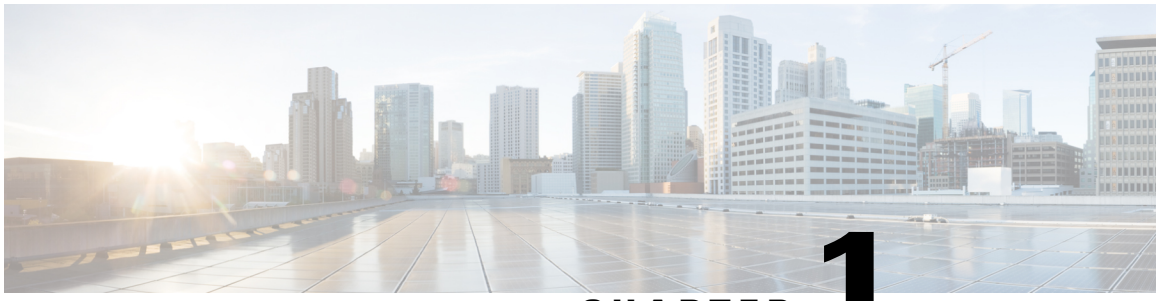
Loading and Managing System Images Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Loading and Managing System Images

Cisco IOS software is packaged in system images. Your router already has an image on it when you receive it. However, you may want to load a different image onto the router at some point. For example, you may want to upgrade your software to the latest release, or use the same version of the software for all the routers in a network. Different system images contain different sets of Cisco IOS features. To determine which version (release number) of Cisco IOS software that is running on your system, and the filename of the system image, use the **showversion** command in user EXEC or privileged EXEC mode. For example, "Version 12.4" indicates Cisco IOS Release 12.4, and "c7200-js-mz" indicates the system image for a Cisco 7200 series router (c7200) containing the "enterprise" feature set (jz).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Loading and Managing System Images

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system. You can create a basic configuration file using the **setup** command (see Using Setup Mode to Configure a Cisco Networking

Device chapter in the *Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.1S* for details).

Restrictions for Loading and Managing System Images

- Many of the Cisco IOS commands described in this document are available and function only in certain configuration modes on the router.
- Some of the Cisco IOS configuration commands are only available on certain router platforms, and the command syntax may vary on different platforms.
- Any software that supports RFC1738 does not allow user name, path, or filename with pattern %xy, where (where x and y are any two hexa values 0-f, 0-F).

Information About Loading and Managing System Images

Types of Images

The following are the two main types of image your router may use:

- System image--The complete Cisco IOS software. This image is loaded when your router boots and is used most of the time.

On most platforms, the image is located in flash memory. On platforms with multiple flash memory file systems (flash, boot flash, slot 0, slot 1, and so on), the image can be located in any existing flash file system. Use the **showfilesystems** privileged EXEC mode command to determine which file systems your router supports. Refer to your hardware documentation for information about where these images are located by default.

- Boot image--A subset of the Cisco IOS software. This image is used to perform network booting or to load Cisco IOS images onto the router. This image is also used if the router cannot find a valid system image. Depending on your platform, this image may be called xboot image, rxboot image, bootstrap image, or boot loader/helper image.

On some platforms, the boot image is contained in ROM. In others, the boot image can be stored in flash memory. On these platforms, you can specify which image should be used as the boot image using the **bootbootldr**global configuration command. Refer to your hardware documentation for information about the boot image used on your router.

Image Naming Conventions

You can identify the platform, features, and image location by the name of the image. The naming convention is *platform-featureset-type*for images.

The *platform* variable indicates which platforms can use this image. Examples of *platform* variables include rsp (Cisco 7000 series with RSP7000 and Cisco 7500 series), c1600 (Cisco 1600 series), and c1005 (Cisco 1005).

The *featureset* variable identifies the feature package that the image contains. Cisco IOS software comes in feature sets tailored to suit certain operating environments, or customized for certain Cisco hardware platforms.

The *type* variable is a code indicating the characteristics of the image:

- f--The image runs from flash memory.
- m--The image runs from RAM.
- r--The image runs from ROM.
- l--The image is relocatable.
- z--The image is zip compressed.
- x--The image is mzip compressed.

General Output Conventions for Copy Operations

During a copy operation, any of the following characters may appear on the screen:

- A pound sign (#) generally means that a flash memory device is being cleared and initialized. (Different platforms use different ways of indicating that Flash is being cleared.)
- An exclamation point (!) means that ten packets have been transferred.
- A series of "V" characters means that a checksum verification of the file is occurring after the file is written to flash memory.
- An "O" means an out-of-order packet.
- A period (.) means a timeout.

The last line in the output indicates whether the copy was successful.

Image Copying from Flash Memory to a Network Server

You may want to copy image files to remote servers as a backup copy, or so that you can perform later checks by comparing the copy in flash to a saved copy.

You can copy system images from flash memory to remote servers using the FTP, the remote copy protocol (rcp), or TFTP. Cisco IOS Software Release 12.4 also supports uploading to (or downloading from) servers using HTTP or HTTPS. The following sections describe these tasks:

The protocol you use depends on which type of server you are using. The FTP and rcp transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because the FTP and rcp transport mechanisms are built on and use the TCP/IP stack, which is connection-oriented.

To stop the copy process, press **Ctrl-**^or**Ctrl-Shift-6**.

In the output, an exclamation point (!) indicates that the copy process is taking place. Each exclamation point (!) indicates that ten packets have been transferred.

Refer to the *Internetwork Troubleshooting Guide* publication for procedures on how to resolve flash memory problems.

Image Copying from Flash Memory Using TFTP

You can copy a system image to a TFTP network server. In some implementations of TFTP, you must first create a "dummy" file on the TFTP server and give it read, write, and execute permissions before copying a file over it. Refer to your TFTP documentation for more information.

Image Copying from Flash Memory to an rcp Server

You can copy a system image from Flash memory to an rcp network server.

If you copy the configuration file to a PC used as a file server, the computer must support remote shell protocol (rsh).

The rcp protocol requires a client to send a remote username on each rcp request to a server. When you copy an image from the router to a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The remote username specified in the **copy** privileged EXEC command, if one if specified.
2. The username set by the **iprcmdremote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** global configuration command, the router software sends the Telnet username as the remote username.
4. The router hostname.

For the rcp copy request to execute, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written or copied relative to the directory associated with the remote username on the server. The path for all files and images to be copied begins at the remote user's home directory. For example, if the system image resides in the home directory of a user on the server, specify that user's name as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the rcp server. For example, suppose the router contains the following configuration lines:

```
hostname Rtr1
ip rcmd remote-username User0
```

If the router's IP address translates to Router1.domain.com, then the .rhosts file for User0 on the rcp server should contain the following line:

```
Router1.domain.com Rtr1
```

Refer to the documentation for your rcp server for more information.

Image Copying from a Network Server to Flash Memory

You can copy system images or boot image from a TFTP, rcp, or FTP server to a flash memory file system to upgrade or change the Cisco IOS software or boot image on your router.

The protocol you use depends on which type of server you are using. The FTP and rcp transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible

because the FTP and rcp transport mechanisms are built on and use the TCP/IP stack, which is connection-oriented.

The following sections describe the copying tasks. The first two tasks and the last task are required. If you have a run-from-flash system, the tasks in the third section are required. Perform one of the remaining tasks, depending on which file transfer protocol you use.

Note When you are upgrading or changing to a different Cisco IOS release, refer to the appropriate release notes for information on system requirements and limitations.

Restrictions on Naming Files

Filenames in flash memory can be up to 63 characters long; they are not case-sensitive and are always converted to lowercase.

Note The destination filename must be an alphanumeric expression (contains all letters or a combination of letters and numerals). For example, "1" is an invalid filename.

The filenamecan be in either lowercase or uppercase; the system ignores case. If more than one file of the same name is copied to flash, regardless of case, the last file copied becomes the valid file.

Flash Memory Space Considerations

Be sure that enough space is available before copying a file to flash memory. Use the **show***flash-filesystem***:** privileged EXEC command, and compare the size of the file you want to copy to the amount of flash memory available. If the space available is less than the amount needed, the **copy** privileged EXEC command will be partially executed, but the entire file will not be copied into flash memory. The failure message "buffer overflow - *xxxx* /*xxxx* " will appear, where *xxxx* /*xxxx* is the number of bytes read from the source file and the number of bytes available on the destination device.

Caution Do not reboot the router if no valid image is in flash memory.

Note For the Cisco 3600 series routers, if you do not have access to a network server and need to download a system image, you can copy an image from a local or remote computer (such as a PC, UNIX workstation, or Macintosh) using the Xmodem or Ymodem protocol. See the section Recovering a System Image Using Xmodem or Ymodemsystem images:recovering:using Xmodem;system images:recovering:using Ymodem later in this chapter.

On Cisco 2500, Cisco 3000, and Cisco 4000 systems, if the file being downloaded to flash memory is an uncompressed system image, the **copy** command automatically determines the size of the file being downloaded and validates it with the space available in flash memory.

On Class B flash file systems, the router gives you the option of erasing the existing contents of flash memory before writing to it. If no free flash memory is available, or if no files have ever been written to flash memory,

the erase routine is required before new files can be copied. If there is enough free flash memory, the router gives you the option of erasing the existing flash memory before writing to it. The system will inform you of these conditions and prompt you for a response.

Note If you enter **n** after the "Erase flash before writing?" prompt, the copy process continues. If you enter **y**and confirm the erasure, the erase routine begins. Be sure to have ample flash memory space before entering **n** at the erasure prompt.

If you attempt to copy a file into flash memory that is already there, a prompt informs you that a file with the same name already exists. This file is deleted when you copy the new file into flash.

- On Class A and B flash file systems, the first copy of the file still resides within flash memory, but it is rendered unusable in favor of the newest version and is listed with the "deleted" tag when you use the **show***flash-filesystem***:** privileged EXEC command. If you terminate the copy process, the newer file is marked "deleted" because the entire file was not copied and is not valid. In this case, the original file in flash memory is valid and available to the system.
- On Class C flash file systems, the first copy of the file is erased.

You can copy normal or compressed images to flash memory. You can produce a compressed system image on any UNIX platform using the **compress** interface configuration command. Refer to your UNIX platform's documentation for the exact usage of the **compress** command.

On some platforms, the flash security jumper must be installed in order to write to flash memory. In addition, some platforms have a write protect switch that must be set to *unprotected* in order to write to flash memory.

Output for Image Downloading Process

The output and dialog varies depending on the platform.

Output for Partitioned Flash Memory

One of the following prompts will be displayed after the command is entered to indicate how a file can be downloaded:

- None--The file cannot be copied.
- RXBOOT-Manual--You must manually reload to the rxboot image in ROM to copy the image.
- RXBOOT-FLH--The copy is done automatically via the flash load helper software in boot ROMs.
- Direct--The copy can be done directly.

If the file can be downloaded into more than one partition, you are prompted for the partition number. To obtain help, enter any of the following characters at the partition number prompt:

- **?** --Displays the directory listings of all partitions.
- **?1** --Displays the directory of the first partition.
- **?2** --Displays the directory of the second partition.
- **q** --Quits the **copy** command.

Flash Memory for Run-from-Flash Systems

You cannot run the system from flash memory and copy to it at the same time. Therefore, for systems that run from flash, preform either of the following tasks before copying to flash:

- Partition flash memory or use flash load helper to allow the system to run from flash memory while you copy to it.
- Reload the system to use a system image from boot ROMs.

See the Understanding Memory Types and Functions section in the Maintaining System Memory chapter of this document for more information on run-from-flash systems.

Refer to the appropriate hardware installation and maintenance publication for information about the jumper settings required for your configuration.

Image Copy from an rcp Server to a Flash Memory File System

You can copy a system image from an rcp network server to a flash memory file system.

If you copy the configuration file to a PC used as a file server, the computer must support rsh.

The rcp Username

The rcp protocol requires a client to send a remote username on each rcp request to a server. When you copy an image from the router to a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following list:

1. The remote username specified in the **copy** privileged EXEC command, if one if specified.
2. The username set by the **iprcmdremote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** global configuration command, the router software sends the Telnet username as the remote username.
4. The router hostname.

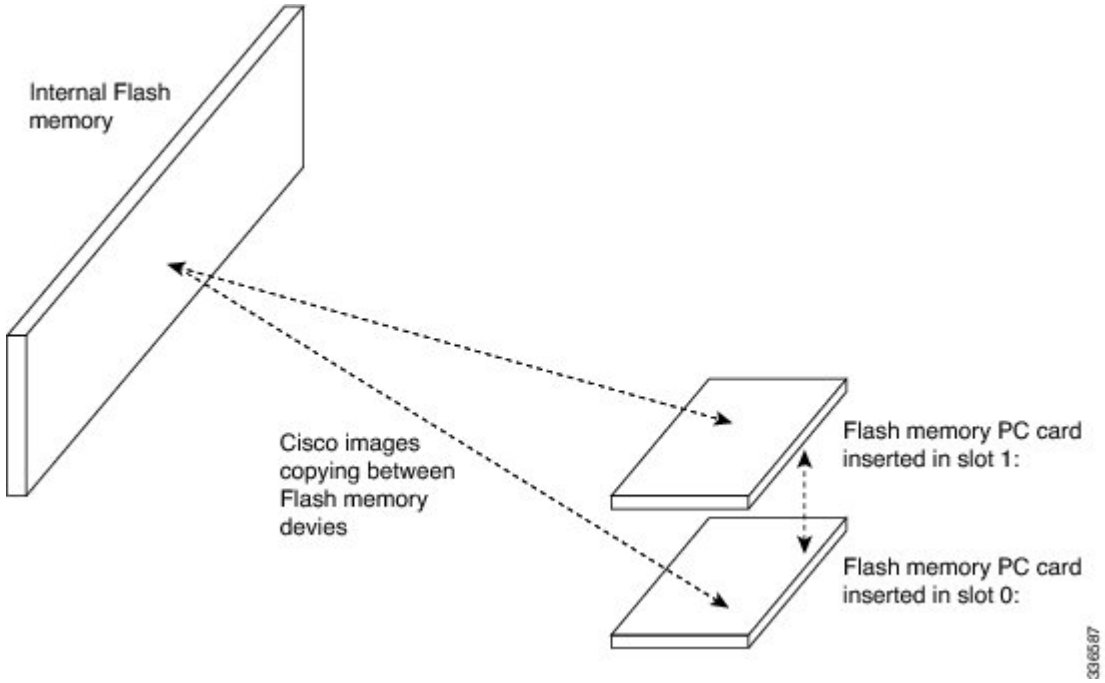
For the rcp copy request to execute, an account must be defined on the network server for the remote username. If the server has a directory structure, the configuration file or image is written or copied relative to the directory associated with the remote username on the server. The path for all files and images to be copied begins at the remote user's home directory. For example, if the system image resides in the home directory of a user on the server, specify that user's name as the remote username.

