTP Session” on page 12.

## Installing New Images onto a Sun Workstation

The following procedure describes how to install the new image onto a desktop SPARCstation with SunOS 4.1.x. The workstation must have a 3.5-inch, 1.44-MB floppy disk drive. Allow ten minutes to complete this procedure.

You must have superuser access to install the new image on a UNIX system.



### Note

If you have a different UNIX-based system, refer to your system’s documentation for instructions on how to load a PC-DOS formatted floppy disk and how to configure the system as a TFTP server.



### Caution

Do not reinstall the new image on the TFTP server after installing it a first time. If you do, the system appends the second image to the first image rather than writing over it, and the altered image will not function in your routers. If you want to install the image a second time, first delete the image from the destination directory on the TFTP server and then reinstall it.

Use the following procedure to create a mount point and install the new image on your TFTP server. Note that filenames are case sensitive.

- Step 1** Create a directory named `pcfs` as follows (you must have superuser capability to execute this instruction):

```
hostname# mkdir /pcfs
```

- Step 2** Insert the disk containing the upgrade into your 3.5-inch floppy disk drive.

- Step 3** Mount the floppy disk drive as a device by entering the following command:

```
hostname# mount -t pcfs /dev/fd0 /pcfs
```

If the disk is write-protected, enter the following command:

```
hostname# mount -rt pcfs /dev/fd0 /pcfs
```

The floppy is now set up as the device `/pcfs`.

- Step 4** Copy the new image to your TFTP directory. To copy it to the default (`/tftpboot`) directory, enter the following command:

```
hostname# /pcfs/install.unx
```

- Step 5** A message appears prompting you to specify the device from which the new image is being installed. The default is `/dev/fd0`. To accept the default, press **Return**. To specify a different directory, type the name of the built-in floppy drive on the SPARCstation.

- Step 6** A prompt asks you to specify the path from the mounted floppy drive. The default is `/pcfs`. To accept the default, press **Return**. To specify a different path, type the full path name.

A screen similar to the following appears. The following screen is for a 10.3(9) system software image. If you are upgrading to a release other than 10.3(9), the header fields (the first four lines of the display) will be different.

```
***** 7K10390Z.DOC *****
PRODUCT NO. SW-G7-10.3.9=
System Software Image 7K10390Z, GS7-K Version 10.3(9)
Compressed size = 1610960 bytes; Checksum=0xa0df
Copyright (c) 1995 Cisco Systems, Inc.

File 7K100390Z supports all software capabilities for the Cisco 7000.
To install this software in a PCDOS environment enter:
 A:install (or use the appropriate drive letter)
To install this software in a UNIX environment enter:
 #mount -rt pcfs /dev/fd0 /pcfs
 #/pcfs/install.unx (where the user has root privileges)

To install this software onto a router, follow the procedures in the
accompanying publication, "Upgrading Software and Microcode in
Cisco 7000 Family Routers."

```

**Step 7** A prompt appears asking if you want to continue with the installation. Press the **Y** key (or **Enter**) to continue, or the **N** key to abort. The screen displays a set of messages indicating the status of the installation. The copy process takes about five minutes.

**Step 8** If you have multiple floppy disks, the system prompts you to insert the subsequent disks and press **Enter**.

After the image is installed on your TFTP server, the disk is automatically ejected and the disk drive is automatically unmounted. When the copy process is complete, a message appears. The following example shows the 10.3(9) image 7k10390Z.

```
Installation for 7k10390Z complete!
```

**Step 9** Eject the disk from the disk drive and keep it in a safe place.

**Step 10** Change to the directory in which you installed the system software or microcode image. For example, if you installed it in the default directory, type:

```
hostname# cd /tftpboot
```

**Step 11** List the contents of the image in this directory. For example, for a 10.3(9) system software image, enter the following command:

```
hostname# ls -l 7k100390z*
```

The following two files should appear (for the 10.3[9] image; other images would be different, such as 7k11110z for the 911.1[1] image):

- 7k10390z
- 7k10390z.doc (the README file that appears when you install the software image on the server)

Proceed to the next section, "Making Network Connections."

## Making Network Connections

This section describes the following topics:

- Testing the TCP/IP software
- Establishing a TFTP session (to the router)
- Establishing a Telnet session (from the router to the TFTP server)

### Testing the TCP/IP Software

After installing the TCP/IP software you will use to copy the new image to the routers on your network, make sure it functions properly by following this procedure:

- Step 1** Make sure a router with which you plan to communicate is up and running by pinging from that router to the TFTP network server. Use the following syntax for the **ping** command:

```
Router# ping ip-address
```

If the router is appropriately connected, you see a series of exclamation points (!!!!!). However, the following messages indicate that you have no connection:

- [timed out]
- [failed]

- Step 2** Verify the connection to the TFTP file server by transmitting a **ping** from the TFTP file server to the router.

If the connection fails, make sure you reconfigure the interface, check the physical connection to the TFTP file server, and retransmit the **ping**.

If you are using PC/TCP Network Software for DOS from FTP Software, Inc., you can verify the appropriate driver and IP address by entering the following command:

```
C:\> ifconfig drivers\drivername show
```

You can verify your IP configuration by entering the following command:

```
C:\> ipconfig ftp_3c\ipcust.sys show
```

If you are using Chameleon TCP/IP for Windows from NetManage, Inc., run its setup program to verify that you are using the appropriate driver and have configured the TCP/IP software properly.

### Establishing a TFTP Session

This section describes how to set up your UNIX system or PC as a TFTP server and start a TFTP session with the router you want to upgrade remotely.

If you are using a PC and do not already have TFTP software, we recommend the following two TCP/IP software packages:

- PC/TCP Network Software for DOS from FTP Software, Inc. (character-based TFTP software capability)
- Chameleon TCP/IP for Windows software from NetManage, Inc. (a Windows-based TFTP server)

The “Prerequisites and Caveats” section on page 5 lists some issues to keep in mind while installing the software.

## Setting Up TFTP on a Sun Workstation

To set up the Sun system as a TFTP server, you must verify that the TFTP daemon is enabled, the TFTP environment variable is set correctly, and a tftpboot directory exists. To see if TFTP is enabled, enter the following command:

```
hostname# netstat -a | grep tftp
```

If the TFTP daemon is already enabled, proceed to “Creating a tftpboot Directory” on page 14.

## Enabling the TFTP Daemon

The TFTP daemon (tftpd) permits the system to be a TFTP server. If you are using the standard Sun software, verify that tftpd is enabled by completing the following steps:

- 
- Step 1** Log in as a superuser.
  - Step 2** Using a text editor such as *vi*, edit the */etc/inetd.conf* file.
  - Step 3** Look in the */etc/inetd.conf* file for the line that invokes tftpd. If the line is commented out (starts with a pound sign [#]), remove the pound sign with an editor. This example shows sample output for the */etc/inetd.conf* file.

```
tftp dgram udp wait root /user/etc/in.tftpd
in.tftpd -s /tftpboot
```

- Step 4** Save the changes in the edited file and exit.
- Step 5** At the UNIX prompt, enter the following command to display the process ID number for the inetd configuration:

```
hostname# ps -ax | grep -v grep | grep inetd
```

The system response is similar to the following:

```
119 ? S 0:05 inetd
```

The first number in the output is the process ID of the inetd process. You must kill this inetd process by entering the following command:

```
hostname# kill -HUP 119
```

- Step 6** Verify that TFTP is enabled by entering the following command:

```
hostname# netstat -a | grep tftp
```

The output should be similar to the following:

```
udp 0 0 *.tftp *
```

If there is no output, tftpd is not enabled. For additional information about TFTP, refer to the UNIX manual pages about **tftp** and **tftpd**.

## Creating a tftpboot Directory

The tftpboot directory can be used to save and store configuration files that are loaded to a device. Device configuration files can be saved as TFTP boot files.



### Note

The tftpboot directory is accessible by all users. To protect the security of your system, do not leave sensitive files in this directory.

## Creating a tftpboot Directory on a Sun Workstation

You must have superuser access to perform the following steps. These steps describe how to create a tftpboot directory.

**Step 1** If the tftpboot directory does not exist, use the following command to create it:

```
hostname# mkdir /tftpboot
```

**Step 2** The /tftpboot directory must have the appropriate permissions. Modify the permissions with the following command:

```
hostname# chmod 777 /tftpboot
```

As a result, all users accessing this directory will have read, write, and execute permissions.

## Creating a tftpboot Directory on a PC

To create a new directory on a PC, enter the following command:

```
C:> MKDIR \TFTPBOOT
```

After completing all the preparations required to set up your Sun workstation or PC as a TFTP server, refer to “Testing the TCP/IP Software” on page 12.

## Establishing a Telnet Session

You must be able to issue commands to the router you plan to upgrade. For example, this publication tells you to issue a command to download an image from the TFTP server to the router. If you have a console port connection to the router, you need not invoke a Telnet session.

If you do not have a console port connection to the router, you must establish a Telnet session with it so that you can issue commands.

You can set up a Telnet session from a Sun workstation or from a PC.

- If you are using a Sun workstation as a TFTP server, you can also establish a Telnet session from the workstation to the router in addition to the TFTP session.
- If you are running TCP/IP software on a PC, is the software character-based or Windows-based?
  - If character-based, you need a second PC from which you can establish a Telnet session.
  - If Windows-based, you can open one window for the TFTP session and one window for the Telnet session.

## Loading the New Image

This section presents the following topics:

- Backing up any current system software and microcode images that are stored in Flash memory, including learning the image names and copying the images from Flash memory to the TFTP server (this is not necessary to back up images stored in ROM)
- Copying the new image from a TFTP server to Flash memory
- Modifying the configuration file with instructions to load the new image at startup, and to disable any existing instructions to load system software or microcode images from ROM or Flash files
- Reloading the software
- Verifying the new image in Flash memory

## Backing Up the Current Contents of Flash Memory

If your system is currently running from a system software image stored in Flash memory and you do not already have the image backed up on a TFTP server, make sure you back up this image before installing the new image. You can also use this procedure to back up other files you have stored in Flash memory.

Also back up any microcode images stored in Flash memory that you want to keep. Microcode upgrades for most Cisco 7000 series interface processors have been released, and all except SP Microcode Version 1.4 were distributed on floppy disk. Because microcode is now bundled with system software images, you no longer need to save the individual microcode images. However, until you verify that the new bundled image is loaded and running successfully, we recommend that you back up all working files that are currently stored in Flash memory. You can delete the backups after you install and verify the new image.

## Learning the Image Names

First, you must know the exact spelling of the name of each image that you will back up. To learn the image name, issue the **show flash all** command. The following sample output shows one system software image (7k91720z) and one microcode image (fip1-1).

```
Router# show flash all
4096K bytes of flash memory on embedded flash (in RP1).
 ROM socket code bytes name
 0 U63 012A 0x40000 AMD 28F020
 1 U62 012A 0x40000 AMD 28F020
 2 U61 012A 0x40000 AMD 28F020
 (display text omitted)
 11 U27 012A 0x40000 AMD 28F020
 12 U17 012A 0x40000 AMD 28F020
 13 U16 012A 0x40000 AMD 28F020
 14 U15 012A 0x40000 AMD 28F020
 15 U14 012A 0x40000 AMD 28F020
security jumper(12V) is installed,
flash memory is programmable.

file offset length name
 0 0x80 3 test3
 1 0x1E72E8 97200 fip1-1
 2 0x13EDE0 1305820 7k91720z
[1582404/4194304 bytes free]
Router#
```

When you back up the image, use the exact filename from the **show flash all** command screen.

## Copying the Image from Flash Memory to the TFTP Server

To copy an image from Flash memory to a TFTP server, use the **copy flash tftp** command:

```
Router# copy flash tftp filename
```

The router prompts you for the IP address of the TFTP server and the name of the image file you are copying to the server. A sample of the output for this command using IP address 131.108.10.6 and filename 7k91720z follows:

```
IP address of remote host [255.255.255.255]? 1.1.1.6
Name of file to copy []? 7k10390z <Return>
writing 7k91720z!!
Router#
```

Use the image you backed up to the TFTP server in case the upgrade image becomes damaged.