Image Copying Between Local Flash Memory Devices

On routers with multiple flash memory devices, you can copy images from one flash memory file system, such as internal flash memory or a flash memory card in a PCMCIA slot, to another flash memory device, as

shown in the figure below. One reason to copy the image to a different flash device is to make a backup copy of it.

Figure 1: Copying Images Between Flash Memory File Systems



Caution Before copying to a new flash device, you must first format that device. All new media should be formatted. Memory media used in Cisco devices does not typically come preformatted. Even if preformatted, an initial format using the Cisco files system may help to prevent potential problems with incompatible formatting. Attempts to copy images to unformatted or improperly formatted flash devices may not generate failure messages on some devices. For this reason, the **show** and **verify** steps shown in the following table are strongly recommended. For instructions on formatting your flash device, see the " Maintaining System Memory " chapter.

Image Copying Using HTTP or HTTPS

Cisco IOS Release 12.4 supports file transfers between your Cisco IOS software-based device and a remote HTTP server using the HTTP or Secure HTTP (HTTPS) protocol.

To copy files to or from a remote HTTP server, your system image must support the HTTP Client feature, which is integrated in most Cisco IOS software images. The HTTP client is enabled by default. To determine if the HTTP client is supported on your system, issue the **showiphttpclientall** privileged EXEC mode command. If you are able to execute the command, the HTTP client is supported.

For a complete description of this feature, see the " Transferring Files Using HTTP or HTTPS " module.

Startup System Image in the Configuration File

You can enter multiple boot commands in the startup configuration file or in the BOOT environment variable to provide backup methods for loading a system image onto the router. The following are three ways to load a system image:

- From flash memory--Flash memory allows you to copy new system images without changing ROM. Information stored in flash memory is not vulnerable to network failures that might occur when loading system images from servers.
- From a network server--In case flash memory becomes corrupted, you can specify that a system image be loaded from a network server using Maintenance Operation Protocol (MOP), TFTP, rcp, or FTP as a backup boot method. For some platforms, you can specify a boot image to be loaded from a network server using TFTP, rcp, or FTP.
- From ROM--In case of both flash memory corruption and network failure, specifying a system image to be loaded from ROM provides a final backup boot method. System images stored in ROM may not always be as current as those stored in flash memory or on network servers.

Note Some platforms cannot boot from ROM.

You can enter the different types of boot commands in any order in the startup configuration file or in the BOOT environment variable. If you enter multiple boot commands, the Cisco IOS software tries them in the order they are entered.

Note Booting from ROM is faster than booting from flash memory. However, booting from flash memory is faster and more reliable than booting from a network server.

System Image Loading from a Network Server

You can configure the Cisco IOS software to load a system image from a network server using FTP, TFTP, rcp, or MOP.

If you do not boot from a network server using MOP and you do not specify either FTP, TFTP, or rcp, by default the system image that you specify is booted from a network server via TFTP.

Note If you are using a Sun workstation as a network server and TFTP to transfer the file, configure the workstation to enable verification and generation of User Datagram Protocol (UDP) checksums. See Sun documentation for details.

For increased performance and reliability, use rcp to boot a system image from a network server. The rcp implementation uses TCP, which ensures reliable delivery of data.

You cannot explicitly specify a remote username when you issue the **boot** ROM monitor command. Instead, the hostname of the router is used. If the remote server has a directory structure, as do UNIX systems, and

you boot the router from a network server using rcp, the Cisco IOS software searches for the system image on the server relative to the directory of the remote username.

You can also boot from a compressed image on a network server. One reason to use a compressed image is to ensure that enough memory is available for storage. On routers that do not contain a run-from-ROM image in EPROM, when the router boots software from a network server, the image being booted and the running image both must fit into memory. If the running image is large, there may not be room in memory for the image being booted from the network server.

If not enough room is in memory to boot a regular image from a network server, you can produce a compressed software image on any UNIX platform using the **compress** interface configuration command. Refer to your UNIX platform's documentation for more information on using of the **compress** command.

System Image Recovery Using Xmodem or Ymodem

If you do not have access to a network server and need to download a system image (to update it, or if all the system images in flash memory somehow are damaged or erased), you can copy an image from a local or remote computer (such as a PC, UNIX workstation, or Macintosh) using the Xmodem or Ymodem protocol. This functionality primarily serves as a disaster recovery technique and is illustrated in the figure below.

Note Recovering system images using Xmodem or Ymodem is performed only on the Cisco1600 series and Cisco3600 series routers.

Xmodem and Ymodem are common protocols used for transferring files and are included in applications such as Windows 3.1 (TERMINAL.EXE), Windows 95 (HyperTerminal), Windows NT 3.5x (TERMINAL.EXE), Windows NT 4.0 (HyperTerminal), and Linux UNIX freeware (minicom).

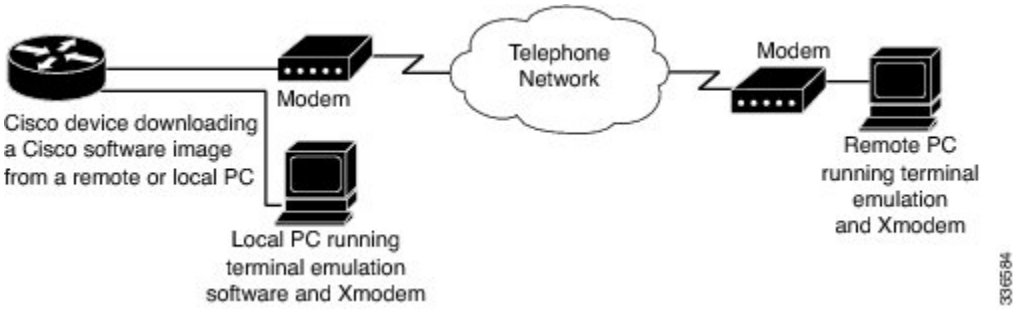
Cisco 3600 series routers do not support XBOOT functionality, a disaster recovery technique for Cisco IOS software, and do not have a separate boot helper (rxboot) image.

Xmodem and Ymodem downloads are slow, so you should use them only when you do not have access to a network server. You can speed up the transfer by setting the transfer port speed to 115200 bps.

On the Cisco 3600 series routers, you can perform the file transfer using Cisco IOS software or, if all local system images are damaged or erased, the ROM monitor. When you use Cisco IOS software for an Xmodem or Ymodem file transfer, the transfer can occur on either the AUX port or the console port. We recommend the AUX port, which supports hardware flow control. File transfers from the ROM monitor must use the console port.

On the Cisco 1600 series routers, you can perform the file transfer only from the ROM monitor over the console port.

Figure 2: Copying a System Image to a Cisco 3600 Series Router with Xmodem or Ymodem



Microcode Images

Microcode is stored on ROM and allows the addition of new machine instructions without requiring that they be designed into electronic circuits when new instructions are needed. Microcode images contain microcode software that runs on various hardware devices. For example, microcode can be updated in Channel Interface Processors (CIPs) on Cisco 7500 series routers, or in Channel Port Adapters (CPAs) on Cisco 7200 series routers.

By default, the system loads the microcode bundled with the Cisco IOS system software image. This microcode is referred to as the default microcode image. However, you can configure the router to use microcode stored in flash.

Cisco 7000 series routers with an RSP7000 and Cisco 7500 series routers each have a writable control store (WCS) that stores microcode. You can load updated microcode onto the WCS from boot flash or from a flash memory card inserted in one of the PCMCIA slots of the Route/Switch Processor (RSP) card.

You can update microcode without having physical access to the router by using the **copy** privileged EXEC command to copy microcode to a flash file system.

Microcode Use on Specific Platforms

The commands for manipulating microcode vary by platform. This section refers you to specialized configuration information found in other Cisco IOS documents.

For information on downloading microcode (Modem Firmware and Portware) into modems on Cisco access servers (like the Cisco AS5800) using the system processing engine (SPE), see the Release 12.4 Cisco IOS Dial Technologies Configuration Guide .

For specific information on loading CIP and CPA microcode into adapters on Cisco 7000, 7200, and 7500 series routers, see the “Configuring Cisco Mainframe Channel Connection Adapters” chapter in the “IBM Networking” part of the Cisco IOS Bridging and IBM Networking Configuration Guide .

How to Work with and Manage System Images

Displaying System Image Information

To display information about the system software, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show bootvar**
3. **show** *flash-filesystem* **:** [**partition***number*] [**all** | **chips** | **detailed** | **err** | **summary**]
4. **show** *flash-filesystem* **:** [**all** | **chips** | **filesys**
5. **show** *flash-filesystem* **:**
6. **show microcode**
7. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show bootvar** **Example:** `Router# show bootvar`	Lists the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, and the contents of the BOOTLDR environment variable.
Step 3	**show** *flash-filesystem* **:** [**partition***number*] [**all** | **chips** | **detailed** | **err** | **summary**] **Example:** `Router# show flash1: detailed`	Lists information about flash memory for Class B file systems.
Step 4	**show** *flash-filesystem* **:** [**all** | **chips** | **filesys** **Example:** `Router# show flash1: filesys`	Lists information about flash memory for Class A file systems.

	Command or Action	Purpose
Step 5	**show** *flash-filesystem* **:** **Example:** `Router# flash1:`	Lists information about flash memory for Class C file systems.
Step 6	**show microcode** **Example:** `Router# show microcode`	Displays microcode information.
Step 7	**show version** **Example:** `Router# show version`	Lists the currently running system image filename, and the system software release version, the configuration register setting, and other information.

Copying an Image from Flash Memory Using TFTP

To copy a system image to a TFTP network server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **copy** *flash-url* **tftp** :[[[//*location*]/*directory*]/*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash:`	(Optional) Displays the system image filename in Flash memory. Use this command to verify the url-path of the file and the exact spelling of the system image filename for use in the next command.
Step 3	**copy** *flash-url* **tftp** :[[[//*location*]/*directory*]/*filename*]	Copies the system image from Flash memory to a TFTP server. Specify the file location and filename as the *flash-url* argument.

	Command or Action	Purpose
	Example: `Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios`	**Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

Examples

The following example uses the **showflash:**EXEC command to learn the name of the system image file and the **copyflash:tftp:**EXEC command to copy the system image to a TFTP server:

```
RouterB# show flash:

System flash directory:
File  Length   Name/status
  1   4137888  c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\
Router# copy flash: tftp:
IP address of remote host [255.255.255.255]? 172.16.13.110
filename to write on tftp host? c3640-c2is-mz.Feb24
writing c3640-c2is-mz.Feb24 !!!!...
successful tftp write.
```

In this example, the file named your-ios is copied from partition 1 of the flash memory PC card in slot 0 to the TFTP server at 172.23.1.129. The file will be saved with the name your-ios in the dirt/sysadmin directory relative to the directory of the remote username.

```
Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios
Verifying checksum for 'your-ios' (file # 1)...  OK
Copy 'your-ios' from Flash to server
  as 'dirt/sysadmin/ios-2'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

The following example uses the **showflash:privileged**EXEC command to learn the name of the system image file and the **copyflash:tftp:** privileged EXEC command to copy the system image (c3640-c2is-mz) to a TFTP server. The router uses the default username and password.

```
Router# show flash:

System flash directory:
File  Length   Name/status
  1   4137888  c3640-c2is-mz
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\
Router# copy flash: tftp:
IP address of remote host [255.255.255.255]? 172.16.13.110
filename to write on tftp host? c3600-c2is-mz
writing c3640-c2is-mz !!!!...
successful ftp write.
```

Copying an Image from Flash Memory to an rcp Server

To copy a system image from flash memory to a rcp server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **configure terminal**
4. **ip rcmd remote-username** *username*
5. **end**
6. **copy** *flash-url* **rcp:** [[[//[*username*@]*location*]/*directory*]/*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash:`	(Optional) Displays the system image filename in flash memory. Use this command to verify the *url-path* of the file and the exact spelling of the system image filename for use in the **copy** privileged EXEC command.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	(Optional) Enters global configuration mode from the terminal. This step is required only if you want to change the default remote username (see Step 3).
Step 4	**ip rcmd remote-username** *username* **Example:** `Router(config)# ep rcmd remote-username user1`	(Optional) Configures the remote username.
Step 5	**end** **Example:** `Router(config)# end`	(Optional) Exits global configuration mode. This step is required only if you want to change the default remote username (see Step 3).
Step 6	**copy** *flash-url* **rcp:** [[[//[*username*@]*location*]/*directory*]/*filename*]	Copies the system image from flash memory to a network server using rcp.

	Command or Action	Purpose
	Example: `Router# copy flash:c5200-ds-l rcp:netadmin1@172.16.1.111/c5200-ds-l`	**Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

Examples

The following example copies the system image named c5200-ds-l to the network server at 172.16.1.111 using rcp and a username of netadmin1:

```
Router# copy flash:c5200-ds-l rcp:netadmin1@172.16.1.111/c5200-ds-l
Verifying checksum for 'c5200-ds-l' (file # 1)...[OK]
Writing c5200-ds-l -
```

The following example copies a system image file named test from the second Personal Computer Memory Card International Association (PCMCIA) slot to a network server using rcp. The remote username is netadmin1. Because the destination address and filename are not specified, the router prompts for this information.