## Copying the Image from a TFTP Server to Flash Memory

The **copy tftp flash** command retrieves an image from a TFTP server and copies (writes) the image into the router's Flash memory. The TFTP server can be another Cisco router serving ROM or Flash system software images, or a PC or UNIX workstation set up as a server for remotely downloading new images to routers on the network. If you have already established a connection with the remote server, proceed to "Downloading the New Image" on page 18.



**Note**

Before you can copy an image to Flash memory, the write-protection jumper (J2) on the RP card must be installed. (See Figure 7). If this jumper is removed, Flash memory is write protected and cannot be overwritten. The RP is shipped with this jumper installed; therefore, Flash memory can be overwritten by default.

In some cases, primarily outside of North America, Cisco Systems distributors may choose not to distribute the new image on floppy disk. Instead, they can place the new image on TFTP servers and provide their customers with the information they will need to access and download the new image. If you are downloading a new image from your distributor with this process, ensure that your distributor has provided you with all of the following information:

- IP address of the TFTP server that contains the new image
- Exact image name
- Image size (length in bytes)
- Checksum

You must have all of this information from your distributor before you can complete the upgrade. Proceed to the following section, “Verifying the Connection.”

## Verifying the Connection

Verify the connection between your router and the remote server by pinging the server using the IP address (this may be provided by your distributor). Following is an example of a successful **ping** command to a remote server with the address 1.1.1.101:

```
Router# ping 1.1.1.101 <Return>
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 1.1.1.101, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/64 ms
Router#
```

The console displays a series of exclamation points (!!!!) to indicate a good connection between your router and the server, or a series of periods (.....) or the messages [timed out] or [failed] to indicate that the connection failed. If the connection fails, verify that you have the correct IP address for the server and that the server is active (powered on), and repeat the **ping** command.

## Verifying Flash Capacity and Configuration

Before copying the new image to Flash memory, use the **show flash all** (or **dir [ bootflash | slot0 | slot1 ]**) command to verify that Flash memory is not write-protected and that there is sufficient space remaining for the new image. The following example shows that writing to Flash memory is enabled (the

write-protection [security] jumper [J2] is installed on the RP) and that Flash memory has approximately 1.7 MB of space available for new images (shown as the amount of bytes free in the last line of the display).

```
Router# show flash all
4096K bytes of flash memory on embedded flash (in RP1).
 ROM socket code bytes name
 0 U63 89BD 0x40000 INTEL 28F020
 (displayed text omitted)
 15 U14 89BD 0x40000 INTEL 28F020
security jumper(12V) is installed,
flash memory is programmable.

file offset length name
 0 0x80 1995304 gs7-k.103.9.1
 1 0x1E72E8 97200 fip1-1
 (displayed text omitted)
 7 0x2483A4 55418 sp1-2
[1731676/4194304 bytes free]
```

Cisco 7000 family routers are shipped with Flash memory enabled for writing. If jumper J2 on the RP has been removed to protect the Flash memory contents, you will not be able to write the new image to Flash memory until you replace the jumper. Refer to “Setting the Flash Write-Protect Jumper” on page 46 for instructions.

Compare the amount of memory available (the bytes free value) with the size of the new image to ensure that there is ample space available in Flash memory. Total Flash memory capacity is 4 MB, and most system software images are close to 2 MB in size. Therefore, you can usually store one system software image and several microcode images. If there is not sufficient space available for the new image, you must erase the entire contents of Flash memory before you can copy in the new image; you cannot selectively delete specific files. You should, however, copy the files you want to keep to a TFTP server and then selectively copy the files back into Flash memory after erasing and installing the new image. Refer to “Backing Up the Current Contents of Flash Memory” on page 15 for instructions.



#### Note

Although you can compress an image and boot the compressed image from Flash memory, this is not recommended. The README file on your master upgrade diskette lists the size and checksum of the uncompressed image. If you compress the image, then load it into Flash memory, you have no way of verifying that the image did not become corrupt during the TFTP process. For more information about verifying that your image is not corrupt, refer to the section “Verifying the New Image in Flash Memory” on page 20.

If you attempt to copy a new image into Flash memory when there is not enough space available, the copy process will begin but the entire image will not copy into Flash memory. A failure message, “*Buffer overflow - xxxx/xxxx*” will appear, where *xxxx/xxxx* is the number of bytes read in/number of bytes available. The partial image will remain in Flash memory until it is erased.

## Downloading the New Image

When you issue the **copy tftp** command for the first time, you are prompted for the IP address (or domain name) of the TFTP server. You are then prompted for the filename of the software image and given the option of erasing the contents of embedded (onboard) Flash memory or a Flash memory card. Accepting the default by pressing **Y** or the **Return** key clears the *entire* contents of Flash memory. If other images, such as updated microcode images, are stored in Flash memory, make sure you do not need these images or back them up before copying the new image into Flash memory.



### Note

Before you can copy an image to Flash memory, the write-protection jumper (J2) on the RP card must be installed. (See Figure 7.) If this jumper is removed, Flash memory is write protected and cannot be overwritten. The RP is shipped with this jumper installed; therefore, Flash memory can be overwritten by default.

The entire copying process takes several minutes, and this time differs from network to network.



### Note

Do not make any typographical errors while using the **copy tftp** command in selecting the filename of the image you are copying. If you type a filename that does not exist when using the **copy tftp** command and then tell the system to erase the current image, the router erases the existing image in Flash memory. If this happens, the router still has a working image in RAM and ROM, so your router will still function. If you think you have tried to load a nonexistent file, *do not reboot the router*. If you do, your router will not have a functional image in Flash memory. To recover from accidental Flash memory erasure, execute the **copy tftp** command again to load the appropriate image into Flash memory. If this procedure does not work, set up the router to boot from the ROM image and reboot it.

The filename can be lowercase or uppercase; the router will see the name as lowercase.



### Caution

If you accept the default for the prompt “erase flash before writing? [confirm]” by pressing either the **Y** key or **Return**, the entire contents of Flash memory will be erased. If your Flash memory contains files that you do not want to erase, back them up to a remote host before erasing Flash memory. (See “Backing Up the Current Contents of Flash Memory” on page 15.)

The following example shows an image named *new.image* being copied into Flash memory:

[illegible]



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.

The series of exclamation points (!!!!) in the preceding sample output indicates that the copying process is taking place. The series of Cs indicates that a checksum is being calculated. The last line in the sample configuration indicates that the file transfer is complete.

If the process was successful, proceed to “Verifying the New Image in Flash Memory” on page 20. If it was not successful, refer to the next section, “Recovering from a Flash Memory Failure.”



Note

To abort the copy process, simultaneously press **Control, Shift, and 6**. The process will abort; however, the partial file copied before the abort was issued will remain until the entire contents of Flash memory is erased.

## Recovering from a Flash Memory Failure

If the image fails to load properly into Flash memory, the following error message appears:

```
Error programming flash memory
```

If three or more attempts to load the image fail and result with this message, contact a technical support immediately. (Refer to the section “Obtaining Technical Assistance” on page 54.)

In an attempt to recover from the error, you also can erase the Flash memory and try to download the file again. You can repeat this procedure. To erase the Flash memory, issue the **copy tftp** command and press **Return** or the **Y** key at the following prompt:

```
erase flash before writing? [confirm] <Return>
```

Having successfully copied an image into Flash memory, you can display the image name by issuing the **show flash all** command.

```
Router# show flash all
4096K bytes of flash memory on embedded flash (in RP1).
 ROM socket code bytes name
 0 U63 012A 0x40000 AMD 28F020
 1 U62 012A 0x40000 AMD 28F020
(display text omitted)
security jumper(12V) is installed,
flash memory is programmable.

file offset length name
 0 0x80 3 test3
 1 0xC4 1305820 gs7-k.917-2.Z
 2 0x13EDE0 1305820 7k91720z
[1582404/4194304 bytes free]
```

## Verifying the New Image in Flash Memory

Before booting from Flash memory, verify that the checksum of the bundled image (shown at the bottom of the screen after you issue the **copy tftp** command) matches the checksum listed in the README file on the master upgrade disk. If the checksum values do not match, enter the **copy tftp** command and compare the checksums again.

You can also verify the presence and file size of the new image by displaying the contents of Flash memory with the **show flash** command. The Flash memory content listing does not include the checksum of individual files. To recompute and verify the image checksum after the image is copied into Flash memory, use the **copy verify** command. When you issue the command, the screen prompts you for the filename to verify. By default, it prompts for the last file in Flash memory (most recent). Press **Return** to recompute the default file checksum or enter the exact filename of a different file at the prompt.

Following are examples of the **show flash** and **copy verify** commands:

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

file offset length name
 0 0x80 2060240 gs7-k.103-8
 1 0x2577F0 98162 flip1-2
[1656560/4194304 bytes free]

Router# copy verify
Name of file to verify [flip1-2]? gs7-k.103-8
Verifying via checksum...
vvvvvvvvvvv
Flash verification successful. Length = 2060240, checksum = 0x0a42
Router#
```

After you verify that the checksum of the new image in Flash memory matches that listed in the README file on the upgrade disk, proceed to the next section to instruct the system to load the new file when you restart the router.

If the **copy tftp** and the **copy verify** commands result in a checksum that repeatedly does not match the checksum listed in the README file, do not reload or restart the router. Copy the original working image (or images) back into Flash memory, and contact a service representative for assistance. (Refer to the section “Obtaining Technical Assistance” on page 54.)



#### Caution

If you have a bad image in Flash memory and try to boot from Flash memory, the router will not function and must be reconfigured through a direct console port connection.

## Using Additional Flash Memory Commands

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

```
Router# pwd
slot0
```

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

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

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

```
Router# dir
-#- -length- ----date/time----- name
1 4601977 May 19 1994 09:42:19 myfile1
6 679 May 19 1994 05:43:56 todays-config
7 1 May 19 1994 09:54:53 fun1
```

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

```
Router# delete slot0:fun1
Router# dir
-#- -length- ----date/time----- name
1 4601977 May 19 1994 09:42:19 myfile1
6 679 May 19 1994 05:43:56 todays-config
```

To verify that the **delete** command was successful, use the **dir/all/long** command.



#### Note

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

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

Following is the syntax of the **squeeze** command:

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

To prevent loss of data due to sudden power loss, the “squeezed” data is temporarily saved to another location of Flash memory, which is specially used by the system.

In the previous command display output, the character “e” means this special location has been erased (which must be performed before any write operation). The character “b” means that the data that is about to be written to this special location has been temporarily copied. The character “E” signifies that the sector that was temporarily occupied by the data has been erased. The character “S” signifies that the data was written to its permanent location in Flash memory.

## Changing the Boot Instructions

Before you reboot with a new image, you must add boot instructions to the configuration file that specify the name and location of the new file (image) to load, and remove any old boot instructions from the configuration file. Otherwise, the system will continue (or attempt) to boot from ROM or from an older image, even though the new image is present in Flash memory. Also, if this is the first time you are upgrading the system software image, you will also need to change the position of a boot field jumper on the configuration register before the router can reboot with the new image in Flash memory. If you are already familiar with the boot field jumper settings and configuration file boot commands, proceed to the following section, “Automatically Booting from Flash Memory.”

The hardware configuration register is a 50-pin jumper block on the RP. The boot field jumper position determines the source of the software image that the system loads at startup. The factory default is to boot from ROM. If you have not changed the factory default setting (if you have not previously upgraded the software by loading a new image into Flash memory and your router is still booting from ROM), you will have to reset the boot field jumper before the system will boot from an image in Flash memory.

Otherwise, a newer system image can be present in Flash memory, but the router will continue to boot with the older image in ROM. To change the jumper setting, refer to “Changing the Boot Field Jumper” on page 43.

If you are running Cisco IOS Release 10.0 or later *and* have Cisco IOS Release 10.0 (or later) boot ROMs installed on the RP, you will access the boot field via the *software configuration register*, which is a feature in IOS Release 10.0 or later. (For complete information on the software configuration register functions, refer to the appropriate software documentation, and to the *RP Configuration and Installation* document, Document Number 78-1057-05 (or later).

**Note**


---

The RSP-based processor modules do not have a hardware configuration register, and use the software configuration register feature exclusively.

---

When the boot field jumper is set to boot from a filename (rather than booting from ROM, which is the factory default, or booting the router manually into the ROM monitor), the system looks in the configuration file for boot instructions. You must add a boot command to the configuration file that specifies the name of the new filename to load (the name of the new image), and the location of the new file (Flash memory). When you add this command to the configuration file, the router will automatically boot from the new image each time the system is restarted or reloaded.

Because the latest microcode images are now bundled and load with the system image, you should also remove any configuration file commands to load individual microcode images from a Flash file. (Earlier microcode images were distributed separately, and needed a line in the configuration file to instruct the system to load the newer microcode image from Flash memory at startup.) With bundled images, the system default is to load the microcode bundled with the system.

**Note**


---

We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility between the various interface processors in the system. The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is shipped separately on floppy disks, Flash memory cards, or is available via Cisco.com.

---

If the configuration file contains a line instructing the system to load a microcode image from Flash memory *and* the microcode image is still present in Flash memory, the command will override the new bundled image and will cause the older image in Flash memory to load instead. Or, if the microcode image was erased from Flash memory when you downloaded the new bundled image, the router will attempt to find and load a nonexistent file. To negate an existing microcode boot command in the configuration file, issue the command **no microcode interface-type flash filename**. (Refer to “Configuring Microcode” on page 26 for a description of this command.)

When the boot field jumper is set to boot into the ROM monitor, you must boot the router manually by specifying the name and location of the image to boot when you restart the router.

The following sections describe how to boot automatically or manually with the new image stored in Flash memory.

## Automatically Booting from Flash Memory

Whenever you add a new image to Flash memory to upgrade the system software, you must add a boot command **boot system flash *filename*** to the system configuration file, where the filename is the exact name of the new system software image. If you use the command **boot system flash** with no argument, the router will attempt to boot from the first file that was loaded into Flash memory. If the first file is a microcode image, the boot will fail. To avoid potential problems, it is good practice to specify the filename.

If your router is already booting from a system image stored in Flash memory, the configuration file contains the line **boot system flash *filename***, which instructs the system to boot the existing image. When you add a newer image to Flash memory to upgrade the system software, you must delete this line by issuing the **no boot system flash *filename*** system configuration command. If you do not do this, the router will repeatedly boot, or try to boot, with the older image.

To display the current configuration file, which includes any existing boot commands, issue the **write terminal (copy running-config)** command at the privileged-level prompt of the EXEC (Router#) as follows:

```
Router# write terminal (or copy running-config)
```

```
Current configuration:
version 10.3
!
hostname Router
!
microcode fip flash fip1-1
microcode sp flash spl-2
microcode reload
```

Configure the router to automatically boot from the image in Flash memory by following this procedure:

- 
- Step 1** Issue the **configure terminal** command in EXEC mode (at the enable [#] prompt).
  - Step 2** If the configuration file already contains instructions to boot from a specific filename, negate the existing command with the **no boot system flash *filename*** command.
  - Step 3** Add the **boot system flash *filename*** system configuration command to the configuration file, where *filename* is the exact name of the file that contains the new bundled image.



### Caution

If you use the command **boot system flash** with no argument, the router will attempt to boot from the first file that was loaded into Flash memory. If the first file is a microcode image, the boot will fail. To avoid potential problems, it is good practice to specify the filename.

- 
- Step 4** If the configuration file contains instructions to boot one or more older, individual microcode images from Flash memory or ROM, negate those commands with the **no microcode *interface-type* [flash | rom] [*filename*]** command. (See “Configuring Microcode” on page 26).
  - Step 5** Write the configuration to NVRAM with the **write memory (copy running-config startup-config)** command.

The following example shows the sequence of steps for replacing a 10.3(8) image with a 10.3(9) image, and for replacing individual microcode images in Flash memory with the newer images that are bundled with the new system image. The filenames shown are examples, and are not necessarily the exact names



of files that you might have currently configured to load in your system. Refer to the contents of the configuration file that you displayed earlier, and use the appropriate software and microcode image filenames for your own system configuration.

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#no boot system flash 7k1038z (Tells system not to boot old filename)
Router(config)#boot system flash 7k10390z (Tells system to boot new filename)
Router(config)#no microcode sp flash spl-2 (Tells system not to boot SP mcode from Flash)
Router(config)#no microcode fip flash fip1-1 (Tells system not to boot FIP mcode from Flash)
Router(config)#^Z
Router# write memory (copy running-config startup-config)
[ok]
Router#
```

**Step 6** Before you reload the system, issue the **write terminal (show running-config)** command to display the contents of the configuration file. Ensure that all old commands are negated and the instructions for booting with the new image are present. If changes are necessary, repeat Step 1 through Step 5 to edit or correct the boot commands.

**Step 7** When all the boot instructions are correct, issue the **reload** command.

The router boots the new software image from Flash memory. The following example shows the output of the **reload** command.

```
Router# reload
[confirm] <Return>

%SYS-5-RELOAD: Reload requested
System Bootstrap, Version 5.3(0.3), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
RP1 processor with 16384 Kbytes of main memory
F3: 8336+3474931+165004 at 0x1000
```

## Manually Booting from Flash Memory

You can also start up the router in the ROM monitor mode and then manually boot from Flash memory. This procedure requires that you shut down the router, remove the RP, and remove the jumper from the hardware configuration register boot field.

If you are running Cisco IOS Release 10.0 or later and have Cisco IOS Release 10.0 (or later) boot ROMs installed on the RP, you will access the boot field via the software configuration register, which is a feature in IOS Release 10.0 or later. (For complete information on the software configuration register functions, refer to the appropriate software documentation and to the *RP Configuration and Installation* document, Document Number 78-1057-05 (or later.)



### Note

The RSP-based processor modules (RSP7000, RSP1, and RSP2) do not have a hardware configuration register, and use the software configuration register feature exclusively.

Removing the boot field jumper causes the router to start up in the ROM monitor mode. From the ROM monitor, you must manually boot the router with the **b (boot)** command. Refer to “Removing and Replacing the RP, SP, SSP, and Interface Processors” on page 31 and to “Changing the Boot Field Jumper” on page 43.



To manually boot the router, perform the following steps:

- ```
System Bootstrap, Version 5.3(0.3), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
RP1 processor with 16384 Kbytes of main memory
F3: 8336+3474931+165004 at 0x1000
```

- [illegible]

Configuring Microcode

Whenever you perform any of the following actions, the system resets all processor modules, loads the microcode for each processor type, and enables the processor modules for operation:

- Boot the system
- Insert or remove a card

- Issue the **microcode reload** configuration command (which reloads all microcode but does not reboot the system)

All processor modules of the same type use the same microcode image. For example, the system loads only one EIP microcode image, and all EIPs in the router use that same image.

With bundled images, the default configuration is to load the new microcode images that are bundled with the new system image. Prior to these releases, software and microcode images were released and distributed separately. Because earlier (unbundled) microcode upgrades required loading the new image into Flash memory and modifying the configuration file to load the new image, your configuration file might contain commands that will affect the new default.



Note

As of Cisco IOS Release 10.0 and later, the software and interface processor microcode images are carefully optimized and bundled to work together. Overriding the bundle can result in incompatibility between the various interface processors in the system. The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is unbundled and shipped as a separate package on floppy disks, Flash memory cards, or is available via Cisco.com.

The following sections describe how to configure the system to load a specific microcode image, negate existing configuration instructions to enable the system default of loading the bundled images, and display a list of the currently installed and running microcode versions.

Changing Microcode Boot Instructions

Although it is recommended that you should use the bundled microcode images, you can override the default if a bundled image appears damaged, or if you discover a bug or other problem in the bundled image. Also, if your configuration file currently contains commands that instruct the system to boot microcode either from ROM or from a Flash memory file, you will need to negate those commands. Otherwise, the commands will override the default of loading the bundled images. If the microcode for a particular interface processor type is somehow corrupted during file transfer, the system will boot the microcode image from the ROM on the interface processor.



Caution

Remove all preexisting microcode configuration commands from the configuration file. Otherwise, they will override the system default of loading the bundled images, and will cause the system to continue loading the older microcode images.

To specify the source of a microcode image that you want to load instead of the bundled image, issue the following command:

```
microcode interface-type [flash | rom] [filename]
```

To negate an existing microcode configuration, use the **no** keyword followed by the command exactly as it appears in the configuration file, as follows:

```
no microcode interface-type [flash | rom] [filename]
```

The argument *interface-type* is one of the following processor names: **aip**, **cip**, **eip**, **fip**, **feip**, **fsip**, **hip**, **mip**, **sip**, **sp**, **ssp**, **trip**, or **vip**.

Use the **rom** keyword to load the microcode image from the microcode ROM on a specific processor type. No further arguments are necessary, and all processors of the same type will use the image from the microcode ROM instead of the bundled microcode image. For example, the command **microcode fip rom** specifies that the system will load the FIP microcode image from the ROM in socket U23 on the FIP instead of loading the FIP microcode image that is bundled with the new system image.

Use the **flash** keyword to specify a microcode image stored in Flash memory, and use the argument *filename* to specify the exact name of the file in which the image is stored. The default configuration is to load the microcode that is bundled with the system image. To retain the default configuration, negate any existing microcode configuration commands in the file with **no** followed by the exact command. For example, if the current configuration file contains the command:

```
microcode fip rom
```

Negate it with the following command:

```
no microcode fip rom
```

Otherwise, the system will load the microcode from the FIP microcode ROM (U23) instead of the FIP microcode image that is bundled with the new system image. Because the latest microcode image is bundled with the system images, this could result in an older, possibly incompatible microcode image loading instead of the latest available image.

To retain new configuration information, enter the **write memory** command at the EXEC prompt after entering microcode configuration commands.

Listing the Bundled Microcode Versions

The **show microcode** command lists all of the microcode images that are bundled with the system software image. In order to support online insertion and removal (OIR), the system loads a microcode image for all available processor types.

Following is sample output for the **show microcode** command:

```
Router# show microcode <Return>
```

```
Microcode bundled in system
```

Card Type	Microcode Version	Target Hardware Version	Description
SP	10.4	11.x	SP version 10.4
SSP	10.4	12.x	SP version 10.4
EIP	10.0	1.x	EIP version 10.0
TRIP	10.1	1.x	TRIP version 10.1
FIP	10.1	2.x	FIP version 10.1
HIP	10.0	1.x	HIP version 10.0
SIP	1.2	1.x	SIP version 1.2
FSIP	10.3	1.x	FSIP version 10.3
MIP	10.1	1.x	MIP version 10.1
AIP	10.1	1.x	AIP version 10.1

(As of Cisco IOS Release 11.1[1], CIP microcode is no longer bundled.)



Note

The combinations of microcode shown in the preceding example are not typical of a standard configuration. We strongly recommend that the microcode bundled with the system software be used as a package. Overriding the bundle could possibly result in incompatibility among the various interface processors. The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is unbundled and shipped as a separate package on floppy disks, Flash memory cards, or is available via Cisco.com.

The microcode version and description lists the bundled microcode version for each processor type, which is not necessarily the version that is currently loaded and running in the system. A microcode image that is loaded from ROM or a Flash memory file is not shown in this display. To display the currently loaded and running microcode version for each processor type, issue the **show controller cbus** command.

The target hardware version lists the minimum hardware revision required to ensure compatibility with the new software and microcode images. When you load and boot from a new bundled image, the system checks the hardware version of each processor module that it finds installed and compares the actual version to its target list. If the target hardware version is different from the actual hardware version, a warning message appears when you boot the router, indicating that there is a disparity between the target hardware and the actual hardware. You will still be able to load the new image, however, contact a service representative for information about upgrades and future compatibility requirements. (Refer to the section “Obtaining Technical Assistance” on page 54.)