```
Router# configure terminal
Router(config)# ip rcmd remote-username
 netadmin1
Router(config)# end
Router# copy slot1:test rcp:
Address or name of remote host [UNKNOWN]? 172.16.1.111
File name to write to? test
Verifying checksum for 'test' (file # 1)...[OK]
Writing test
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:08 [hh:mm:ss]
```

Copying an Image from a TFTP Server to a Flash Memory File System

To copy a system image from a TFTP server to a flash memory file system, complete the tasks in this section.

Before You Begin

Before you copy a system image or boot image to flash memory, you should make a backup copy of the current software or bootstap image. See the "Copying an Image from Flash Memory Using TFTPTFTP server:images:copying to;images:TFTP server:copying to" section on page 14 for details.

SUMMARY STEPS

1. **enable**
2. **copy tftp:** [[[//*location*]/*directory*]/*filename*]*flash-filesystem*:[*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy tftp:** [[[*//location*]*/directory*]*/filename*]*flash-filesystem***:**[*filename*] **Example:** `Router# copy tftp://theserver/tftpboot/space2/sub2/c7200-js-mz slot1:`	Copies a system image or a boot image to flash memory. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

Examples

In the following example, a file is copied from a TFTP server to slot1:

```
Router# copy tftp://theserver/tftpboot/space2/sub2/c7200-js-mz slot1:
Destination filename [c7200-js-mz]?
Accessing tftp://theserver/tftpboot/space2/sub2/c7200-js-mz...Translating "theserver"...domain
 server (192.168.2.132) [OK]

Loading tftpboot/space2/sub2/c7200-js-mz from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4823492 bytes]

4823492 bytes copied in 264.312 secs (18270 bytes/sec)
```

The following example copies a system image named igs-p-l from a TFTP server to a Class B flash file system when flash memory is too full to copy the file:

```
Router# copy tftp: flash:
IP address or name of remote host [255.255.255.255]? dirt
Translating "DIRT"...domain server (255.255.255.255) [OK]
Name of file to copy? igs-p-l
Copy igs-p-l from 172.16.13.111 into flash memory? [confirm]
Flash is filled to capacity.
Erasure is needed before flash may be written.
Erase flash before writing? [confirm]
Erasing flash EPROMs bank 0
Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee
Erasing flash EPROMs bank 1
Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee
Erasing flash EPROMs bank 2
Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee
Erasing flash EPROMs bank 3
Zeroing bank...zzzzzzzzzzzzzzzz
```

```
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee
Loading from 172.16.1.111:!!!!...
 [OK - 1906676 bytes]
Verifying via checksum...
vvvvvvvvvvvvvvvvvvvvvvvv
Flash verification successful. Length = 1906676, checksum = 0x12AD
```

The following example shows how to copy a system image named igs-p-l into the current flash configuration in which a file named igs-p-l already exists:

```
Router# copy tftp://172.16.13.111/igs-p-l flash:igs-p-l
File igs-p-l already exists; it will be invalidated!
Copy igs-p-l from 172.16.13.111 into flash memory? [confirm]
2287500 bytes available for writing without erasure.
Erase flash before writing? [confirm]n
Loading from 172.16.1.111:!!!!...
[OK - 1906676 bytes]
Verifying via checksum...
vvvvvvvvvvvvvvvvvvvvvvvv
Flash verification successful. Length = 1902192, checksum = 0x12AD
```

In the following example, the flash security jumper is not installed, so you cannot write files to flash memory:

```
Router# copy tftp: flash:
Flash: embedded flash security jumper(12V)
       must be strapped to modify flash memory
```

In the following example, the file named c3600-i-mz on the TFTP server at 172.23.1.129 is copied to the first partition of internal flash Memory:

```
Router# copy tftp://172.23.1.129/c3600-i-mz flash:1:c3600-i-mz/c3600-i-mz
Accessing file 'c3600-i-mz' on 172.23.1.129...
Loading c3600-i-mz from 172.23.1.129 (via Ethernet1/0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'c3600-i-mz' from server
  as 'c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeee ...erased
Loading c3600-i-mz from 172.23.1.129 (via Ethernet1/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1711088 bytes]
Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:17 [hh:mm:ss]
```

Copying from an rcp Server to Flash Memory

To copy an image from an rcp server to flash memory, use the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **copy** *flash-url* **tftp** :[[[*//location*]*/directory*]*/filename*]
4. **configure terminal**
5. **ip rcmd remote-username** *username*
6. **end**
7. **copy rcp:** [[[*//*[*username@*]*location*]*/directory*] */filename*] *flash-filesystem***:**[*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash:`	(Optional) Displays the system image filename in Flash memory. Use this command to verify the url-path of the file and the exact spelling of the system image filename for use in the next command.
Step 3	**copy** *flash-url* **tftp** :[[[*//location*]*/directory*]*/filename*] **Example:** `Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios`	Copies the system image from Flash memory to a TFTP server. Specify the file location and filename as the *flash-url* argument. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.
Step 4	**configure terminal** **Example:** `Router# configure terminal`	(Optional) Enters global configuration mode from the terminal. This step is required only if you override the default remote username (see Step 3).
Step 5	**ip rcmd remote-username** *username* **Example:** `Router(config)# ip rcmd remote-username netuser1`	(Optional) Specifies the remote username.
Step 6	**end** **Example:** `Router(config)# end`	(Optional) Exits global configuration mode. This step is required only if you override the default remote username (see Step 3).
Step 7	**copy rcp:** [[[*//*[*username@*]*location*]*/directory*] */filename*] *flash-filesystem***:**[*filename*] **Example:** `Router#copy rcp flash:`	Copies the image from an rcp server to a Flash memory file system. **Note** After you have issued the **copy** privileged EXEC command, you may be prompted for additional information or for confirmation of the action. The prompting will depend on how much information you provide in the **copy** command and the current setting of the **fileprompt** global configuration command.

Examples

The following example copies a system image named mysysim1 from the netadmin1 directory on the remote server named SERVER1.CISCO.COM with an IP address of 172.16.101.101 to flash memory. To ensure that enough flash memory is available to accommodate the system image to be copied, the Cisco IOS software allows you to first erase the contents of flash memory.

```
Router1# configure terminal
Router1(config)# ip rcmd remote-username
 netadmin1
Router1(config)# end
Router# copy rcp: flash:

System flash directory:
File name/status
   1
mysysim1
[2076072 bytes used, 21080 bytes available]
Address or name of remote host[UNKNOWN]? 172.16.101.101
Name of file to copy? mysysim1
Copy mysysim1 from
SERVER1
.CISCO.COM?[confirm]
Checking for file ‘
mysysim1
’ on SERVER1.CISCO.COM...[OK]
Erase Flash device before writing?[confirm]
Are you sure?[confirm]
Erasing device...ezeeze...erased.
Connected to
172.16.101.101
Loading 2076007 byte file
mysysim1
:!!!!...
[OK]
Verifying checksum... (0x87FD)...[OK]
```

In the following example, the file named c3600-i-mz on the rcp server at the IP address 172.23.1.129 is copied to partition 3 in slot 0. Because no username is specified, the router uses the default rcp remote username.

```
Router# show slot0: partition 3
PCMCIA Slot0 flash directory, partition 3:
File  Length   Name/status
  1   426      running-config
[492 bytes used, 4193812 available, 4194304 total]
Router# copy rcp://172.23.1.129/tftpboot/gate/c3600-i-mz slot0:3:/tftpboot/gate/c3600-i-mz
Accessing file '/tftpboot/gate/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy '/tftpboot/gate/c3600-i-mz' from server
  as '/tftpboot/gate/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:16 [hh:mm:ss]
```

Verifying the Image in Flash Memory

To recompute and verify the image checksum after an image is copied into flash memory or a flash memory device, complete the tasks in this section.

Before You Begin

Before booting from flash memory, use the **verify** privileged EXEC command to verify that the checksum of the image in flash memory matches the checksum listed in the README file that was distributed with the system software image. The checksum of the image in flash memory is displayed at the bottom of the screen when you issue the **copy**privilegedEXEC command to copy an image. The README file was copied to the network server automatically when you installed the system software image on the server.

Caution If the checksum value does not match the value in the README file, do not reboot the router. Instead, issue the **copy** command and compare the checksums again. If the checksum repeatedly is incorrect, copy the original system software image back into flash memory before you reboot the router from flash memory. If you have a corrupted image in flash memory and try to boot from flash, the router will start the system image contained in ROM (assuming that booting from a network server is not configured). If ROM does not contain a fully functional system image, the router will not function and must be reconfigured through a direct console port connection.

The flash memory content listing does not include the checksum of individual files.

SUMMARY STEPS

1. **enable**
2. **verify** *flash-filesystem* **:** [*partition-number***:**] [*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**verify** *flash-filesystem* **:** [*partition-number***:**] [*filename*] **Example:** `Router# verify slot0:c7200-js-mz` **Example:**	Recomputes and verifies the image checksum after the image is copied into flash memory. **Note** If you do not provide the filename in the command, the router prompts you. By default, it prompts for the last (most recent) file in flash. Press Return to recompute the default file checksum, or enter the filename of a different file at the prompt. Note that the checksum for microcode images is always 0x0000.

Examples

The following example verifies the image named c7200-js-mz in slot0:

```
Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

Copying Images Between Local Flash Memory Devices

To copy an image between flash memory devices, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **copy** *source-url destination-url*
4. **verify** *flash-filesystem* **:** *filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash: partition 1`	Displays the layout and contents of flash memory.
Step 3	**copy** *source-url destination-url* **Example:** `Router# copy flash:1:admin/images/new-ios slot0:admin/images/new-ios`	Copies an image between flash memory devices. **Note** The source device and the destination device cannot be the same. For example, the **copyslot1:slot1:**command is invalid.
Step 4	**verify** *flash-filesystem* **:** *filename* **Example:** `Router# verify slot0:`	Verifies the checksum of the image you copied. (You can get the MD5 checksum for your image from Cisco.com).

Examples

The following example copies the file named new-ios from partition 1 of internal flash memory to slot 0:

```
Router# show flash: partition 1
System flash directory, partition 1:
File  Length   Name/status
  1   3142748 admin/images/new-ios
[3142812 bytes used, 1051492 available, 4194304 total]
Router# show slot0:
PCMCIA Slot0 flash directory
File  Length   Name/status
  1   1711088  /tftpboot/gate/c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]
Router# copy flash:1:admin/images/new-ios slot0:admin/images/new-ios
Verifying checksum for 'admin/images/new-ios' (file # 1)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'admin/images/new-ios' from flash: device
  as 'admin/images/new-ios' into slot0: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 [OK - 3142748 bytes]
Flash device copy took 00:00:50 [hh:mm:ss]
Verifying checksum...  OK (0xB732)
Router# show slot0:
PCMCIA Slot0 flash directory
File  Length   Name/status
  1   3142748 admin/images/new-ios
[3142812 bytes used, 1051492 available, 4194304 total]
Router# verify slot0:

Verify filename []? new-ios

! long pause ...
Verifying file integrity of slot0:new-ios.....................!
Embedded Hash   MD5 : E1A04D4DE1ED00407E6E560B315DA505
Computed Hash   MD5 : E1A04D4DE1ED00407E6E560B315DA505
CCO Hash        MD5 : C03EC4564F86F9A24201C88A9DA67317
Signature Verified
Verified slot0:
Router#
```

Loading the System Image from Flash Memory

Flash memory can reduce the effects of network failure by reducing dependency on files that can be accessed only over the network. To configure your router to boot from flash memory, complete the tasks described in these section:

Configuring Flash Memory

To configure the router to load a system image in flash memory, complete the tasks in this section:

SUMMARY STEPS

1. (Optional) Copy a system image or boot image to flash memory using TFTP, rcp, or FTP. See the "Copying an Image from Flash Memory to an FTP ServerTFTP server:images:copying to;images:TFTP server:copying to " section for more information on performing this step.
2. Configure the system to automatically boot from the desired file and location in flash memory or boot flash memory. See the "Configuring the Router to Automatically Boot from an Image in Flash MemoryFlash memory:automatically booting from:configuring " section.
3. (Optional) Depending on the current configuration register setting, change the configuration register value. See the "Configuring the Router to Automatically Boot from an Image in Flash MemoryFlash memory:automatically booting from:configuring " section for more information on modifying the configuration register.
4. (Optional) For some platforms, set the BOOTLDR environment variable to change the location of the boot image.
5. Save your configuration.
6. Power-cycle and reboot your system to ensure that all is working as expected.

DETAILED STEPS

Step 1 (Optional) Copy a system image or boot image to flash memory using TFTP, rcp, or FTP. See the "Copying an Image from Flash Memory to an FTP ServerTFTP server:images:copying to;images:TFTP server:copying to " section for more information on performing this step.

Step 2 Configure the system to automatically boot from the desired file and location in flash memory or boot flash memory. See the "Configuring the Router to Automatically Boot from an Image in Flash MemoryFlash memory:automatically booting from:configuring " section.

Step 3 (Optional) Depending on the current configuration register setting, change the configuration register value. See the "Configuring the Router to Automatically Boot from an Image in Flash MemoryFlash memory:automatically booting from:configuring " section for more information on modifying the configuration register.

Step 4 (Optional) For some platforms, set the BOOTLDR environment variable to change the location of the boot image.

Step 5 Save your configuration.

Step 6 Power-cycle and reboot your system to ensure that all is working as expected.

Configuring the Router to Automatically Boot from an Image in Flash Memory

To configure a router to automatically boot from an image in flash memory, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show** *flash-filesystem* **:**
3. **configure terminal**
4. **boot system flash** [*flash-filesystem***:**] [*partition-number***:**] *filename*
5. **config-register** *value*
6. **end**
7. **copy system:running-config nvram:startup-config**
8. **more nvram:startup-config**
9. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show** *flash-filesystem* **:** **Example:** `Router# show flash: partition 1`	Displays the layout and contents of flash memory.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	(Optional) Enters global configuration mode from the terminal. This step is required only if you want to override the default remote username or password (see Steps 3 and 4).
Step 4	**boot system flash** [*flash-filesystem***:**] [*partition-number***:**] *filename* **Example:** `Router(config)# boot system flash new-image`	Specifies the filename of an image stored in flash memory that should be used for booting.
Step 5	**config-register** *value* **Example:** `Router(config)# config-register 0x010F`	Sets the configuration register to enable loading of the system image specified in the configuration file.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.
Step 7	**copy system:running-config nvram:startup-config** **Example:** `Router# copy system:running-config nvram:startup-config`	Saves the system running configurattion as the device startup configuration (startup-config file).
Step 8	**more nvram:startup-config** **Example:** `Router# more nvram: startup-config`	(Optional) Allows verification of the contents of the startup configuration.
Step 9	**reload** **Example:** `Router# reload`	Reboots the system.