Repeating the Installation Process

Before repeating the system software upgrade process on subsequent machines, make sure the upgraded router functions properly by performing the following steps:

-
- Step 1** Ping from the upgraded router to a system on the local network to make sure you have network connectivity. Refer to “Testing the TCP/IP Software” on page 12.
 - Step 2** Look at the routing tables in the updated router. To review all of the routes established in your router, issue the **show protocol route network EXEC** command.
 - Step 3** Make sure the upgraded router is listed properly in the routing tables of nearby routers.
 - Step 4** If the command **boot system flash filename** exists as a line in the configuration file on a subsequent router to be upgraded, remove the argument *filename* from the command before rebooting the router. Refer to “Automatically Booting from Flash Memory” on page 24.

If the **ping** and **show route** commands generate positive results, upgrade subsequent routers.

Upgrading Software and Microcode with Replacement ROMs

This section describes the procedures for replacing the system software ROMs on the RP and the single microcode ROM on the SP, SSP, and interface processors. Cisco 7000 family routers support downloadable software and microcode, which in most cases allows you to download, store, and boot with new (upgraded) images without having to physically access the router to replace ROMs. Occasionally, ROM replacement is necessary to ensure that the router can boot and operate properly.

Procedural Overview

This procedure describes the general steps required to upgrade your system software or microcode by replacing the ROMs. The sections that follow describe these steps in greater detail.

-
- Step 1** Gather the tools and equipment you will need to complete the upgrade.

- Step 2** If you will remove the RP (to replace system software ROMs) or the SP or SSP (to replace the SP or SSP microcode ROM), turn off power to the system. All CxBus interface processors support OIR, so it is not necessary to shut down the system to remove and replace interface processors.



Note The RSP7000 and RSP processor modules do not have microcode ROM devices.

- Step 3** Remove the appropriate processor module (RP, SP, SSP, or any interface processor).
- Step 4** Replace the ROM components.
- Step 5** If necessary, change jumper settings on the RP to reflect a change to the size (capacity) of the system software ROMs, or to change the configuration register boot field instructions.
- Step 6** Replace the processor module in the chassis.
- Step 7** Restart the system (if it is shut down) and verify that it boots (or reloads) successfully.
- Step 8** Use **show** commands to verify that the new image is loaded and running.
- Step 9** If necessary, modify the boot commands in the system configuration file.
- Step 10** Repeat Steps 7 through 9 until the router boots and runs successfully with the new image.

Tools and Equipment

You need the following tools to replace the microcode component:

- Number 1 Phillips or 3/16-inch flat-blade screwdriver for the captive installation screws (Most systems use Phillips screws, but early systems used slotted screws.)
- Chip extractor or puller (You need a PLCC-type extractor to remove the FSIP component.)
- Needlenose pliers to straighten any bent pins
- Antistatic mat or foam pad
- Grounding strap (A disposable wrist strap is included in microcode upgrade kits.)

Whenever you handle interface processors, use a wrist strap or other grounding device to prevent electrostatic discharge (ESD) damage to components. Refer to the section “Preventing Electrostatic Discharge (ESD) Damage.”

Preventing Electrostatic Discharge (ESD) Damage

ESD damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Each processor module comprises 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 handling any electronic system component. Handle processor modules by the handles and the carrier edges only; never touch the boards or connector pins. 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 or to one of the following grounding points:

- When installing a processor module, use the ejector levers to properly seat the bus connectors in the backplane, then tighten both captive installation screws. These screws prevent accidental removal, provide proper grounding for the system, and they help to ensure that the bus connectors are seated in the backplane.
- Handle processor modules by the carrier handles and carrier edges only; avoid touching the board or any connector pins.
- Place a removed processor module board-side-up on an antistatic surface or in a static shielding bag. If you will return the module to the factory, immediately place it in a static shielding bag.
- Avoid contact between electronic equipment and clothing. Antistatic straps only protect the equipment 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 megohms.

Removing and Replacing the RP, SP, SSP, and Interface Processors

The online insertion and replacement (OIR) feature allows you to remove and replace CxBus interface processors while the system is operating; you do not need to notify the software or shut down the system power. All CxBus interface processors (AIP, CIP, EIP, FIP, FEIP, FSIP, HIP, MIP, and TRIP,) support OIR. The RP, SP, and SSP processor modules, which are required system components, should not be removed and replaced without first shutting down the system.

**Note**

Figure 1, Figure 2 , Figure 3, and Figure 4 show the currently shipping Cisco 7000 series routers and the locations of the interface processor and RP and SP (or SSP) slots in each.

Figure 1 Cisco 7000 with RP and SP (or SSP) Installed

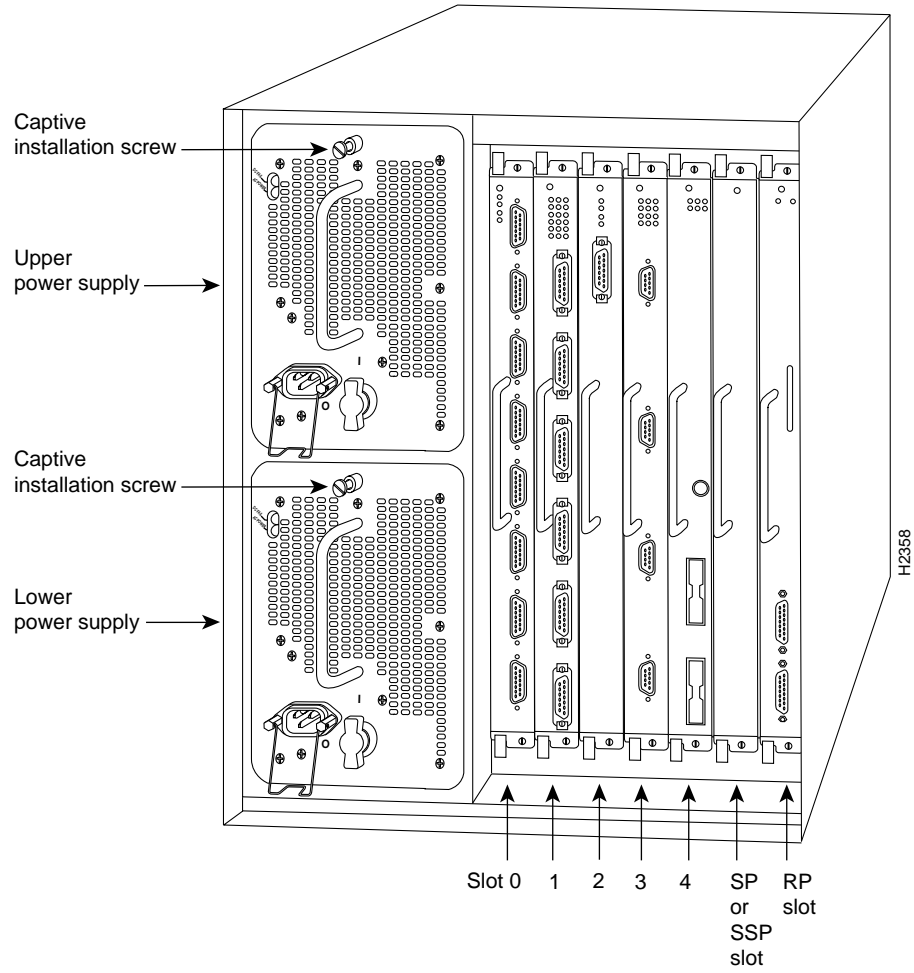


Figure 2 Cisco 7000 with RSP7000 and RSP7000CI Installed

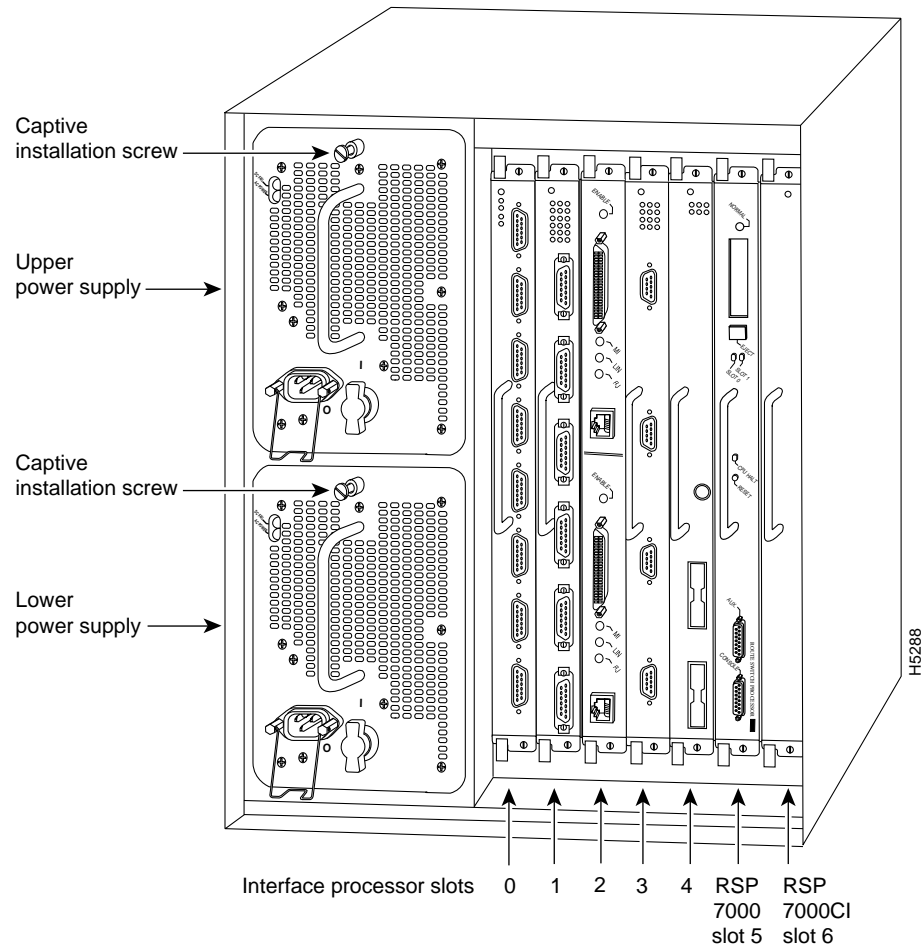


Figure 3 Cisco 7010 with RP and SP (or SSP) Installed

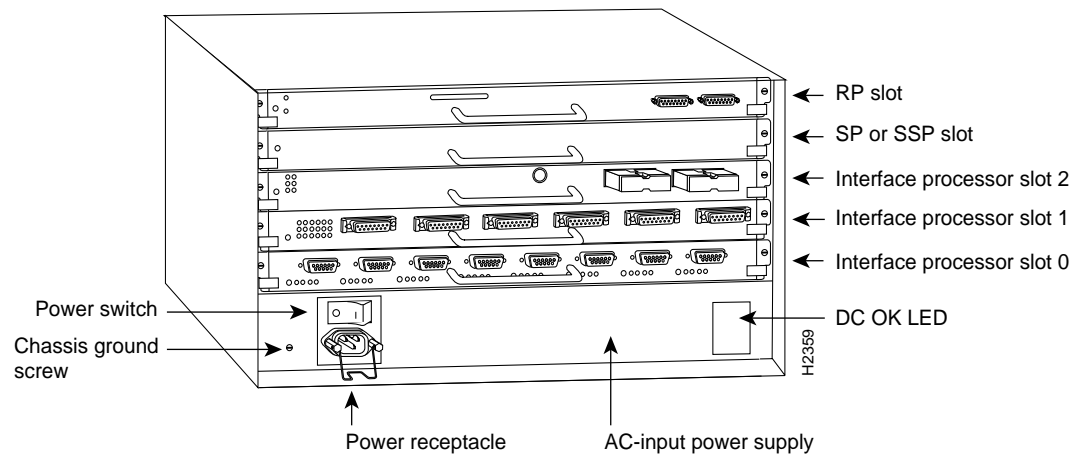
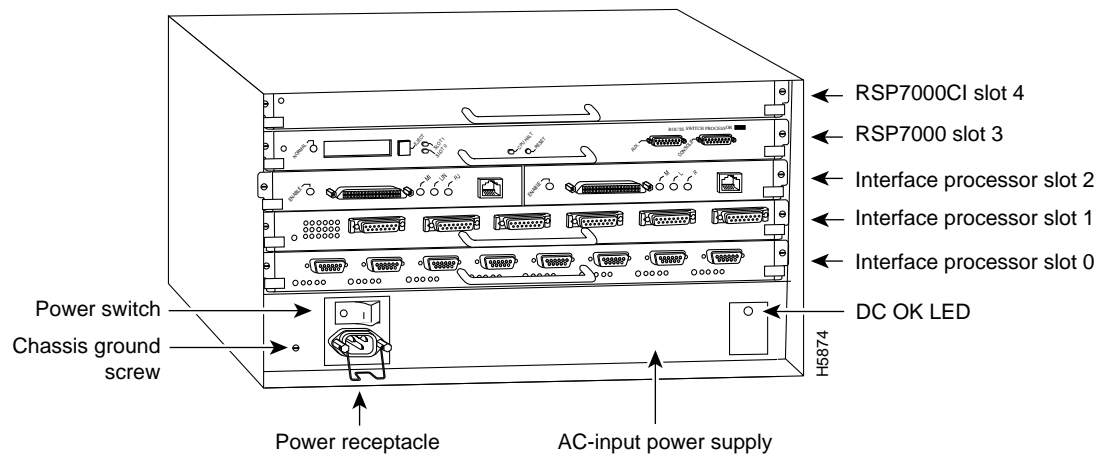


Figure 4 Cisco 7010 with RSP7000 and RSP7000CI Installed

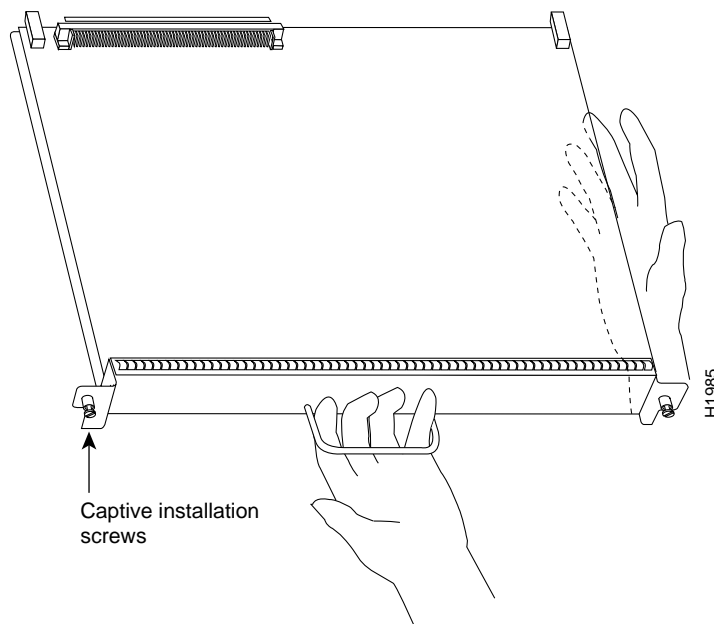


Removing the RP, SP, SSP, or Interface Processors

Following are detailed steps for removing the RP, SP, SSP, and interface processors. Be sure to use the ejector levers to ensure that the system continues proper operation. Failure to use the ejector levers properly can result in a partial connection between the board connectors and the backplane, which can cause the system to hang and subsequently crash. For detailed descriptions of the OIR function, refer to the *Cisco 7000 Hardware Installation and Maintenance* and *Cisco 7010 Hardware Installation and Maintenance*.

Figure 5 shows proper handling of a processor module for installation in the Cisco 7010 models. The processor slots are oriented horizontally in the Cisco 7010 and vertically in the Cisco 7000. For this latter chassis, handle the interface processor in the same manner but rotated 90 degrees clockwise.

Figure 5 Handling a Processor Module During Installation



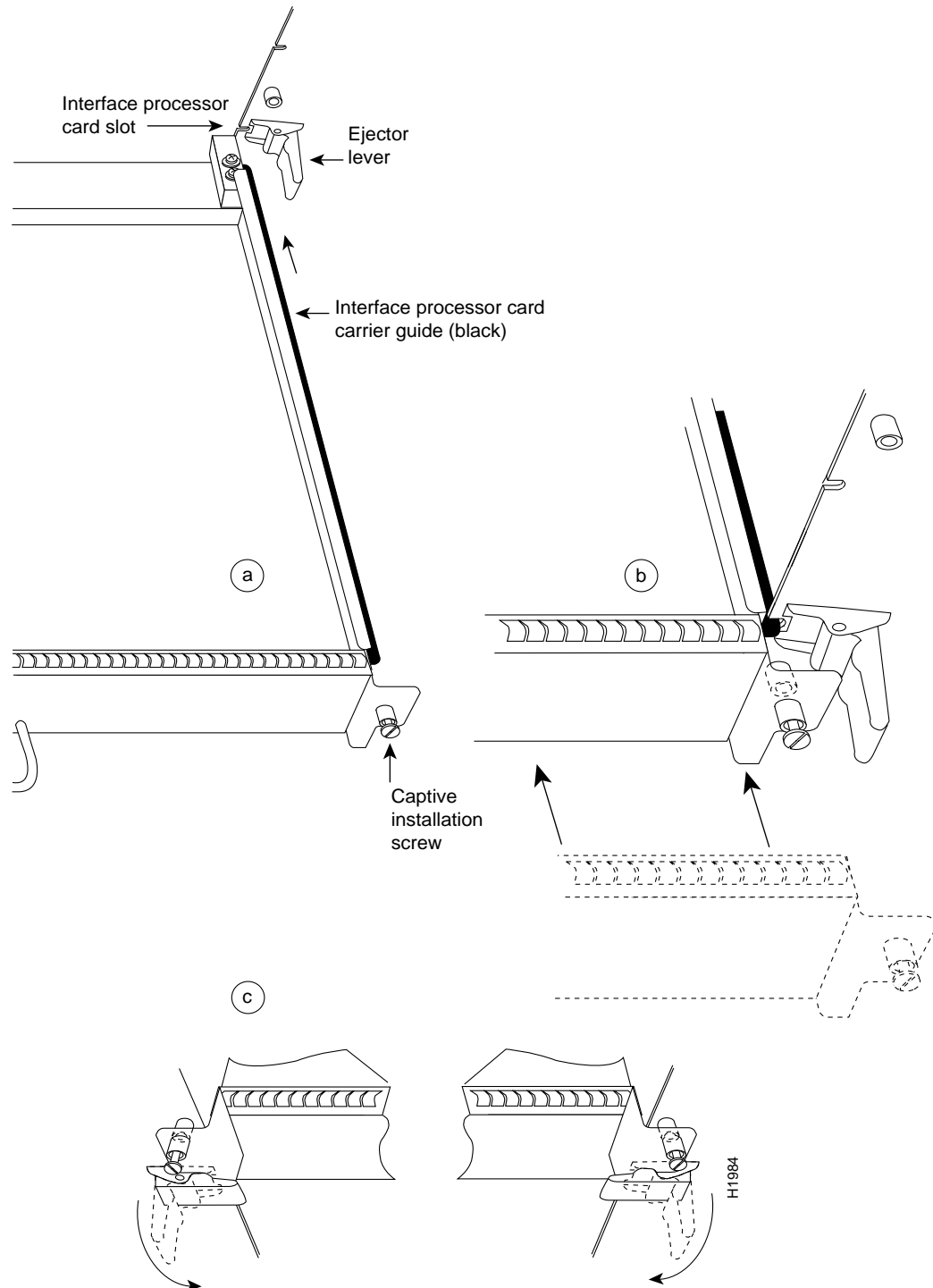
**Caution**

The RP, SP, and SSP are required system components; removing any of them without first shutting down the system will cause an abrupt shutdown and can damage or destroy memory files.

Follow these steps and refer to Figure 6 to remove a processor module:

-
- Step 1** If you are removing the RP, SP, or SSP, shut down the system by turning off all power supplies.
 - Step 2** Check the slack on any network interface cables connected to the processor module you will remove. If you can remove the processor module and replace the ROMs (RP only) without straining the cables, leave the cables connected to the ports; otherwise, disconnect them.
 - Step 3** Use a screwdriver to loosen both of the captive installation screws on the processor module.

Figure 6 *Ejector Levers and Captive Installation Screws*



Note

Processor modules are oriented horizontally in the Cisco 7010 and vertically in the Cisco 7000.

- Step 4** Place your thumbs on the ends of each of the ejector levers and simultaneously pull them both outward, away from the carrier handle (in the opposite direction from that shown in c). This action also releases the board connector from the backplane.
- Step 5** Grasp the handle with one hand and carefully pull the processor module straight out of the slot, keeping your other hand underneath the carrier to guide it. (See Figure 5) Keep the carrier at a 90-degree orientation to the backplane.
- Step 6** Place the removed processor module on an antistatic mat or antistatic foam and proceed to one of the following sections:
- “Upgrading the System Software ROMs” on page 39
 - “Upgrading Microcode ROMs” on page 46

Replacing the RP, SP, SSP, or Interface Processors

Following are the steps for replacing the RP, SP, SSP, or interface processors in the router.



Caution

You must turn off the system power before removing or installing an RP, SP, or SSP. After the chassis power has been turned off, the installation and removal procedure is the same as that for interface processors.

- Step 1** If you are replacing the RP, SP, or SSP, ensure that all system power is turned off. The system cannot operate without both an RP and SP (or SSP) installed, but inserting either one when the power is on can cause a partial backplane connection, prevent the system from starting up properly, and damage or destroy memory files.
- Step 2** Hold the handle with one hand, and place your other hand under the carrier to support and guide it into the slot (See Figure 5). Avoid touching the board.
- Step 3** Place the back edge of the carrier in the slot and align the notches along the edge of the carrier with the grooves in the slot. (See part a of Figure 6).
- Step 4** While keeping the processor module at a 90-degree orientation to the backplane, carefully slide it into the slot until the faceplate makes contact with the ejector levers, then *stop*. (See part b of Figure 6).



Caution

Always use the ejector levers when installing or removing processor modules. A module that is partially seated in the backplane will cause the system to hang and subsequently crash, and shoving or slamming the interface processor into the slot can damage the backplane and connector pins.

- Step 5** Using the thumb and forefinger of each hand to pinch the ejector levers, simultaneously push both ejector levers inward (toward the carrier handle) until they snap into place and are at a full 90-degree orientation to the faceplate. (See Part c of Figure 6).
- Step 6** Use a screwdriver to tighten the two captive installation screws on the interface processor faceplate to prevent the interface processor from becoming partially dislodged from the backplane and to ensure proper EMI shielding. (These screws must be tightened to meet EMI specifications).
- Step 7** Replace any network interface cables or other devices that you removed from the interface ports.
- Step 8** If the system is shut down, turn the system power back on.
- Step 9** Check the console terminal, and verify that it displays the expected information according to the descriptions that follow.