Troubleshooting Tips

For routers that are partitioned, if you do not specify a partition, the router boots from the first partition. If you do not specify a filename, the router boots from the first valid image found in the partition.

If you enter more than one image filename, the router tries the filenames in the order entered.

To remove a filename from the configuration file, enter the **nobootsystemflash** global configuration command and specify the file location.

Note The **nobootsystem** configuration command disablesall **bootsystem** configuration commands regardless of argument. Specifying the **flash** keyword or the*filename*argument with the **nobootsystem** command disables only the commands specified by these arguments.

Examples

The following example shows a router configured to automatically boot from an image in flash memory:

```
Router# configure terminal
Router(config)# boot system flash new-image
Router(config)# config-register 0x010F
Router(config)# end
```

```
Router# copy system:running-config nvram:startup-config
[ok]
Router# reload
[confirm]
%SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.0(7)W5(15) RELEASE SOFTWARE
     Copyright (c) 1986-2001 by Cisco Systems, Inc.
RP1 processor with 16384 Kbytes of memory
F3: 1871404+45476+167028 at 0x1000
Booting new-image from flash memory RRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK - 1916912 bytes]
F3: 1871404+45476+167028 at 0x1000
              Restricted Rights Legend
.
.
.
```

Loading the System Image from a Network Server

To specify the loading of a system image from a network server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **boot system** [**rcp** | **tftp**] *filename* [*ip-address*]
   -
   - **boot system mop** *filename* [*mac-address*] [*interface*]
4. **config-register** *value*
5. **exit**
6. Do one of the following:
   - **copy system:running-config nvram:startup-config**
   -
   - Router#**copyrunstart**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **boot system** [**rcp** | **tftp**] *filename* [*ip-address*] • • **boot system mop** *filename* [*mac-address*] [*interface*] **Example:** `Router(config)#boot system rcp testme5.tester 172.16.0.1`	Specifies the system image file to be booted from a network server using rcp, TFTP, or MOP.
Step 4	**config-register** *value* **Example:** `Router(config)# config-register 0x010F`	Sets the configuration register to enable loading of the image specified in the configuration file.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.
Step 6	Do one of the following: • **copy system:running-config nvram:startup-config** • • Router#**copyrunstart** **Example:** `Router# copy system:running-config nvram:startup-config`	Saves the configuration file to your startup configuration.

Examples

In the following example, a router uses rcp to boot from the testme5.tester system image file on a network server at IP address 172.16.0.1:

```
Router# configure terminal
Router(config)# boot system rcp testme5.tester 172.16.0.1
Router(config)# config-register 0x010F
Router(config)# exit
Router# copy system:running-config nvram:startup-config
```

Changing MOP Request Parameters

To change the Cisco IOS software request parameters for sending boot requests to a MOP server, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mop device-code** {**cisco** | **ds200**} **mopretransmit-timer***seconds* **mopretries***count*
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode from the terminal.
Step 3	**mop device-code** {**cisco** | **ds200**} **mopretransmit-timer***seconds* **mopretries***count* **Example:** `Router (config)#` **mop device-code cisco mop retransmit-timer 10**	Changes MOP server parameters.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 5	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the configuration file to your startup configuration.

Examples

In the following example, if the MOP boot server does not respond within 10 seconds after the router sends a message, the software will resend the message:

```
Router# configure terminal
Router (config)# mop device-code cisco mop retransmit-timer 10
Router (config)# end
Router# copy running-config startup-config
```

Troubleshooting Tips

If you configure your router to boot from a network server using MOP (using the **bootsystemmop** global configuration mode command), the router will send a request for the configuration file to the MOP boot server during startup. By default, when the software sends a request that requires a response from a MOP boot server and the server does not respond, the message will be re-sent after 4 seconds. The message will be re-sent a maximum of eight times. The MOP device code is set to the Cisco device code by default.

If the MOP boot server and router are separated by a slow serial link, it may take longer than 4 seconds for the router to receive a response to its message. Therefore, you may want to configure the software to wait longer than 4 seconds before resending the message if you are using such a link. You may also want to change the maximum number of retries for the MOP request or the MOP device code.

Loading the System Image From ROM

To load the ROM system image as a backup to other boot instructions in the configuration file, complete the tasks in this section.

Note The Cisco 7000 series routers cannot load from ROM.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot system rom**
4. **config-register** *value*
5. **end**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode from the terminal.
Step 3	**boot system rom** **Example:** `Router(config)# boot system rom`	Specifies use of the ROM system image as a backup image.
Step 4	**config-register** *value* **Example:** `Router(config)# config-register 0x010F`	Sets the configuration register to enable loading of the system image specified in the configuration file.
Step 5	**end** **Example:** `Router(config)#` **end**	Exits global configuration mode.
Step 6	**copy system:running-config nvram:startup-config** **Example:** `Router# copy system:running-config nvram:startup-config`	Saves the configuration file to your startup configuration.

Examples

In the following example, a router is configured to boot from ROM:

```
Router# configure terminal
Router(config)# boot system rom
Router(config)# config-register 0x010F
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

Using a Fault-Tolerant Booting Strategy

Occasionally network failures make booting from a network server impossible. To provide the most fault-tolerant booting strategy, you can configure the router to boot first from flash, then from a system file from a network server, and finally from ROM by completing the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot system flash** [*flash-filesystem***:**][*partition-number***:**] *filename*
4. **boot system** [**rcp**| **tftp**]*filename* [*ip-address*]
5. **boot system rom**
6. **config-register** *value*
7. **end**
8. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode from the terminal.
Step 3	**boot system flash** [*flash-filesystem***:**][*partition-number***:**] *filename* **Example:** `Router(config)# boot system flash gsxx`	Configures the router to boot from flash memory.

	Command or Action	Purpose
Step 4	**boot system** [**rcp**| **tftp**]*filename* [*ip-address*] **Example:** `Router(config)# boot system gsxx 172.16.101.101`	Configures the router to boot from a network server.
Step 5	**boot system rom** **Example:** `Router(config)#` **`boot system rom`**	Configures the router to boot from ROM.
Step 6	**config-register** *value* **Example:** `Router(config)#` **`config-register 0x010F`**	Sets the configuration register to enable loading of the system image specified in the configuration file.
Step 7	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 8	**copy system:running-config nvram:startup-config** **Example:** `Router# copy system:running-config nvram:startup-config`	Saves the configuration file to your startup configuration.

Examples

In the following example, a router is configured to first boot aninternal flash image named *gsxx* . Should that image fail, the router will boot the configuration file *gsxx* from a network server. If that method should fail, then the system will boot from ROM.

```
Router# configure terminal
Router(config)# boot system flash gsxx
Router(config)# boot system gsxx 172.16.101.101
Router(config)# boot system rom
Router(config)# config-register 0x010F
Router(config)# end
Router# copy system:running-config nvram:startup-config
[ok]
```

Recovering a System Image Using Xmodem or Ymodem

To copy a Cisco IOS image from a computer or workstation to a router using the Xmodem or Ymodem protocol, complete the tasks in this section.

Note The computer from which you transfer the Cisco IOS image must be running terminal emulation software and the Xmodem or Ymodem protocol.

For the Cisco 1600 series routers, if you include the **-r** option (download to DRAM), your router must have enough DRAM to hold the file being transferred. To run from flash memory, an image must be positioned as the first file in flash memory. If you are copying a new image to boot from flash memory, erase all existing files first.

SUMMARY STEPS

1. **enable**
2. **copy xmodem:** *flash-filesystem* :[*partition* :][*filename*]
3. **xmodem** [**-c**] [**-y**] [**-e**] [**-f**] [**-r**] [**-x**] [**-s***data-rate*] [*filename*]
4. **xmodem** [**-c** | **-y** | **-r** | **-x**] [*filename*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**copy xmodem:** *flash-filesystem* :[*partition* :][*filename*]
	
	Example:
	`or`
	
	Example:
	copy ymodem: *flash-filesystem* :[*partition* :][*filename*]
	
	Example:
	`Router# copy xmodem: flash`
		Copies a system image from a computer to flash memory using Cisco IOS software in EXEC mode (Cisco 3600 series routers only).

	Command or Action	Purpose
Step 3	**xmodem** [**-c**] [**-y**] [**-e**] [**-f**] [**-r**] [**-x**] [**-s***data-rate*] [*filename*] **Example:** `ROMMON> xmodem -c new-ios-image`	Copies a system image from a computer to flash memory in ROM monitor mode for the Cisco 1600 series routers. The **-c** option provides CRC-16 checksumming;**-y** uses the Ymodem protocol; **-e** erases the first partition in flash memory; **-f** erases all of flash memory; **-r** downloads the image to DRAM (the default is flash memory); **-x** prevents the image from executing after download; and **-s** sets the console port data rate.
Step 4	**xmodem** [**-c** | **-y** | **-r** | **-x**] [*filename*] **Example:** `ROMMON> xmodem -c updated-image`	Copies a system image from a computer to flash memory in ROM monitor mode for the Cisco 3600 series routers.

Xmodem Transfer Using the Cisco IOS Software

The Ymodem protocol follows a similar procedure, using the **copyymodem:**privilegedEXEC command--To complete a file transfer using Cisco IOS software and the Xmodem protocol, complete the tasks in this section.

Note This functionality is enabled on Cisco 3600 series routers only.

SUMMARY STEPS

1. Place a Cisco IOS software image on the remote computer's hard drive. You can download an image from Cisco.com.
2. To transfer from a remote computer, connect a modem to the AUX port of your Cisco 3600 series router and to the standard telephone network. The AUX port is set by default to a speed of 9600 bps, 2 stop bits, and no parity. The maximum speed is 115200 bps. Configure the router for both incoming and outgoing calls by entering the **modeminout** line configuration command.
3. At the privileged EXEC prompt in the terminal emulator window of the computer, enter the **copyxmodem:flash:** privileged EXEC command:
4. Press **Enter** to continue.
5. Specify whether to use cyclic redundancy check (CRC) block checksumming, which verifies that your data has been correctly transferred from the computer to the router. If your computer does not support CRC block checksumming, enter **no** at the prompt:
6. Determine how many times the software should try to receive a bad block of data before it declares the copy operation a failure. The default is ten retries. A higher number may be needed for noisy telephone lines. You can configure an unlimited number of retries.
7. Decide whether you want to check that the file is a valid Cisco 3600 series image:
8. Enter the destination filename:
9. If you do not want the contents of internal flash memory erased before the file transfer, enter **no**:
10. Start an Xmodem or Ymodem send operation with the terminal emulation software on the computer that is sending the system image to the router. See your emulation software application's documentation for instructions on how to execute a file transfer. Depending on the application you use, the emulation software may display the progress of the file transfer.

DETAILED STEPS

Step 1 Place a Cisco IOS software image on the remote computer's hard drive. You can download an image from Cisco.com.

Step 2 To transfer from a remote computer, connect a modem to the AUX port of your Cisco 3600 series router and to the standard telephone network. The AUX port is set by default to a speed of 9600 bps, 2 stop bits, and no parity. The maximum speed is 115200 bps. Configure the router for both incoming and outgoing calls by entering the **modeminout** line configuration command.
Connect a modem to the remote computer and to the telephone network. The remote computer dials through the telephone network and connects to the router.

To transfer from a local computer, connect the router's AUX port to a serial port on the computer, using a null-modem cable. The AUX speed configured on the router must match the transfer speed configured on the local computer.

Step 3 At the privileged EXEC prompt in the terminal emulator window of the computer, enter the **copyxmodem:flash:** privileged EXEC command:

Example:

```
Router# copy xmodem: flash:
                          **** WARNING ****
x/ymodem is a slow transfer protocol limited to the current speed
settings of the auxiliary/console ports. The use of the auxiliary
port for this download is strongly recommended.
During the course of the download no exec input/output will be
```

```
available.
                          ---- ******* ----
```

Step 4 Press **Enter** to continue.

Step 5 Specify whether to use cyclic redundancy check (CRC) block checksumming, which verifies that your data has been correctly transferred from the computer to the router. If your computer does not support CRC block checksumming, enter **no** at the prompt:

Example:

```
Proceed? [confirm]
Use crc block checksumming? [confirm] no
```

Step 6 Determine how many times the software should try to receive a bad block of data before it declares the copy operation a failure. The default is ten retries. A higher number may be needed for noisy telephone lines. You can configure an unlimited number of retries.

Example:

```
Max Retry Count [10]: 7
```

Step 7 Decide whether you want to check that the file is a valid Cisco 3600 series image:

Example:

```
Perform image validation checks? [confirm]
Xmodem download using simple checksumming with image validation
Continue? [confirm]
```

After the transfer has begun, and if the image is valid, the software determines whether enough flash memory space exists on the router to accommodate the transfer:

Example:

```
System flash directory:
File  Length   Name/status
  1   1738244  images/c3600-i-mz
[1738308 bytes used, 2455996 available, 4194304 total]
```

Step 8 Enter the destination filename:

Example:

```
Destination file name ? new-ios-image
```

Step 9 If you do not want the contents of internal flash memory erased before the file transfer, enter **no**:

Example:

```
Erase flash device before writing? [confirm] no
Copy '' from server
```

```
  as 'new-ios-image' into Flash WITHOUT erase? [yes/no] yes
Ready to receive file..........
```

Step 10 Start an Xmodem or Ymodem send operation with the terminal emulation software on the computer that is sending the system image to the router. See your emulation software application's documentation for instructions on how to execute a file transfer. Depending on the application you use, the emulation software may display the progress of the file transfer.

Xmodem Transfer Using the ROM Monitor

To complete a file transfer using the ROM monitor and the Xmodem protocol, complete the tasks in this section. To send with the Ymodem protocol, use the **xmodem-y**ROM monitor command.

Before You Begin

For the Cisco 3600 series routers, the router must have enough DRAM to hold the file being transferred, even if you are copying to flash memory. The image is copied to the first file in internal flash memory. Any existing files in flash memory are erased. Copying files to flash partitions or to the second-file position is not supported.

Caution A modem connection from the telephone network to your console port introduces security issues that you should consider before enabling the connection. For example, remote users can dial in to your modem and access the router's configuration settings.

SUMMARY STEPS

1. Place a Cisco IOS software image on the remote computer's hard drive. You can download an image from Cisco.com or from the Feature Pack (Cisco 1600 series routers only).
2. To transfer from a remote computer, connect a modem to the console port of your router and to the standard telephone network. The modem and console port must communicate at the same speed, which can be from 9600 to 115200 bps (Cisco 3600 series routers) or from 1200 to 115200 bps (Cisco 1600 series routers), depending on the speed supported by your modem. Use the **confreg** ROM monitor command to configure the console port transmission speed for the router. For the Cisco 1600 series routers, you can also set the transmission speed with the **-s** option.
3. You should see a ROM monitor prompt in the terminal emulation window:
4. Start an Xmodem send operation, which is initiated from the terminal emulation software on the remote computer that is sending the system image to the router. See your emulation software application's documentation for instructions on how to execute an Xmodem file transfer.
5. The Cisco IOS image is transferred and executed. If you are transferring from a remote computer, the computer maintains control of your console port even after the new Cisco IOS image is running. To release control to a local terminal, reconfigure the speed of the router's console port to match the speed of the local terminal by entering the **speed***bps* line configuration command from the remote computer at the router prompt:

DETAILED STEPS

Step 1 Place a Cisco IOS software image on the remote computer's hard drive. You can download an image from Cisco.com or from the Feature Pack (Cisco 1600 series routers only).

Step 2 To transfer from a remote computer, connect a modem to the console port of your router and to the standard telephone network. The modem and console port must communicate at the same speed, which can be from 9600 to 115200 bps (Cisco 3600 series routers) or from 1200 to 115200 bps (Cisco 1600 series routers), depending on the speed supported by your modem. Use the **confreg** ROM monitor command to configure the console port transmission speed for the router. For the Cisco 1600 series routers, you can also set the transmission speed with the **-s** option.
Connect a modem to the remote computer and to the telephone network. The remote computer dials through the telephone network and connects to the router.

To transfer from a local computer, connect the router's console port to a serial port on the computer, using a null-modem cable. The console port speed configured on the router must match the transfer speed configured on the local computer.

Note If you are transferring from a local computer, you may need to configure the terminal emulation program to ignore Request To Send (RTS)/data terminal ready (DTR) signals.

Step 3 You should see a ROM monitor prompt in the terminal emulation window:

Example:

```
rommon >
```

Enter the **xmodem**ROM monitor command, along with any desired copy options and, optionally, the filename of the Cisco IOS image. The image loads into flash memory by default; to download to DRAM instead, use the **-r** option. The image is normally executed on completion of the file transfer; to prevent execution, use the **-x** option. The **-c** option specifies CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming, if it is supported by the computer:

Example:

```
rommon > xmodem -c new-ios-image
Do not start the sending program yet...
         File size           Checksum   File name
   1738244 bytes (0x1a8604)   0xdd25 george-admin/c3600-i-mz
```

Example:

```
WARNING: All existing data in flash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:  yes
Ready to receive file new-ios-image ...
```

Step 4 Start an Xmodem send operation, which is initiated from the terminal emulation software on the remote computer that is sending the system image to the router. See your emulation software application's documentation for instructions on how to execute an Xmodem file transfer.

Step 5 The Cisco IOS image is transferred and executed. If you are transferring from a remote computer, the computer maintains control of your console port even after the new Cisco IOS image is running. To release control to a local terminal, reconfigure the speed of the router's console port to match the speed of the local terminal by entering the **speed***bps* line configuration command from the remote computer at the router prompt:

Example:

```
Router# configure terminal
Router(config)# line 0
Router(config-line)# speed 9600
```

The remote connection is broken, and you can disconnect the modem from the console port and reconnect the terminal line.

Loading Upgrading and Verifying Microcode Images

To update microcode by loading it into peripheral components, on some Cisco routers, including Cisco 7200, 7500, and 12000 series Internet routers, complete the tasks in these sections:

Specifying the Location of the Microcode Images

To specify the location from where the microcode image should be loaded, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **copy tftp: flash:**
3. **configure terminal**
4. **microcode** *interface* [*flash-filesystem*:*filename* [*slot*] | **system** [*slot*]]
5. **end**
6. **copy system:running-config nvram:startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**copy tftp: flash:** **Example:** `or`	(Optional) Copies microcode files into flash. Perform this step only if you want to load the microcode from flash. See the section “Image Copying from a Network Server to Flash MemoryFlash memory:images:copying to;system images:TFTP server:copying from ” for more information about how to copy images to flash memory.

	Command or Action	Purpose
	Example: **copy tftp:** *file-id* **Example:** `Router# copy tftp: flash`	
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**microcode** *interface* [*flash-filesystem*:*filename* [*slot*] | **system** [*slot*]] **Example:** `Router(config)# microcode fip slot0:fip.v141-7`	Configures the router to load microcode on a target interface from the specified memory location.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 6	**copy system:running-config nvram:startup-config** **Example:** `Router# copy system:running-config nvram:startup-config`	Saves the new configuration information.

Troubleshooting Tips

If an error occurs when you are attempting to download a microcode image, the system loads the default system microcode image.

Microcode images cannot be compressed.

Reloading the Microcode Image

To signal to the system that all microcode configuration commands have been entered and the processor cards should be reloaded, complete the tasks in this section.

Before You Begin

One of the following must occur before a microcode image is reloaded:

- The system is booted.
- A card is inserted or removed.
- The **microcodereload**global configuration command is issued.

After you have entered a microcode configuration command and one of these events has taken place, all cards are reset, loaded with microcode from the appropriate sources, tested, and enabled for operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **microcode reload**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**microcode reload** **Example:** `Router# microcode reload`	Reloads the microcode from the source specified in the configuration on all interface and processor cards.
Step 4	**end** **Example:** `Router# end`	After the reload is complete, enter the **exit** global configuration command to return to the privileged EXEC prompt.

Examples

In the following example, all controllers are reset, the specified microcode is loaded, and the CxBus complex is reinitialized according to the microcode configuration commands that have been written to memory:

```
Router# configure terminal
Router(config)# microcode reload
Router(config)# end
```

Troubleshooting Tips

If flash memory is busy because a card is being removed or inserted, or a**microcodereload** command is executed while flash is locked, the files will not be available and the onboard ROM microcode will be loaded. Issue another **microcodereload** command when flash memory is available, and the proper microcode will be loaded. The **showflash** privileged EXEC command will reveal if another user or process has locked flash memory.

Note The **microcodereload**command should not be used while flash is in use. For example, do not use this command when a **copyftp:** | **rcp:** |**tftp:**} *flash-filesystem*or **show***flash-filesystem***:**privilegedEXEC command is active.

The **microcodereload** command is automatically added to your running configuration when you issue a microcode command that changes the system's default behavior of loading all processors from ROM.

Displaying Microcode Image Information

To display microcode image information, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **show microcode**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show microcode** **Example:** `Router# show microcode`	Displays microcode information.

Loading Microcode Images on the Cisco 12000 Internet Router

To load a microcode image on the Cisco 12000 Internet Router, complete the tasks in this section.

Before You Begin

In addition to the Cisco IOS image that resides on the Internet router, each line card on the Cisco 12000 series has a Cisco IOS image. When the router is reloaded, the specified Cisco IOS image is loaded onto the GRP, and that image is automatically downloaded to all the line cards.

Normally, you want the same Cisco IOS image on the Internet router and all line cards. However, if you want to upgrade a line card with a new version of microcode for testing or to fix a defect, you may need to load a microcode system image that is different from the one on the line card. You may also need to load a new image on the line card to work around a problem that is affecting only one of the line cards.

To load a Cisco IOS image on a line card, first use the **copytftp** privileged EXEC command to download the Cisco IOS image to a slot on one of the PCMCIA flash cards.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **microcode** {**oc12-atm** | **oc12-pos** | **oc3-pos-4**} **flash***file-idslot-number*
4. **microcode reload** *slot-number*
5. **exit**
6. Do one of the following:
   - **execute-on slot** *slot-number* **show version**
   -
   -
   - **attach** *slot-number*

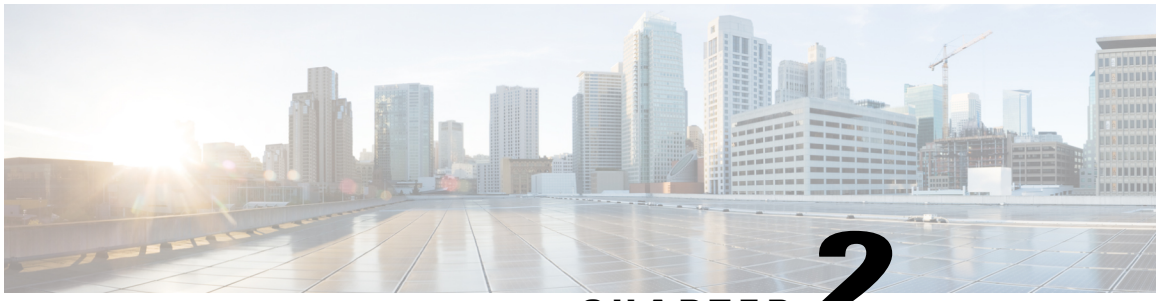
DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**microcode** {**oc12-atm** | **oc12-pos** | **oc3-pos-4**} **flash***file-id*:*slot-number* **Example:** `Router(config)# microcode oc3-POS-4 flash slot0:fip.v141-7 10`	Specifies the type of line card, location of the microcode image, and the slot of the line card to download the image. If the slot number is omitted, the microcode image is downloaded to all line cards.
Step 4	**microcode reload** *slot-number* **Example:** `Router(config)# microcode reload 10`	Reloads the microcode on the specified line card.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits configuration mode.
Step 6	Do one of the following: • **execute-on slot** *slot-number* **show version** • • • **attach** *slot-number* **Example:** `Router# execute-on slot 10 show version`	Connects to the line card and verifies that the new Cisco IOS image is on the line card by checking the version number in the display output.

What to Do Next

For more detailed configuration information, refer to the Cisco 12 http://www.cisco.com/en/US/products/hw/routers/ps167/tsd_products_support_series_home.html 000 series routers documentation.



CHAPTER 2

MD5 File Validation

The MD5 File Validation feature provides a Cisco IOS software command you can use to ensure file validation using the Message Digest 5 (MD5) algorithm in the Cisco IOS File System (IFS).

The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for MD5 File Validation

The MD5 File Validation feature can only be used to check the integrity of a Cisco IOS software image that is stored on a Cisco IOS device. It cannot be used to check the integrity of an image on a remote file system or an image running in memory.

Information About MD5 File Validation

MD5 File Validation Overview

The MD5 File Validation feature provides a mechanism for users to verify that system image files are not corrupted or incomplete. This feature uses the industry-standard MD5 algorithm for improved reliability and security. MD5 file validation computes and displays the MD5 values from the Cisco IOS command-line interface (CLI). Files do not have to be checked on another device.

Note The MD5 file does not have to be on the router in order to verify the Cisco IOS software image.

How to Validate Files Using the MD5 Algorithm

Verifying an Image

The MD5 File Validation feature allows you to generate the MD5 checksum for the Cisco IOS image stored on your router and compare it to the value posted on Cisco.com to verify that the image on your router is not corrupted.

Perform this task to run the MD5 integrity check after transferring an image file.

Image Information

You can obtain the MD5 value for your system image from the Software Center at Cisco.com. The most convenient way to get this value is to click the name of the file prior to download. For example, if you select the 12.2.2T4 Release for the 3640 Platform with the Enterprise Plus Feature Set, before clicking the Download button, you can click the filename for the image (c3640-js-mz.122-2.T4.bin) and the image information will be displayed.

Image information typically includes the Release, Description, File Size, BSD Checksum, Router Checksum, Date Published, and MD5 value for the image. You should record the MD5 value for the image prior to download. However, if you do not have the MD5 value for a previously downloaded image, you can select the same image on Cisco.com (using the same process you would use to download the image) to get the MD5 value.

SUMMARY STEPS

1. **enable**
2. Do one of the following:
   - **verify /md5** *filesystem* **:** *filename*
   -
   - **verify /md5** *filesystem* **:** *filename md5-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	Do one of the following:
	
	• **verify /md5** *filesystem* **:** *filename*
	•
	• **verify /md5** *filesystem* **:** *filename md5-value*
	
	Example:
	
	`Router# verify /md5 disk1:c7200-js-mz`
	
	Example:
	
	Example:
	
	`Router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3`
		Verifies the checksum of a file on a flash memory file system or computes an MD5 signature for a file.
		
		• In the example, disk1 is specified as the filesystem and c7200-js-mz is specified as the filename.
		
		or
		
		Displays a message indicating whether the MD5 values match.
		
		• In the example, the md5-value is specified as 0f369ed9e98756f179d4f29d6e7755d3.

Troubleshooting Tips

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Configuration Examples for MD5 File Validation

Verifying an Image Example

In the following example, the **/md5** keyword is used to display the MD5 value for the image stored in disk1 of the device. The MD5 value shown in the last line can be compared to the value provided on Cisco.com.

```
Router# verify /md5 disk1:

Verify filename []? c7200-js-mz
```

```
.................................
.................................
.................................
.................................
.................................
.............................Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?

  WORD  Expected md5 signature
  <cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3

.................................
.................................
.................................
.................................
.................................
.............................Done!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

Additional References

The following sections provide references related to the MD5 File Validation feature.