When you remove and replace CxBus interface processors, the system provides status messages across the console screen. The messages are for information only. In the following sample display, you can follow the events logged by the system as an EIP was removed from slot 3, then the system reinitialized the remaining interface processors and marked the EIP that was removed from slot 3 as *down*. When the EIP was reinserted, the system marked the interfaces as *up* again.

```
Router#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
%LINK-5-CHANGED: Interface TokenRing4/0, changed state to initializing
%LINK-5-CHANGED: Interface Ethernet3/1, changed state to administratively down
%LINK-5-CHANGED: Interface Ethernet3/5, changed state to administratively down
%LINK-5-CHANGED: Interface TokenRing4/0, changed state to up
```

```
Router#
%OIR-6-INSCARD: Card inserted in slot 3, interfaces administratively shut down
%LINK-5-CHANGED: Interface TokenRing4/0, changed state to initializing
%LINK-5-CHANGED: Interface Ethernet3/1, changed state to up
%LINK-5-CHANGED: Interface Ethernet3/5, changed state to up
%LINK-5-CHANGED: Interface TokenRing4/0, changed state to up
```

When you restart the system after replacing the RP, SP or SSP, the console displays the system startup banner, which lists the system software version and all interface types, as follows:

```
Restricted Rights Legend
System Bootstrap, Version 5.3(0.3), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
RP1 processor with 16384 Kbytes of main memory
F3: 8336+3474931+165004 at 0x1000

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) GS Software (GS7-K), Version 10.3(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 01-Nov-95 13:55 by vatan
Image text-base: 0x00001000, data-base: 0x0061E5B4

RP (68040) processor with 16384K bytes of memory.
G.703/E1 software, Version 1.0.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
1 EIP controller (2 Ethernet).
2 FSIP controllers (4 Serial).
2 Ethernet/IEEE 802.3 interfaces.
4 Serial network interfaces.
128K bytes of non-volatile configuration memory.
4096K bytes of flash memory sized on embedded flash.
8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
```

If the system does not display these message or otherwise displays an error message or fails to restart properly, turn off the system power and check the RP, SP, SSP, and interface processor to ensure that all are properly seated. If a second startup attempt fails, contact a service representative. (Refer to the section “Obtaining Technical Assistance” on page 53.)

Upgrading the System Software ROMs

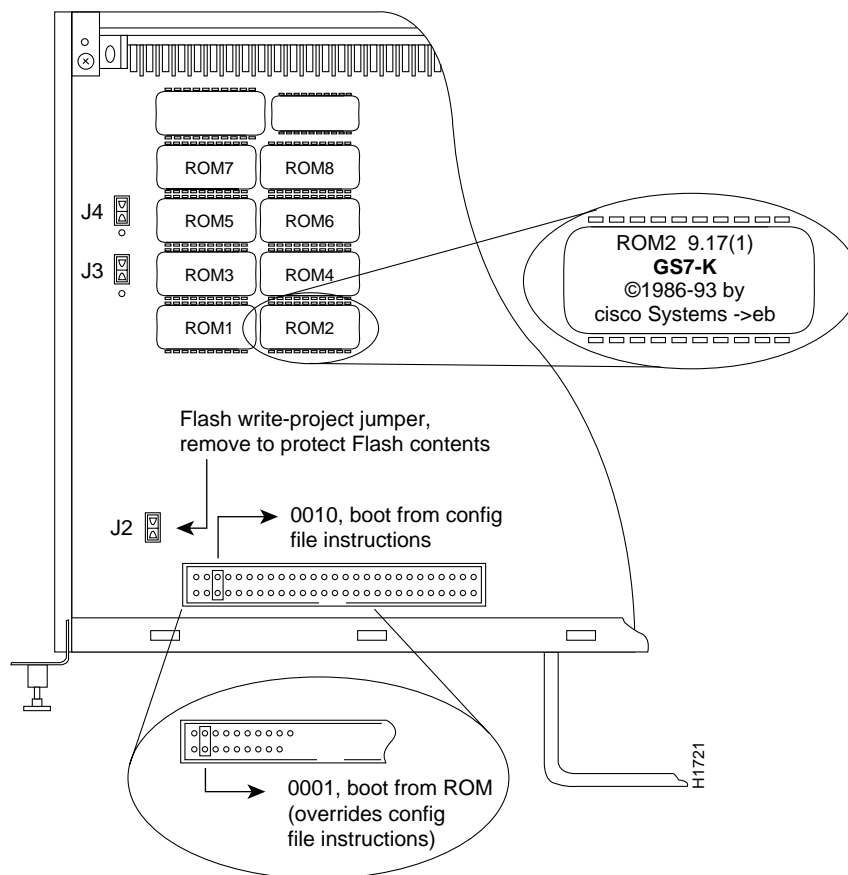
This section describes procedures for upgrading the system software by replacing the eight read-only memory (ROM) components on the RP and, if necessary, changing the positions of the jumpers on J3 and J4. Currently, most maintenance releases for Software Releases 9.17 and 9.21 are distributed on floppy disk instead of on replacement ROMs (as is done for earlier releases). However, you will need this procedure if ROM replacement is required for a future upgrade or if you want to change the default system boot ROMs in your router.

Cisco 7000 series routers can also netboot system software images, or netboot as part of a fault-tolerant strategy if attempts to boot a Flash memory or ROM image fails. Refer to the appropriate software configuration documentation for details.

Replacing the ROMs

For the RP, the software resides on a set of eight ROMs. The ROMs are labeled with a number that corresponds to the ROM socket in which it should be installed. The sockets have labels too, although obscure, on the silk-screen portion of the RP board. Each ROM has a notch cut on one end to indicate proper orientation. Position new ROMs with the notches in the same position as the notches silkscreened onto the ROM socket. Do *not* rely on the orientation of the ROM labels to indicate the correct position on the board. Figure 7 shows the ROM numbers of each socket and the location of each on the RP.

Figure 7 System Software ROMs, Hardware Configuration Register, and Jumpers J2, J3, and J4











The jumpers on J3 and J4 (see Figure 7) correspond to the size (capacity) of the eight system software ROMs. Figure 7 shows the orientation of J3 and J4 on the RP when set for 2 MB. If you replace the system software ROMs with new ROMs of a different size (larger or smaller than the ROMs you remove), you will also need to change the jumper settings on J3 or J4.

The initial release of System Software 9.17 and all subsequent maintenance releases up to 9.17(6.3) were distributed on 2-MB ROMs. Maintenance release 9.17(7) and subsequent maintenance releases to 9.17, and all releases of Release 9.21, reside on 4-MB ROMs. Cisco IOS Release 10.0 or later resides on 4-MB ROMs. Figure 8 shows the settings for various ROM sizes.

For example, if you are installing a new image that resides on 4-MB ROMs, you will need to move the jumper on J3 from the upper two posts to the lower two posts. This action is not required if you upgrade by downloading a new software image into Flash memory; it is necessary only when you physically replace the ROMs.

Figure 8 Jumper Settings for Software ROM Sizes

Jumper	EPROM Types	27010	27020	27040	27080
	Memory	1 Mb	2 Mb	4 Mb	8 Mb
J4					
J3					

H1485a

Follow these steps to upgrade the ROMs in the RP:

- Step 1** Turn off all system power and disconnect any devices connected to the RP console and auxiliary ports.
- Step 2** Put on a wrist strap or other antistatic device and connect the equipment end to the captive installation screw on an installed interface processor, or to another grounding point.
- Step 3** Follow the procedure in “Removing and Replacing the RP, SP, SSP, and Interface Processors” on page 31 to remove the RP from the router and place it on an antistatic mat or foam pad.
- Step 4** Referring to Figure 7, locate the eight system software ROMs. The label on each installed ROM indicates the ROM number (1 through 8) as shown. Note the orientation of the notches on the end of each ROM to aid in inserting the new ones. Do not rely on the orientation of the ROM labels for correct positioning.
- Step 5** Use a chip extractor to remove the first ROM from its socket. If you do not have a chip extractor available, use the tip of a screwdriver blade to gently pry the ROM out of its socket.

**Caution**

The correct placement of the ROM is crucial. If improperly positioned, the ROM could be damaged when the system is powered on. Also, to prevent damage to the board or any of the components from electrostatic discharge, be sure to follow the ESD procedures described in the section “Preventing Electrostatic Discharge (ESD) Damage” on page 30.

- Step 6** Install the new ROM in the same numbered socket as the old ROM you just removed. Observe the correct notch orientation for the new ROM.
- Step 7** Repeat Steps 5 and 6 until all new ROMs are installed. Be careful not to bend or break any of the pins. Use needlenose pliers to straighten a bent pin. If a pin breaks, you must obtain a replacement.
- Step 8** Check the positions of jumpers J3 and J4, and compare them to the jumper position shown in Figure 8. Refer to for the correct jumper settings and change them if necessary for the ROMs you just installed.

- Step 9** On the configuration register (on the RP only), verify that a jumper is installed on one of the following bits:
- To direct the system to boot from ROM only and ignore all boot instructions in the system configuration file, place the jumper on bit 0. Bit 0 is the far left jumper pair when viewing the RP in the orientation shown in Figure 7.
 - To direct the system to use the boot instructions in the configuration file, place a jumper on any one of the other three boot field bits: bit 1, 2, or 3.
- Refer to “Changing the Boot Field Jumper” on page 43 for specific instructions for configuring boot instructions.
- Step 10** When all ROMs have been replaced, follow the steps in “Replacing the RP, SP, SSP, or Interface Processors” on page 37 to reinstall the RP.
- Step 11** Reconnect any console or auxiliary port cables to the connectors on the RP.
- Step 12** Turn on the system power and proceed to the next section to check the installation.

Checking the Installation

When you restart the system after replacing the system software ROMs, the system console should display the startup system banner similar to the following example, and the software version should indicate that the router booted from the new ROMs that you just installed.

```

Restricted Rights Legend
System Bootstrap, Version 5.3(0.3), SOFTWARE
Copyright (c) 1986-1995 by cisco Systems
RP1 processor with 16384 Kbytes of main memory
F3: 8336+3474931+165004 at 0x1000

(displayed text omitted)

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) GS Software (GS7-K), Version 10.3(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 01-Nov-95 13:55 by biff
Image text-base: 0x00001000, data-base: 0x0061E5B4

```

Verify the installation with the following steps:

- Step 1** Check the software version and boot source shown in the system banner. The preceding example shows System Software Release 10.3(9) booted from ROM:
- System image file is "gs7-k.103-9", booted via ROM
- If the display shows the correct (new) software version, the replacement is complete.
 - If the system boots successfully but did not boot from the new ROMs (if the system boots an image from Flash memory or netboots from a remote server), you will need to configure the boot instructions. Proceed to “Changing the Boot Field Jumper” on page 43.
 - If the system fails to start up or reports a checksum error, or if the CPU halt or boot error LEDs on the RP remain on, proceed to the next step.

- Step 2** Turn off all system power and use the ejector levers to ensure that the RP is fully seated in its slot. Use the eject levers to eject the RP, then use the ejector levers again to seat it. If necessary, refer to “Removing and Replacing the RP, SP, SSP, and Interface Processors” on page 31.
- Step 3** After reseating the RP, turn the system power back on. If reseating the RP corrected the problem, return to step 1. If it did not, proceed to the next step.
- Step 4** Turn off the system power and remove the RP to check the condition of the ROMs you just installed.
- Check each of the ROMs to ensure that all are seated properly.
 - Carefully check around the edges of each ROM socket to ensure that none of the pins are bent and that each pin is in its socket.
 - If you find a bent or unsocketed pin, remove the ROM, straighten any bent pins with needlenose pliers, then carefully replace the ROM in the socket. If a pin breaks, you must obtain a replacement ROM.
- Step 5** After replacing the RP, turn the power supplies back on. If reseating the RP corrected the problem, return to step 1.
- Step 6** If the console screen continues to display a checksum error, or if the CPU halt or boot error LEDs continue to stay on, contact a service representative for assistance. Report the steps you have already taken to isolate the problem, and any messages displayed on the console screen.
- This completes the installation verification.

Changing the Boot Field Jumper

The hardware configuration register is a 50-pin jumper block near the front of the RP. (See Figure 7.) The lowest four bits (bits 0 through 3, shown at the far left of the hardware configuration register in Figure 7) form the boot field. The jumper settings of the four boot field bits form a binary value that defines the boot source for the system. This procedure addresses only the settings for booting from ROM and for booting from the instructions in the configuration file. The section “Manually Booting from Flash Memory” on page 25 describes the steps for starting up in the ROM monitor and manually booting from Flash memory.

This section describes the hardware configuration register boot field jumper settings required for each boot method. For a complete description of the configuration register, refer to the following hardware publications: *Route Processor (RP) Installation and Configuration* (Document Number 78-1057-xx), *Cisco 7000 Hardware Installation and Maintenance*, or *Cisco 7010 Hardware Installation and Maintenance*.