Related Documents

Related Topic	Document Title
Additional commands for loading, maintaining, and rebooting system images	*Cisco IOS Configuration Fundamentals Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1321	*MD5 Message-Digest Algorithm*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

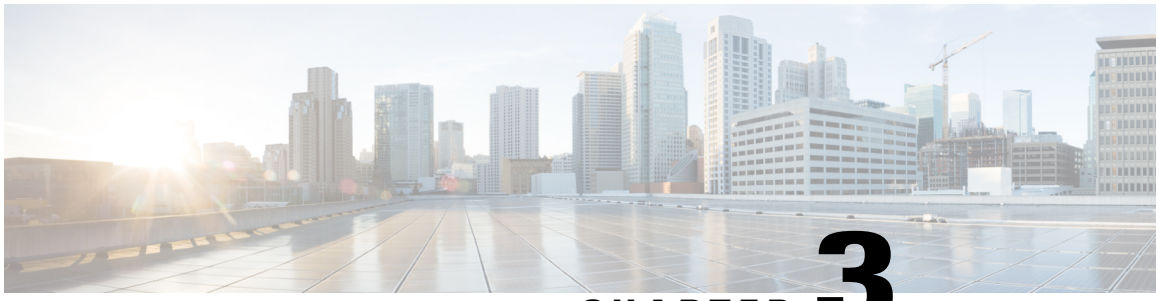
Feature Information for MD5 File Validation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for MD5 File Vaildation

Feature Name	Releases	Feature Information
MD5 File Validation	12.2(4)T 12.0(22)S	The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. The following command was introduced or modified: **verify**.



CHAPTER 3

Warm Upgrade

The Warm Upgrade feature provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades. The Warm Upgrade feature is complementary with the Warm Reload feature introduced in Cisco IOS Release 12.3(2)T.

Feature History for the Warm Upgrade Feature

Release	Modification
12.3(11)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Warm Upgrade

Warm Upgrade Functionality

The Warm Upgrade feature provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades. To perform a warm upgrade, use the **reloadwarmfile***url* command. The Warm Upgrade feature is complementary with the Warm Reload feature introduced in Cisco IOS Release 12.3(2)T.

Prior to the Warm Upgrade feature, a Cisco IOS image transferred control to ROM monitor mode (ROMMON) to perform a Cisco IOS software upgrade or downgrade. ROMMON, along with the help of the boot loader image, carried out the required upgrade or downgrade procedures. While this process is in progress, the networking device is down. With the introduction of the Warm Upgrade feature, packet forwarding is able to continue while the new Cisco IOS image is read and decompressed. The device is down only when the current image is overwritten with the new image, and the new image loads and reconfigures the operating system.

If a warm upgrade operation fails, the current Cisco IOS image should continue to run unless it has been partly or fully overwritten. In this case, ROMMON is allowed to load any image that is configured.

Note For cases where a Cisco IOS image is to be downgraded to an image that does not support the image verification functionality of the **reload** command, a warning message will be displayed before the warm upgrade operation is performed telling the user that the image does not have a digital signature.

How to Reload a Cisco IOS Image Using the Warm Upgrade Functionality

Reloading a Cisco IOS Image Using the Warm Upgrade Functionality

Perform this task to reload a Cisco IOS image using the warm upgrade functionality.

Before You Begin

- The Warm Reload feature introduced in Cisco IOS Release 12.3(2)T must be enabled.
- The ability to upgrade or downgrade a Cisco IOS image using the Warm Upgrade feature assumes that the current Cisco IOS image supports the warm upgrade functionality. However, the new image to which the current image is being upgraded or downgraded does not need to support the warm upgrade functionality.

Note A software upgrade or downgrade using the warm upgrade functionality can only be performed if there is enough free memory in the system to accommodate a decompressed Cisco IOS image.

SUMMARY STEPS

1. **enable**
2. **reload** [**/verify** | **/noverify**] [**warm** [**file***url*]] [**in** [*hh***:**]*mm* | **at***hh***:***mm* [*monthday* | *daymonth*]] [**cancel**] [*text*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** [**/verify** | **/noverify**] [**warm** [**file***url*]] [**in** [*hh***:**]*mm* | **at***hh***:***mm* [*monthday* | *daymonth*]] [**cancel**] [*text*] **Example:** `Router> reload warm file flash:c3745-ipvoice-mz.12.3.11.T.bin`	Reloads the operating system. • Use the **reloadwarmfile***url* command to reload the operating system with a new image whose location and name is specified by the *url* argument. The reload will be performed using the warm upgrade functionality. • You must issue the **warm** keyword if you do not want to override the warm reboot functionality when you reload the router.

Monitoring and Troubleshooting the Warm Upgrade Functionality

Perform this task to monitor and troubleshoot the warm upgrade functionality.

SUMMARY STEPS

1. **show warm-reboot**
2. **debug warm-reboot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show warm-reboot** **Example:** `Router> show warm-reboot`	Displays the statistics for attempted warm reboots.
Step 2	**debug warm-reboot** **Example:** `Router> debug warm-reboot`	Displays warm reboot debug information.

Configuration Examples for the Warm Upgrade Feature

Reloading a Cisco IOS Image Using the Warm Upgrade Functionality Example

The following example shows how to reload the operating system with a new image whose location and name is tftp://9.1.0.1/c7200-p-mz.port. The reload is performed using the warm upgrade functionality.

```
Router> reload warm file tftp://9.1.0.1/c7200-p-mz.port
Proceed with reload? [confirm]
Loading c7200-p-mz.port from 9.1.0.1 (via Ethernet5/0):!!!
[OK - 15323964 bytes]
Decompressing the image :### [OK]
02:37:42:%SYS-5-RELOAD:Reload requested by console. Reload Reason:Reload Command.
             Restricted Rights Legend
.
.
.
Press RETURN to get started!
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/0, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/1, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/2, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/3, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface FastEthernet6/0, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface FastEthernet6/1, changed state to up
00:00:12:%SYS-5-CONFIG_I:Configured from memory by console
00:00:13:%SYS-5-RESTART:System restarted --
00:00:13:%SYS-6-BOOTTIME:Time taken to reboot after reload =   25 seconds
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/0, changed state to up
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/1, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/2, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/3, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet6/0, changed state to
down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet6/1, changed state to
down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Fddi4/0, changed state to down
00:00:14:%LINK-5-CHANGED:Interface Fddi4/0, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/1, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/2, changed state to administratively down
```

```
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/3, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface FastEthernet6/0, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface FastEthernet6/1, changed state to administratively down
```

Additional References

The following sections provide references related to the Warm Upgrade feature.

Related Documents

Related Topic	Document Title
Additional booting commands	Cisco IOS Configuration Fundamentals Command Reference

Standards

Standards	Title
None	--

MIBs

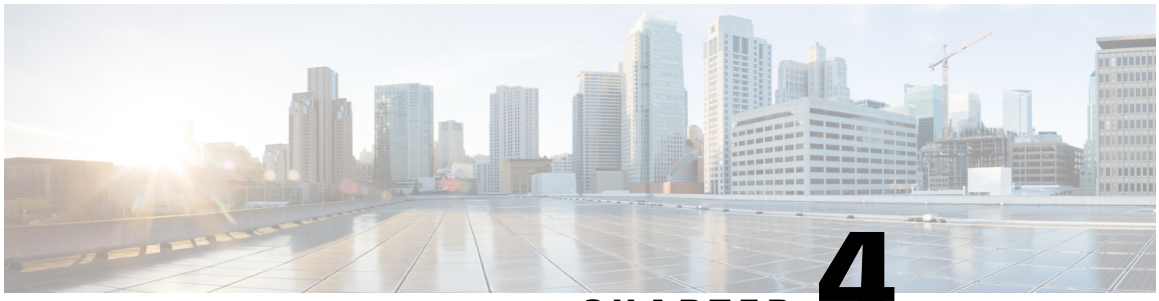
MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml



CHAPTER 4

Rebooting and Reloading - Configuring Image Loading Characteristics

The basic processes completed by a Cisco device (such as a router) when it reboots can be specifically configured to improve function and performance by using the ROM monitor.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Rebooting and Reloading Procedures

- You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.
- You should have at least a minimal configuration running on your system.

Restrictions for Rebooting and Reloading Procedures

- You must have your network up and running, with Cisco IOS Release 12.2 or a later release installed.
- Some of the Cisco IOS configuration commands are only available on certain router platforms, and the command syntax may vary on different platforms.

Information About Rebooting and Reloading Procedures

Determination of Configuration File the Router Uses for Startup

On all platforms except Class A Flash file system platforms:

- If the configuration register is set to ignore NVRAM, the router enters setup mode.
- If the configuration register is not set to ignore NVRAM,
  - The startup software checks for configuration information in NVRAM.
  - If NVRAM holds valid configuration commands, the Cisco IOS software executes the commands automatically at startup.
  - If the software detects a problem with NVRAM or the configuration it contains (a CRC checksum error), it enters **setup** mode and prompts for configuration.

On Class A Flash file system platforms:

- If the configuration register is set to ignore NVRAM, the router enters setup mode.
- If the configuration register is not set to ignore NVRAM,
  - The startup software uses the configuration pointed to by the CONFIG_FILE environment variable.
  - When the CONFIG_FILE environment variable does not exist or is null (such as at first-time startup), the router uses NVRAM as the default startup device.
  - When the router uses NVRAM to start up and the system detects a problem with NVRAM or the configuration it contains, the router enters **setup** mode.

Problems can include a bad checksum for the information in NVRAM or an empty NVRAM with no configuration information.

For more information on environment variables, refer to the “Setting the BOOTLDR Environment Variable ” section.

Determination of Image File the Router Uses for Startup

When a router is powered on or rebooted, the following events happen:

- The ROM monitor initializes.

- The ROM monitor checks the boot field (the lowest four bits) in the configuration register.
  - If the last digit of the boot field is 0 (for example, 0x100), the system does not boot. Instead the system enters ROM monitor mode and waits for user intervention. From ROM monitor mode, you can manually boot the system using the **boot** or **b** command.
  - If the last digit of the boot field is1 (for example, 0x101), the boot helper image is loaded from ROM. (On some platforms, the boot helper image is specified by the BOOTLDR environment variable.)
  - If the last digit of the boot field is 2 through F (for example, 0x102 through 0x10F), the router boots the first valid image specified in the configuration file or specified by the BOOT environment variable.

Note The configuration register boot field value is expressed in hexadecimal. Because the boot field only encompasses the last four bits (represented by the last hexadecimal digit) of the configuration register value, the only digit we are concerned with in this discussion is the last digit. Consequently, 0x1 (0000 0001) is equivalent to 0x101 (1 0000 0001) in discussions of the boot field, because in both cases the last four bits are 0001.

When the boot field is 0x102 through 0x10F, the router goes through each **bootsystem** command in order until it boots a valid image. If bit 13 in the configuration register is set, each command will be tried once (bit 13 is indicated by the position occupied by *b* in the following hexadecimal notation: 0x*b* 000). If bit 13 is not set, the **bootsystem** commands specifying a network server will be tried up to five more times. The timeouts between each consecutive attempt are 2, 4, 16, 256, and 300 seconds.

If the router cannot find a valid image, the following events happen:

- If all boot commands in the system configuration file specify booting from a network server and all commands fail, the system attempts to boot the first valid file in Flash memory.
- If the “boot-default-ROM-software” option in the configuration register is set, the router will start the boot image (the image contained in boot ROM or specified by the BOORLDR environment variable).
- If the “boot-default-ROM-software” option in the configuration register is not set, the system waits for user intervention at the ROM monitor prompt. You must boot the router manually.
- If a fully functional system image is not found, the router will not function and must be reconfigured through a direct console port connection.

Note Refer to your platform documentation for information on the default location of the boot image.

When looking for a bootable file in Flash memory:

- The system searches for the filename in Flash memory. If a filename is not specified, the software searches through the entire Flash directory for a bootable file instead of picking only the first file.
- The system attempts to recognize the file in Flash memory. If the file is recognized, the software decides whether it is bootable by performing the following checks:
  - For run-from-Flash images, the software determines whether it is loaded at the correct execution address.

- For run-from-RAM images, the software determines whether the system has enough RAM to execute the image.

The figure below illustrates the basic booting decision process.

Figure 3: Booting Process

How the Router Uses the Boot Field

The lowest four bits of the 16-bit configuration register (bits 3, 2, 1, and 0) form the boot field. The following boot field values determine if the router loads an operating system and where it obtains the system image:

- When the entire boot field equals 0-0-0-0 (0x0), the router does not load a system image. Instead, it enters ROM monitor or "maintenance" mode from which you can enter ROM monitor commands to manually load a system image. Refer to the "Manually Booting from Flash Memory in ROMMON " section for details on ROM monitor mode.
- When the entire boot field equals 0-0-0-1 (0x1), the router loads the boot helper or rxboot image.
- When the entire boot field equals a value between 0-0-1-0 (0x2) and 1-1-1-1 (0xF), the router loads the system image specified by **bootsystem** commands in the startup configuration file. When the startup configuration file does not contain **bootsystem** commands, the router tries to load a default system image stored on a network server.

When loading a default system image from a network server, the router uses the configuration register settings to determine the default system image filename for booting from a network server. The router forms the default boot filename by starting with the word cisco and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen (-) and the processor type name (cisconn-cpu). See the appropriate hardware installation guide for details on the configuration register and the default filename.

Hardware Versus Software Configuration Register Boot Fields

You modify the boot field from either the hardware configuration register or the software configuration register, depending on the platform.

Most platforms have use a software configuration register. Refer to your hardware documentation for information on the configuration register for your platform.

The hardware configuration register can be changed only on the processor card with dual in-line package (DIP) switches located at the back of the router. For information on modifying the hardware configuration register, refer to the appropriate hardware installation guide.

Environment Variables

Because many platforms can boot images from several locations, these systems use special ROM monitor environment variables to specify the location and filename of images that the router is to use. In addition, Class A Flash file systems can load configuration files from several locations and use an environment variable to specify startup configurations:

BOOT Environment Variable

The BOOT environment variable specifies a list of bootable system images on various file systems.

After you save the BOOT environment variable to your startup configuration, the router checks the variable upon startup to determine the device and filename of the image to boot.

The router tries to boot the first image in the BOOT environment variable list. If the router is unsuccessful at booting that image, it tries to boot the next image specified in the list. The router tries each image in the list

until it successfully boots. If the router cannot boot any image in the BOOT environment variable list, the router attempts to boot the boot image.