Note

If you are running Cisco IOS Release 10.0 or later, *and* you have Cisco IOS Release 10.0 (or later) boot ROMs installed on the RP, the hardware configuration register on the RP is ignored, and the software configuration register feature, available in Cisco IOS Release 10.0, is enabled. If you are running Cisco IOS Release 10.0 or later, and you *do not* have Cisco IOS Release 10.0 (or later) boot ROMs installed in the RP, then the software configuration register feature will not be recognized by the system and the hardware configuration register will be the default. For a complete description of the functions of the software configuration register feature, refer to one of the following hardware publications: *Route Processor (RP) Installation and Configuration* (Document Number 78-1057-05 [or later]), or the hardware installation and maintenance publications listed in the section ““If You Need More Information” on page 52.”

Figure 8 shows the four boot field bits in the hardware configuration register, which are used in systems running software releases other than Cisco IOS Release 10.0 or later.

Removing the jumper completely from the boot field sets the boot field value to 0, which causes the router to start up in the ROM monitor mode. From the ROM monitor, you must manually boot the router with the **b (boot)** command. (Refer to “Manually Booting from Flash Memory” on page 25.)

A jumper on bit 0 sets the boot field value to 1 (the factory default), which directs the system to boot from the software ROMs. This setting overrides all boot instructions in the system configuration file.

Moving the jumper to any of the other 3 boot field bits directs the system to use the boot instructions in the configuration file. (The system also uses the boot field value to form a filename that it uses for netbooting if it does not find boot instructions in the configuration file; refer to the aforementioned hardware publications for a complete description.)

The factory default boot field setting is 1 (a jumper is on bit 0). However, if you have downloaded and stored a newer system image in Flash memory, you would have had to move the jumper to one of the other three boot field bits, 1, 2, and 3. To set the system to boot from ROM always and ignore all boot instructions in the system configuration file, place the jumper on bit 0. If you choose this setting, however, you will have to change the jumper before the system can boot from a new image stored in Flash memory, or netboot from a remote router or server.

A more practical and fault-tolerant approach is to set the jumper to any of the other three bits and provide boot instructions in the system configuration file, which you can edit and reconfigure from the system console. Setting boot instructions in the configuration file allows you to define more than one boot source, which directs the system to alternate sources in case the primary boot source fails or is not available. List boot source instructions in the same order that you wish the system to execute them. Use the following commands to direct the system to a boot image:

- Use the **boot system rom** configuration command to instruct the system to boot from the default image in ROM.
- Use the **boot system flash [filename]** command to boot from an image stored in Flash memory. If you do not specify the filename, the router will attempt to boot the first undeleted file it finds, which may not be a system image file.
- Use the **boot system filename [address]** command to netboot (boot an image that the router retrieves from a remote router or server).

The following example shows a fault-tolerant boot sequence, which will first attempt to boot from the Flash file g7-103.9. If it cannot boot from this file, it attempts to netboot from a server at the IP address 1.1.1.101. If it cannot netboot, it will boot from ROM. This example assumes that the hardware configuration register boot field (bits 0 through 3) is set to a value of 0x0002 or greater.

```
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#boot system flash g7-103.9
Router(config)#boot system g7-103.9 1.1.1.101
Router(config)#boot system rom
Router(config)#^z
Router# write memory (copy running-config startup-config)
[ok]
Router#
```

```
Router# conf term
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#config-register 0x002
Router(config)#boot system flash g7-103.9
Router(config)#boot system g7-103.9 1.1.1.101
Router(config)#boot system rom
Router(config)#^z
Router# write memory (copy running-config startup-config)
[ok]
Router#
```



The following example session instructs the system to boot from the image in ROM, saves the new configuration by writing it to NVRAM, then issues a **reload** command to execute a soft boot to reload the new software according to the new configuration instructions:

```
Router> enable  
Password: (not displayed)  
  
Router# configure terminal  
Enter configuration commands, one per line.  
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z  
Router(config)#boot system rom  
Router(config)#^z  
  
Router# write memory (copy running-config startup-config)  
[ok]  
Router#  
Router# reload  
[confirm]  
  
%SYS-5-RELOAD: Reload requested  
Cisco Internetwork Operating System Software  
IOS (tm) GS Software (GS7-K), Version 10.3(9), RELEASE SOFTWARE (fc1)  
Copyright (c) 1986-1995 by cisco Systems, Inc.  
Compiled Wed 01-Nov-95 13:55 by biff  
  
Booting from g7-l03.9 from rom  
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR  
(displayed text omitted)  
RRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK - 1582404/4194304 bytes]  
F1: 1871414+45476+167028 at 0x1000
```

Use, duplication, or disclosure by the Government is
(displayed text omitted)

Setting the Flash Write-Protect Jumper

On the RP, jumper J2 provides Flash write protection. A jumper is installed on J2, which is the factory default and allows writing (copying) to Flash memory. To protect the contents of Flash memory (which prevents writing to it), remove the jumper from J2; however, you must replace the jumper on J2 before you can download or copy any new files or system images to Flash memory.

Figure 7 shows the location of J2, which is just behind and to the left of the configuration register when viewing the RP in the orientation shown.

Upgrading Microcode ROMs

Microcode is board-specific firmware that resides on ROM on the SP, SSP and on each interface processor. As new software and hardware features are introduced, the microcode may be updated and maintenance versions are released in order to implement new features, improve performance, or fix bugs found in earlier versions. Effective with Cisco IOS Release 10.0, microcode images for all interface processors are bundled with system software upgrades and load automatically with the new system image.

**Note**

The exception to this is CIP microcode, which, as of Cisco IOS Release 11.1(1), is unbundled and shipped as a separate package on floppy disks, Flash memory cards, or is available via Cisco.com.

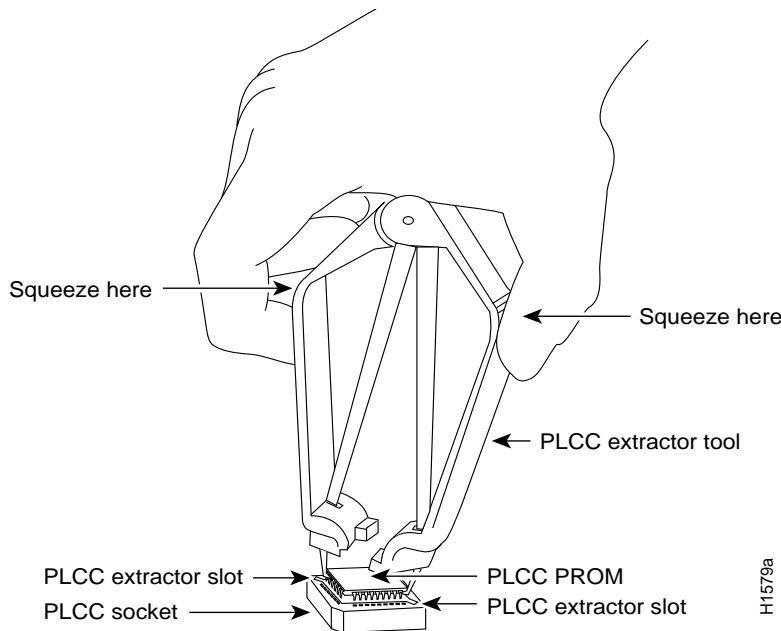
Although in most cases the newer images loaded from Flash memory will override the default ROM images, some exceptions require ROM replacement to ensure proper startup and operation. Currently, SP Microcode Version 1.4 is the only microcode maintenance release for which ROM replacement is required; all previous microcode maintenance releases for the SP, SSP, and interface processors can be loaded from Flash memory or as part of a bundled system image and are not available on replacement ROMs.

Replacing the ROM

Use the following instructions to replace the microcode ROM on the SP, SSP, or any interface processor. The replacement procedures are the same for each board with the exception of the FSIP, which uses a PLCC-type package for the microcode.

You must use a PLCC extractor to remove the FSIP microcode component. (See Figure 9.) You cannot use a small flat-blade screwdriver to pry it out of the socket as with the older type of ICs. A PLCC IC does not have legs or pins that plug into the socket; instead, the contacts are on the sides of the IC and along the inner sides of the socket. When the IC is seated in the socket, the top of the IC is flush with the top of the socket.

Forcing a small screwdriver or other tool between the IC and the sides of the socket to pry out the IC will damage the component or the socket or both, and you will have to replace them. Figure 10 shows the location of the microcode ROM on each processor module.

Figure 9 Removing a Microcode Component from a PLCC-Type Package**Caution**

Always use a grounding strap to prevent ESD damage. Handle interface processors by the handles and carrier edges only. When handling components, avoid contact with metal traces or pins.

Following are the steps for replacing the microcode on the SP, SSP, and any interface processor.

- Step 1** If you are removing the SP or SSP, turn all power supply switches off (O). If you are removing an interface processor, check the state of each interface and note any that are shut down.
- Step 2** Put on a wrist strap or other antistatic device and connect the equipment end to the captive installation screw on an installed interface processor or to another grounding point.

**Note**

To channel ESD voltages to ground, do not disconnect the power cable.

- Step 3** Follow the procedure in “Removing and Replacing the RP, SP, SSP, and Interface Processors” on page 31 to remove the SP, SSP, or interface processor from the router and place it on an antistatic mat or foam pad. If you perform the replacement close enough to the chassis to avoid straining the interface cables attached to the interface processor (if any), leave the cables connected. Otherwise, label the cables before disconnecting them to avoid crossing them later.
- Step 4** Locate the microcode components and show the socket locations of the microcode ROMs on the following interface processors and switch processors:
- AIP: U111,
 - CIP: U37,
 - EIP: U101,
 - FIP: U23,

**Note**

The microcode ROM on the FEIP is located at U37; the FEIP is not shown.

- FSIP: U81,
- HIP: U133,
- MIP: U41,
- SP: U173,
- SSP: U231,
- TRIP: U41,

- Step 5** Note the orientation of the notch on the existing microcode component so that you can install the new component with the same orientation.
- Step 6** Use a chip or PLCC-type extractor to remove the microcode component from the FSIP socket. Use the same type of extractor or a standard chip extractor to remove the ROM from the other interface processor types. Place the removed component on antistatic foam or into an antistatic bag.
- Step 7** Insert the new microcode component in the socket with the notched end in the same orientation as the previous component.
- Step 8** Follow the steps in “Replacing the RP, SP, SSP, or Interface Processors” on page 37 to replace the SP, SSP, or interface processor.
- Step 9** If you insert an interface processor, verify that the Enabled LED remains on. If it does not, immediately use the ejector levers to eject the interface processor and reinsert it in the slot.
- Step 10** Connect any network interface cables that were removed.
- Step 11** If the system power is off, turn it back on.

**Note**

If you power up the system or insert an interface processor online when a ROM is incorrectly inserted, the system may print a message on the console port reporting a checksum error. If this happens, and if the ROM is not the PLCC-type, remove the microcode ROM, straighten the pins with needlenose pliers, then reinsert the ROM and restart the system.

This completes the ROM replacement. Proceed to the following section to check the installation and verify the microcode version.