If an entry in the BOOT environment variable list does not specify a device, the router assumes the device is **tftp**. If an entry in the BOOT environment variable list specifies an invalid device, the router skips that entry.

BOOTLDR Environment Variable

The BOOTLDR environment specifies the Flash file system and filename containing the boot image that the ROM monitor uses if it cannot find a valid system image. In addition, a boot image is required to boot the router with an image from a network server.

You can change the BOOTLDR environment variable on platforms that use a software boot image rather than boot ROMs. On these platforms, the boot image can be changed without having to replace the boot ROM.

This environment variable allows you to have several boot images. After you save the BOOTLDR environment variable to your startup configuration, the router checks the variable upon startup to determine which boot image to use if the system cannot be loaded.

Note Refer to your platform documentation for information on the default location of the boot image.

CONFIG_FILE Environment Variable

For Class A Flash file systems, the CONFIG_FILE environment variable specifies the file system and filename of the configuration file to use for initialization (startup). Valid file systems can include **nvram:**, **bootflash:**, **slot0:**, and **slot1:**. Refer to the "Managing Configuration Files" chapter for more information on devices. After you save the CONFIG_FILE environment variable to your startup configuration, the router checks the variable upon startup to determine the location and filename of the configuration file to use for initialization.

The router uses the NVRAM configuration during initialization when the CONFIG_FILE environment variable does not exist or when it is null (such as at first-time startup). If the router detects a problem with NVRAM or a checksum error, the router enters **setup** mode.

Controlling Environment Variables

Although the ROM monitor controls environment variables, you can create, modify, or view them with certain commands. To create or modify the BOOT, BOOTLDR, and CONFIG_FILE environment variables, use the **bootsystem**, **bootbootldr**, and **bootconfig** global configuration commands, respectively.

Refer to the "Specify the Startup System Image in the Configuration File" section in the "Loading and Maintaining System Images" book for details on setting the BOOT environment variable. Refer to the "Specify the Startup Configuration File" section in the "Managing Configuration Files" chapter of this document for details on setting the CONFIG_FILE variable.

Note When you use these three global configuration commands, you affect only the running configuration. You must save the environment variable settings to your startup configuration to place the information under ROM monitor control and for the environment variables to function as expected. Use the **copysystem:running-configngvram:startup-config** command to save the environment variables from your running configuration to your startup configuration.

You can view the contents of the BOOT, BOOTLDR, and the CONFIG_FILE environment variables by issuing the **showbootvar** command. This command displays the settings for these variables as they exist in the startup configuration as well as in the running configuration if a running configuration setting differs from a startup configuration setting.

Use the **morenvram:startup-config** command to display the contents of the configuration file pointed to by the CONFIG_FILE environment variable.

Manually Loading a System Image from ROM Monitor

If your router does not find a valid system image, or if its configuration file is corrupted at startup, or the configuration register is set to enter ROM monitor mode, the system enters ROM monitor mode. From this mode, you can manually load a system image from the following locations:

- Internal Flash memory or a Flash memory PC card
- A network server file
- ROM
- A local or remote computer, using the Xmodem or Ymodem protocol (Cisco 1600 series and Cisco 3600 series routers only)

You may only boot from a location if the router can store an image there. Therefore, not all platforms can manually load from these locations.

You can also enter ROM monitor mode by restarting the router and then pressing the **Break** key or issuing a “send break” command from a telnet session during the first 60 seconds of startup.

Note Versions of ROMMON are forward compatible with versions released subsequent to it. ROMMON is not backward compatible with previous releases. It isn't possible to roll-back ROMMON to a previous version.

Aliasing ROM Monitoring Commands

The ROM monitor supports command aliasing modeled on the aliasing function built into the Korn shell. The **alias** command is used to set and view aliased names. This allows the user to alias command names to a letter or word. Aliasing is often used to shorten command names or automatically invoke command options.

Aliases are stored in NVRAM and remain intact across periods of no power. These are some of the set aliases:

- **b** --boot
- **h** --history

- **i** --intialize/reset
- **r** --repeat
- **k** --stack
- **?** --help

The following example shows a pre-aliased menu-type list for ROMMON commands:

```
> ?
$ state      Toggle cache state (? for help)
B [filename] [TFTP Server IP address | TFTP Server Name]
             Load and execute system image from ROM or from TFTP server
C [address]  Continue execution [optional address]
D /S M L V   Deposit value V of size S into location L with modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin execution
H            Help for commands
I            Initialize
K            Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
             Load system image from ROM or from TFTP server, but do not
             begin execution
O            Show configuration register option settings
P            Set the break point
S            Single step next instruction
T function   Test device (? for help)
Deposit and Examine sizes may be B (byte), L (long) or S (short).
Modifiers may be R (register) or S (byte swap).
Register names are: D0-D7, A0-A6, SS, US, SR, and PC
```

If your options appear in the above menu-type format, you can use the listed aliased commands. To initialize the router or access server, enter the **i** command. The **i** command causes the bootstrap program to reinitialize the hardware, clear the contents of memory, and boot the system. To boot the system image file, use the **b** command.

The ROM monitor software characteristics will vary depending on your platform. For further details on ROM monitor mode commands, refer to the appropriate hardware installation guide, or perform a search on Cisco.com.

How to Configure Rebooting and Reloading Procedures

Displaying Boot Information

To display information about system software, system image files, and configuration files, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show bootvar**
3. **more nvram:startup-config**
4. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show bootvar** **Example:** `Router# show bootvar`	Lists the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, and the contents of the BOOTLDR environment variable.
Step 3	**more nvram:startup-config** **Example:** `Router# more nvram:startup-config`	Lists the startup configuration information. On all platforms except the Class A Flash file systems, the startup configuration is usually in NVRAM. On Class A Flash file systems, the CONFIG_FILE environment variable points to the startup configuration, defaulting to NVRAM.
Step 4	**show version** **Example:** `Router# show version`	Lists the system software release version, system image name, configuration register setting, and other information. **Note** You can also use the **o** command (or the **confreg** command for some platforms) in ROM monitor mode to list the configuration register settings on some platforms.

Modifying the Configuration Register Boot Field

To modify the configuration register boot field to determine whether the router loads an operating system image, and if so, where it obtains this system image, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**
4. **config-register** *value*
5. **end**
6. **show version**
7. **copy running-config startup-config**
8. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show version** **Example:** `Router# show version`	Obtains the current configuration register setting. The configuration register is listed as a hexadecimal value.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**config-register** *value* **Example:** `Router(config)# config-register 0x0101`	Modify the current configuration register setting to reflect the way in which you want to load a system image. To do so, change the least significant hexadecimal digit to one of the following: • 0 to load the system image manually using the **boot**command in ROM monitor mode. • 1 to load the system image from boot ROMs. On the Cisco 7200 series and Cisco 7500 series, this setting configures the system to automatically load the system image from bootflash. • 2-F to load the system image from **bootsystem**commands in the startup configuration file or from a default system image stored on a network server. For example, if the current configuration register setting is 0x101 and you want to load a system image from **bootsystem**commands in the startup configuration file, you would change the configuration register setting to 0x102. **Note** In ROM monitor mode, use the **o** command or the **confreg** command on some platforms to list the value of the configuration register boot field.
Step 5	**end** **Example:** `Router(config)# end`	Exits configuration mode.

	Command or Action	Purpose
Step 6	**show version** **Example:** `Router# show version`	(Optional) Verifies that the configuration register setting is correct. Repeat steps 2 through 5 if the setting is not correct.
Step 7	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	Saves the running configuration to the startup configuration.
Step 8	**reload** **Example:** `Router# reload`	(Optional) Reboots the router to make your changes take effect.

Examples

In the following example, the **showversion** command indicates that the current configuration register is set so that the router does not automatically load an operating system image. Instead, it enters ROM monitor mode and waits for user-entered ROM monitor commands. The new setting instructs the router to a load a system image from commands in the startup configuration file or from a default system image stored on a network server.

```
Router1# show version
Cisco IOS (tm) Software
4500 Software (C4500-J-M), Version 11.1(10.4), RELEASE SOFTWARE
Copyright (c) 1986-1997 by Cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by lmiller
Image text-base: 0x600088A0, data-base: 0x60718000
ROM: System Bootstrap, Version 5.1(1), RELEASE SOFTWARE (fc1)
FLASH: 4500-XBOOT Bootstrap Software, Version 10.1(1), RELEASE SOFTWARE (fc1)
Router1 uptime is 6 weeks, 5 days, 2 hours, 22 minutes
System restarted by error - a SegV exception, PC 0x6070F7AC
System image file is "c4500-j-mz.111-current", booted via flash
cisco 4500 (R4K) processor (revision 0x00) with 32768K/4096K bytes of memory.
Processor board ID 01242622
R4600 processor, Implementation 32, Revision 1.0
G.703/E1 software, Version 1.0.
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
Basic Rate ISDN software, Version 1.0.
2 Ethernet/IEEE 802.3 interfaces.
2 Token Ring/IEEE 802.5 interfaces.
4 ISDN Basic Rate interfaces.
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)
Configuration register is 0x2100
Router1# configure terminal
```

```
Router1(config)# config-register 0x210F
Router1(config)# end
Router1# reload
```

Setting the BOOTLDR Environment Variable

To set the BOOTLDR environment variable, complete the tasks in this section:

Examples

The following example sets the BOOTLDR environment to change the location of the boot helper image from internal Flash to slot 0:

```
Router# dir bootflash:
-#- -length- -----date/time------ name
1   620      May 04 1995 26:22:04 rsp-boot-m
2   620      May 24 1995 21:38:14 config2
7993896 bytes available (1496 bytes used)
Router# configure terminal
Router (config)# boot bootldr slot0:rsp-boot-m
Router (config)# end
Router# copy system:running-config nvram:startup-config
[ok]
Router# show bootvar
BOOT variable = slot0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = slot0:router-config

Configuration register is 0x0
```

Scheduling a Reload of the System Image

To schedule a reload of the system image to occur on the router at a later time (for example, late at night or during the weekend when the router is used less) or to synchronize a reload network-wide (for example, to perform a software upgrade on all routers in the network), complete the task in this section.

Note A scheduled reload must take place within approximately 24 days.

SUMMARY STEPS

1. **enable**
2. **reload in** [*hh***:**]*mm* [*text*]
3. **reload at** *hh* **:** *mm* [*month day* | *day month*] [*text*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**reload in** [*hh***:**]*mm* [*text*] **Example:** `Router# reload in 05:00`	Schedules a reload of the software to take effect in *mm* minutes (or *hh* hours and *mm* minutes) from now.
Step 3	**reload at** *hh* **:** *mm* [*month day* | *day month*] [*text*] **Example:** `Router# reload at 02:00 jun 20`	Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. **Note** The **at** keyword can only be used if the system clock has been set on the router (either through NTP, the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, the time on each router must be synchronized with NTP.

Examples

The following example illustrates how to use the **reload** command to reload the software on the router on the current day at 7:30 p.m.:

```
Router# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

The following example illustrates how to use the **reload** command to reload the software on the router at a future time:

```
Router# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

Displaying Information about a Scheduled Reload

To display information about a previously scheduled reload or to determine if a reload has been scheduled on the router, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **show reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show reload** **Example:** `Router# show reload`	Displays reload information, including the time the reload is scheduled to occur, and the reason for the reload if it was specified when the reload was scheduled.

Cancelling a Scheduled Reload

To cancel a previously scheduled reload, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **reload cancel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload cancel** **Example:** `Router# reload cancel`	Cancels a previously scheduled reload of the software.

Examples

The following example illustrates how to use the **reloadcancel**command to stop a scheduled reload:

```
Router# reload cancel
Router#
***
*** --- SHUTDOWN ABORTED ---
***
```

Entering ROM Monitor Mode

During the first 60 seconds of startup, you can force the router to stop booting. The router will enter ROM monitor mode, where you can change the configuration register value or boot the router manually. To stop booting and enter ROM monitor mode, complete the tasks in this section:

SUMMARY STEPS

1. **enable**
2. **reload**
3. Press the Break key during the first 60 seconds while the system is booting.
4. **?**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** **Example:** `Router# reload`	Reboots the router.
Step 3	Press the Break key during the first 60 seconds while the system is booting.	**Note** Enters ROM monitor mode from privileged EXEC mode. This key will not work on the Cisco 7000 unless it has at least Cisco IOS Release 10 boot ROMs.
Step 4	**?** **Example:** `ROMMON> ?`	List the ROM monitor commands.

What to Do Next

If you are planning to use ROM monitor mode on a regular basis, or wish users to load using ROM monitor commands, you can configure the system to default to ROMMON. To automatically boot your system in ROM monitor mode, reset the configuration register to 0x0 by using the **config-register0x0**configuration command. The new configuration register value, 0x0, takes effect after the router or access server is rebooted with the **reload** command. If you set the configuration to 0x0, you will have to manually boot the system from the console each time you reload the router or access server.

To exit ROMMON mode, use the **continue** command. If you have changed the configuration, use the **copyrunning-configstartup-config**command and then issue the **reload** command to save your configuration changes.

Manually Booting from Flash Memory in ROMMON

To manually boot from Flash memory, complete the tasks in Step 1, 2, and 3, and then one of the commands in Step 4:

SUMMARY STEPS

1. **enable**
2. **reload**
3. Press the Break key during the first 60 seconds while the system is booting.
4. Do one of the following:
   - **boot flash** [*filename*]
   -
   - **boot flash** *partition-number* **:** [*filename*]
   -
   - **boot flash flash:** [*partition-number***:**][*filename*]
   -
   - **boot** [*flash-fs***:**][*partition-number***:**][*filename*] (Cisco 1600 series and Cisco 3600 series)
   -
   - **boot** *device* **:** [*filename*] (Cisco 7000 family)

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**reload** **Example:** `Router# reload`	Reboots the router.
Step 3	Press the Break key during the first 60 seconds while the system is booting.	**Note** Enters ROM monitor mode from privileged EXEC mode. This key will not work on the Cisco 7000 unless it has at least Cisco IOS Release 10 boot ROMs.