Figure 10 Microcode ROM Locations

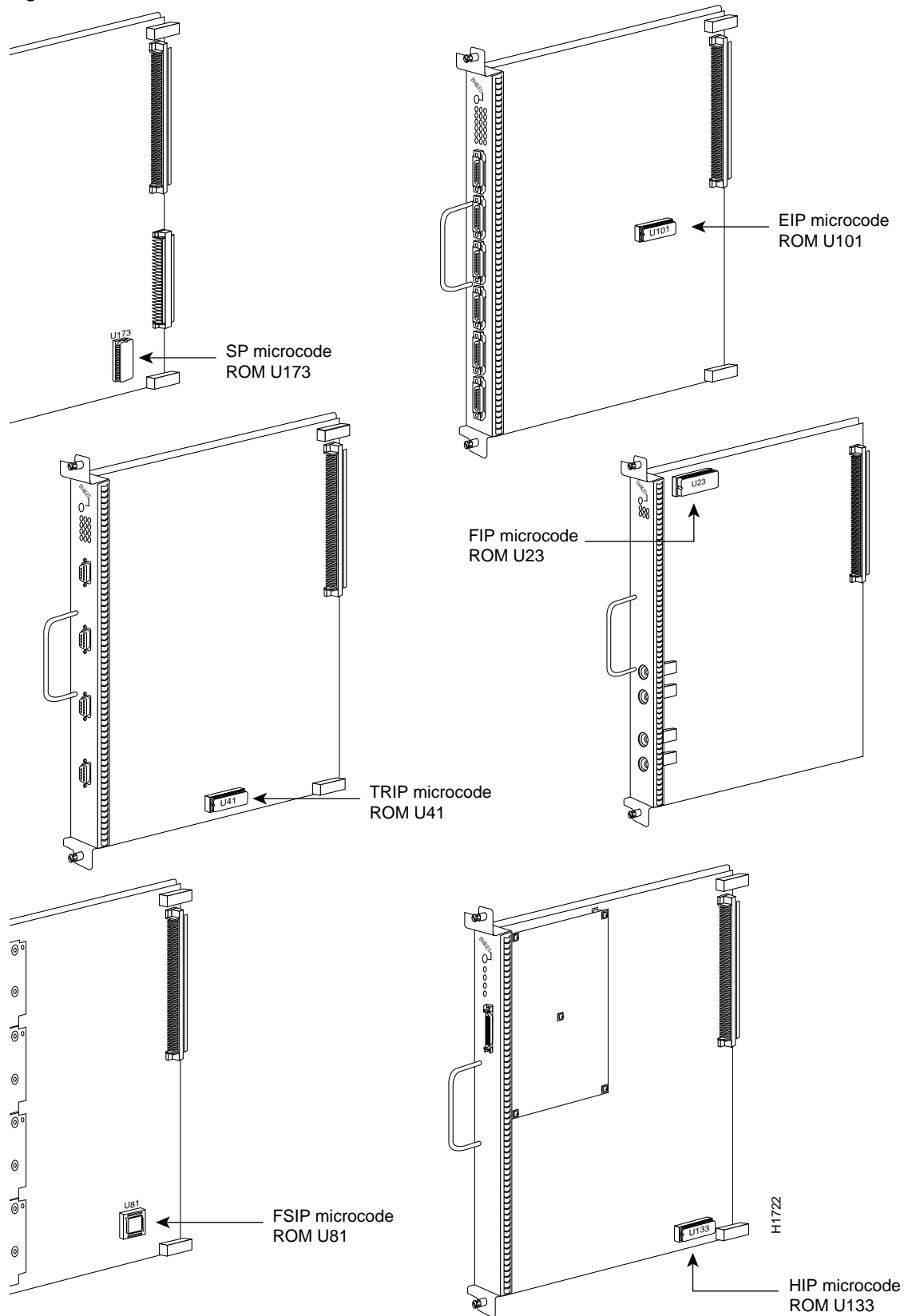
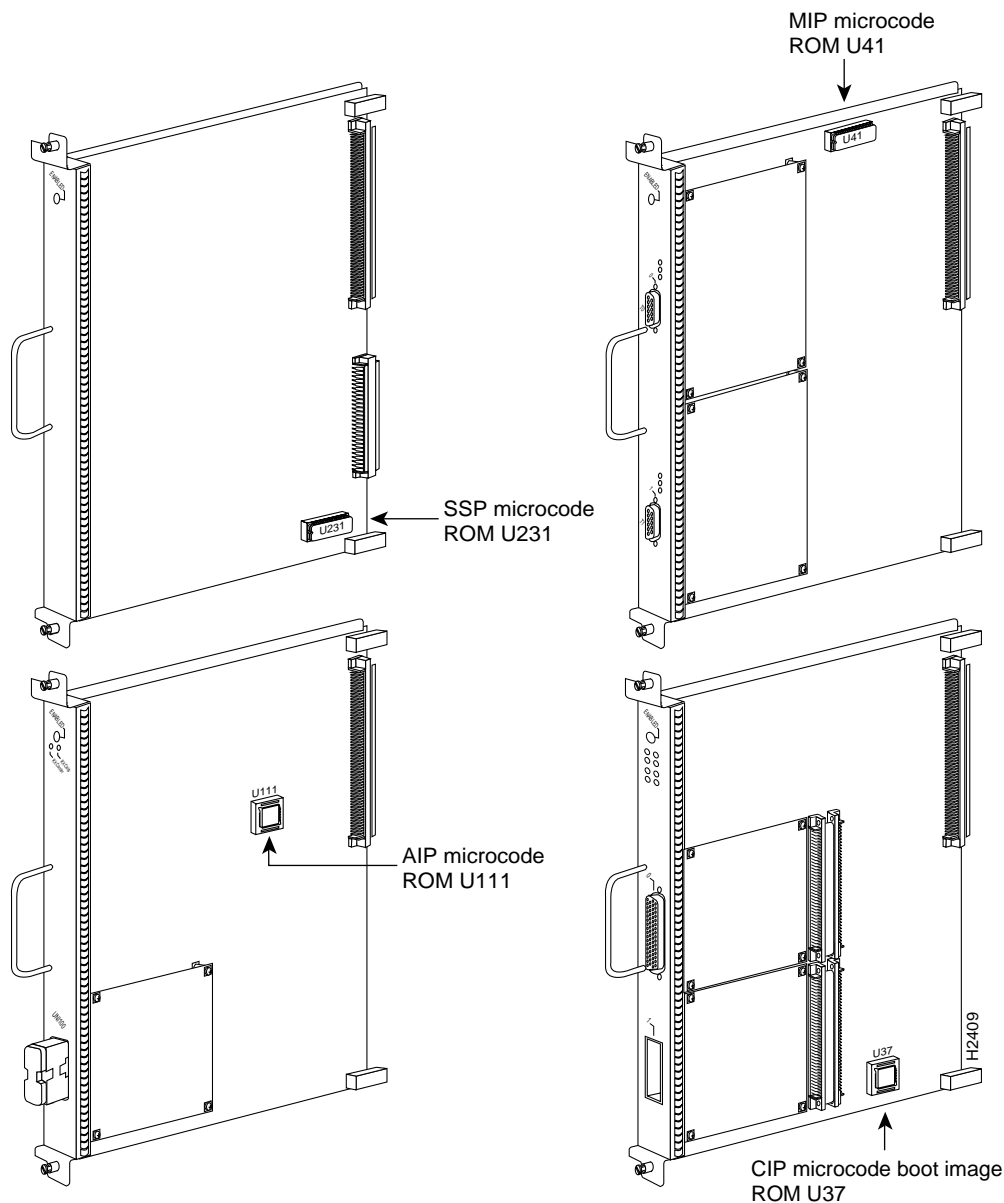


Figure 11 Microcode ROM Locations



Verifying the Microcode Version

OIR allows you to remove and replace interface processors without causing the system to reboot. However, each time you remove or replace an interface processor or SP (or SSP), the system reloads the microcode. If you replace a microcode ROM and the system is already configured to load the microcode for that interface type from ROM, the system automatically loads the new microcode when you reinsert the interface processor in the chassis. However, if the system is using the default image that is bundled with the system image, or if the system is configured to load the microcode for that interface type from a Flash memory file, you will have to modify the boot instructions in the configuration file and instruct the system to load the microcode from ROM for the specific processor module.

The **microcode reload** configuration command reloads only the microcode without rebooting the system. After making any necessary changes to the configuration file, the system automatically issues a **microcode reload**, which reloads all microcode according to the new configuration instructions. The **show controller cbus** command displays the currently loaded and running microcode version on the first line of the display for each card type. The following example shows that the EIP in slot 4 is running EIP Microcode Version 1.0 that loaded from an image bundled with the system code.

```
Router# show cont cbus
EIP 4, hardware version 5.1, microcode version 1.0
  Microcode loaded from flash micro/eipl-1
  Interface 32 - Ethernet4/0, station addr 0000.0c02.d0ec (bia 0000.0c02.d0cc)
```

If the display shows that the microcode is loading from a Flash file from a bundled image instead of from the ROM you just installed, use the **microcode card-type rom** command to modify the configuration file boot instructions. (See “Changing Microcode Boot Instructions” on page 27.) The command instructs all boards of the specified type to load the microcode stored in their onboard ROM. Verify that the new microcode version is loaded with the following steps:

-
- Step 1** Verify that the system boots correctly. If the Enabled LED fails to light on the SP, SSP, or interface processor you just reinstalled, repeat the steps in “Replacing the ROM” on page 46.
 - Ensure that the ROM is installed with the notch at the correct end and that none of the pins are bent.
 - If a pin is bent, remove the ROM, straighten the pin with needlenose pliers, and try the installation again.
 - Step 2** Check the state of the interfaces with the interface processor state LEDs and verify that the interfaces return to the same state they were in before you removed the interface processor (some may have been shut down).
 - Step 3** Enter the **show controller cbus** command to display the interfaces for all interface processor types.
 - Step 4** If the new microcode version is displayed, your installation is complete. If a different (older) version is displayed, the microcode is still loading from a source other than the ROM. Perform the following steps to load the ROM microcode image.
 - Step 5** Enter the configuration command **microcode card-type rom** (refer to the sections “Configuring Microcode” on page 26 and “Verifying the Microcode Version” on page 50.)

The following example instructs the system to load the EIP microcode from ROM, reloads the new microcode, then saves the new configuration in NVRAM:

```
Router> enable
Password: (not displayed)
Router# configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#microcode eip rom
Router(config)#microcode reload
Router(config)#^Z
Router# write memory (copy running-config startup-config)
[ok]
Router#
```

- Step 6** Enter the **show controller cbus** command again. The first line of the display for the interface should show the new microcode version loaded from ROM. If the Enabled LED remains off after a second installation attempt, or if any of the interfaces fail to return to their previous state, contact a service representative; otherwise, the procedure is complete.

If You Need More Information

The Cisco IOS software running the routers contains extensive features and functionality. The effective use of many of many of these features is easier if you have more information at hand. To obtain general information about documentation, call Customer Service at 800 553-6387 or 408 526-7208. You can also send e-mail to cs-rep@cisco.com. You can also refer to the *Cisco Information Packet* that shipped with your router.

For additional information on configuring Cisco 7000 series routers, the following documentation resources are available to you:

- UniverCD

This publication and all other Cisco Systems publications are available on UniverCD, which is Cisco's online library of product information. UniverCD is updated and shipped monthly, so it might be more up to date than printed documentation. To order UniverCD, contact a Cisco Sales or Customer Service representative.

- For systems with Cisco IOS Release 10.0 (1) or later, refer to the following publications:
 - *Router Products Configuration Guide*
 - *Router Products Command Reference*
 - *Troubleshooting Internetworking Systems*
- For systems with Cisco IOS Release 11.1(1) or later, refer to the following modular configuration and modular command reference publications, as appropriate for your configuration:
 - *Configuration Fundamentals Configuration Guide*
 - *Configuration Fundamentals Command Reference*
 - *Wide-Area Networking Configuration Guide*
 - *Wide-Area Networking Command Reference*
 - *Standard Network Protocols Configuration Guide*
 - *Standard Network Protocols Command Reference*
 - *Network Protocols Configuration Guide*
 - *Network Protocols Command Reference*
 - *Bridging and IBM Networking Configuration Guide*
 - *Bridging and IBM Networking Command Reference*
 - *Configuration Builder Getting Started Guide*
 - *Troubleshooting Internetworking Systems*
- For chassis-specific hardware configuration or troubleshooting information, refer to the following publications:
 - *Cisco 7000 Hardware Installation and Maintenance*
 - *Cisco 7010 Hardware Installation and Maintenance*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products Marketplace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “If You Need More Information” section.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)

Copyright © 2000-2001, Cisco Systems, Inc.
All rights reserved.