Step 4	Do one of the following:
	• **boot flash** [*filename*]
	•
	• **boot flash** *partition-number* **:** [*filename*]
	•
	• **boot flash flash:** [*partition-number***:**][*filename*]
	•
	• **boot** [*flash-fs***:**][*partition-number***:**][*filename*] (Cisco 1600 series and Cisco 3600 series)
	•
	• **boot** *device* **:** [*filename*] (Cisco 7000 family)
	Example:
	`ROMMON> boot tftp://172.16.15.112/routertest`
	Example:
	Example:
	`ROMMON> boot flash flash:2:igs-bpx-l`
		Manually boot the router from Flash. Refer to your hardware documentation for the correct form of this command to use.
		• If the filename is not specified, the first bootable file found in the device and partition is used.

Examples

In the following example, a router is manually booted from Flash memory. Because the optional *filename* argument is absent, the first valid file in Flash memory is loaded.

```
> boot flash
F3: 1858656+45204+166896 at 0x1000
Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK -
1903912/13765276 bytes]
F3: 1858676+45204+166896 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
```

In the following example, the **bootflash**command is used with the filename gs7-k--the name of the file that is loaded:

```
> boot flash gs7-k
F3: 1858656+45204+166896 at 0x1000
Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRR [OK - 1903912/13765276 bytes]
F3: 1858676+45204+166896 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
System Bootstrap, Version 4.6(1012) [mlw 99], INTERIM SOFTWARE
Copyright (c) 1986-1992 by cisco Systems
RP1 processor with 16384 Kbytes of memory
```

The following command instructs the ROM monitor to boot the first file in the first partition of internal Flash memory:

```
>
boot flash:
```

This command instructs the ROM monitor to boot the first file in the second partition of the Flash memory card in slot 0:

```
>
boot slot0:2:
```

In this example, the ROM monitor boots the file named image name from the third partition of the Flash memory card in slot 0:

```
>
boot slot0:3:imagename
```

The following command fails to specify a valid device type (**flash:**, **slot0:**, or **slot1:**), so the ROM monitor invokes the boot helper to boot a system image.

```
>
boot flash
```

Manually Booting from a Network File in ROMMON

To manually boot from a network file, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **reload**
3. Press the Break key during the first 60 seconds while the system is booting.
4. **boot** *filename* [*ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** **Example:** `Router# reload`	Reboots the router.

Step 3	Press the Break key during the first 60 seconds while the system is booting.
	
	Example:
	`or`
	
	Example:
	config-register 0x0
	
	Example:
	`Router# <brk>`
		Enters ROM monitor mode from privileged EXEC mode.
		The **config-register0x0** commands instructs the router to boot from ROMMON on the next reload.

Step 4	**boot** *filename* [*ip-address*] **Example:** `ROMMON> boot network1`	Manually boots the router from a network file.

Examples

In the following example, a router is manually booted from the network file *network1*:

```
ROMMON>boot network1
```

Manually Booting from ROM in ROMMON

To manually boot the router from ROM, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **reload**
3. Press the Break key during the first 60 seconds while the system is booting.
4. **boot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** **Example:** `Router# reload`	Reboots the router.
Step 3	Press the Break key during the first 60 seconds while the system is booting. **Example:** `or` **Example:** **config-register 0x0**	Enters ROM monitor mode from privileged EXEC mode. The **config-register0x0** commands instructs the router to boot from ROMMON on the next reload.

	Command or Action	Purpose
	Example: `Router# <brk>`	
Step 4	**boot** **Example:** `ROMMON> boot`	Manually boots the router from ROM. **Note** On the Cisco 7200 series and Cisco 7500 series, the **boot** command loads the first bootable image located in bootflash.

Examples

In the following example, a router is manually booted from ROM:

```
ROMMON> boot
```

Manually Booting Using MOP in ROMMON

You can interactively boot system software using MOP. Typically, you do this to verify that system software has been properly installed on the MOP boot server before configuring the router to automatically boot the system software image. To manually boot the router using MOP, complete the task in this section:

SUMMARY STEPS

1. **enable**
2. **reload**
3. Press the Break key during the first 60 seconds while the system is booting.
4. **boot system mop** *filename* [*mac-address*] [*interface*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**reload** **Example:** `Router# reload`	Reboots the router.

Step 3	Press the Break key during the first 60 seconds while the system is booting.
	
	Example:
	`or`
	
	Example:
	config-register 0x0
	
	Example:
	`Router# <brk>`
		Enters ROM monitor mode from privileged EXEC mode.
		The **config-register0x0** commands instructs the router to boot from ROMMON on the next reload.

Step 4	**boot system mop** *filename* [*mac-address*] [*interface*] **Example:** `ROMMON> boot mop network1`	Manually boots the router using MOP. **Note** The Cisco 7200 series and Cisco 7500 series do not support the **bootmop** command.

Examples

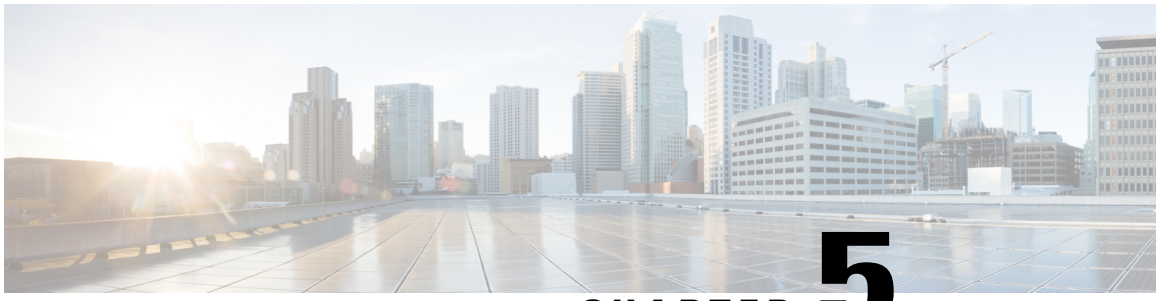
In the following example, a router is manually booted from a MOP server:

```
ROMMON> boot mop network1
```

Exiting from ROMMON

To return to EXEC mode from the ROM monitor, you must continue loading from the default system image. To exit ROMMON mode and resume loading, use the following command in ROM monitor mode:

Command	Purpose
continue `ROMMON > continue`	Resumes loading the startup configuration file and brings the user to EXEC mode.



CHAPTER 5

Warm Reload

The Warm Reload feature allows users to reload their routers without reading images from storage. That is, the Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the image from flash to RAM or self-decompression of the image. Thus, the overall availability of your system improves because the time to reboot your router is significantly reduced.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for Warm Reload.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required..

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To

find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Warm Reload

Additional Memory Consumption

Additional memory is consumed because a copy of the initialized variables must be stored for a warm reboot to function. However, to consume as little memory as possible, a copy of the initialized variables is kept in a compressed form, which is marked as “read-only” to prevent corruption.

Software Support Only

A warm reboot should be used only for forced software crashes. Hardware failure of any kind will result in a cold reboot.

Information About Warm Reload

Benefits of Warm Reload

Quicker Router Reload

By eliminating the need to copy an image from flash to RAM and decompress it, the reload time of a router is reduced by 2 to four minutes. The time savings is greater on platforms that use the BOOTLDR images because tha additional step of loading a BOOTLDR image and parsing the configuration file by the BOOTLDR image can be avoided.

Flash Card Removal

The router is not useless if a flash card is removed because it can still reboot as long as it is not forced into a cold reboot (such as a power failure).

Warm Reload Functionality

When encountering a crash, a Cisco IOS image transfers control to ROMMON, which copies the system image from the storage device (which is typically flash) to main memory, decompresses the system image, and transfers control back to Cisco IOS. Warm rebooting allows the image to return to the start of the text segment in memory and restart execution from that point, thereby, eliminating ROMMON intervention. A copy of the initialized variables is kept in memory and is used to overwrite the existing memory location where the initialized variables are stored. Thus, when the CPU returns to the start of the text segment and begins operating, the information is the same as if execution had begun after the binary had been read from flash and decompressed.

How to Use Warm Reload

Configuring a Warm Reload

Use this task to configure your router for a warm reload in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **warm-reboot** [**count***number*] [**uptime***minutes*
4. **exit**
5. **show warm-reboot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**warm-reboot** [**count***number*] [**uptime***minutes* **Example:** `Router(config)# warm-reboot count 10 uptime 10`	Enables a router to warm-reboot. • **count** *number* --Maximum number of warm reboots allowed between any intervening cold reboot. Valid values range from 1 to 50. The default value is 5 times. • **uptime** *minutes* --Minimum number of minutes that must elapse between initial system configuration and an exception before a warm reboot is attempted. If the system crashes before the specified time elapses, a warm reboot is not attempted. Valid values range from 0 to 120. The default value is 5 minutes. **Note** After a warm reboot is enabled, it will not become active until after the next cold reboot because a warm reboot requires a copy of the initialized memory.
Step 4	**exit**	Exits global configuration mode and return to EXEC mode.

	Command or Action	Purpose
Step 5	**show warm-reboot** **Example:** `Router# show warm-reboot`	(Optional) Displays statistics for attempted warm reboots.

Reloading Your System Without Overriding the Warm-Reload Functionality

If you issue the **reload** command after you have configured the **warm-reboot** global command, a cold reboot will occur. Thus, if you wish to reload your system, but do not want to override the warm-reboot functionality, you should specify the **warm** keyword with the **reload** command. Use this task to configure your router for a warm reboot while you reload your system.

SUMMARY STEPS

1. **enable**
2. **reload** [[**warm**] *text* | [**warm**] **in** [*hh*:*mm* [*text*] | [**warm**] **at***hh*:*mm* [*monthday* | *daymonth*] [*text*] | [**warm**] **cancel**
3. **show reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**reload** [[**warm**] *text* | [**warm**] **in** [*hh*:*mm* [*text*] | [**warm**] **at***hh*:*mm* [*monthday* | *daymonth*] [*text*] | [**warm**] **cancel** **Example:** `Router# reload warm at 10:30`	Reloads the operating system. You must issue the **warm** keyword if you do not want to override the warm reboot functionality when you reload the router.
Step 3	**show reload** **Example:** `Router# show reload`	Displays the reload status on the router.

Configuration Examples for Cisco IOS Warm Reload

Warm Reload Configuration Example

The following example shows how to enable and verify a warm reboot:

```
Router#(config) warm-reboot count 10 uptime 10
Router#(config) exit
!
Router# show warm-reboot
Warm Reboot is enabled
Statistics:
10 warm reboots have taken place since the last cold reboot
XXX KB taken up by warm reboot storage
```

Additional References

The following sections provide references related to the Warm Reload feature.

Related Documents

Related Topic	Document Title
Additional information on rebooting your router	Rebooting and Reloading - Configuring Image Loading Characteristics
Additional booting commands	Cisco IOS Configuration Fundamentals Command Reference

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Glossary

cold reboot --Process of reloading a Cisco IOS image in which the ROMMON copies the configured image from a storage device, such as flash, into main memory. Thereafter, the image is decompressed and execution is started.

warm reboot --Process of reloading a Cisco IOS image without ROMMON intervention in which the image restores read-write data from a previously saved copy in the RAM and starts execution. Unlike a cold reboot, this process does not involve a flash to RAM copy or self-decompression of the image.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.

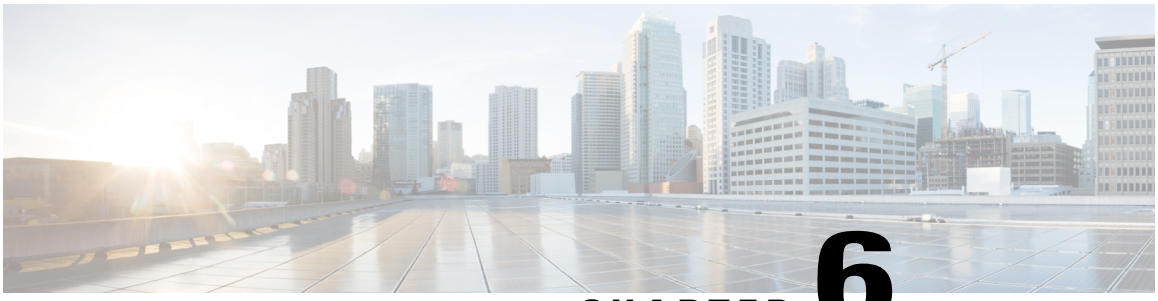
Feature Information for Warm Reload

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 2: Feature Information for Warm Reload

Feature Name	Releases	Feature Information
Warm Reload	12.3(2)T 12.2(18)S 12.2(27)SBC	The Warm Reload feature allows users to reload their routers without reading images from storage. The following sections provide information about this feature: • Information About Warm Reload • How to Use Warm Reload



CHAPTER 6

Configuring the Cisco IOS Auto-Upgrade Manager

The Cisco IOS Auto-Upgrade Manager (AUM) feature simplifies the software image upgrade process by providing a simple interface to specify, download, and upgrade a new Cisco IOS image.

You can upgrade to a new Cisco IOS image in interactive mode by allowing the Auto-Upgrade Manager to guide you through the process. Alternatively, you can perform the upgrade by issuing a single Cisco IOS command or a series of commands. All three methods utilize the Warm Upgrade functionality to perform the upgrade and minimize downtime.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco IOS Auto-Upgrade Manager

- You must configure the DNS server IP address on the router for a download from Cisco. For more details, refer to the “Configuring the DNS Server IP Address: Example” section and the “Related Documents” section.
- You must configure the Secure Socket Layer (SSL) certificate from the Cisco website (www.cisco.com) on the router for a download from Cisco. This configuration is not required for a download from a non-Cisco server. For more details, refer to the “Configuring the SSL Certificate for a Cisco Download” section and the “Related Documents” section.
- You must register with Cisco Systems for cryptographic software downloads if you want to download cryptographic Cisco IOS software images.

Restrictions for Cisco IOS Auto-Upgrade Manager

The Cisco IOS Auto-Upgrade Manager will not run to completion if the router does not have sufficient memory resource to load and store the requested Cisco IOS software image. The Cisco IOS software image can be downloaded from www.cisco.com only if the current Cisco IOS software image running in the router is a cryptographic image.

Information About Cisco IOS Auto-Upgrade Manager

Cisco IOS Auto-Upgrade Manager Overview

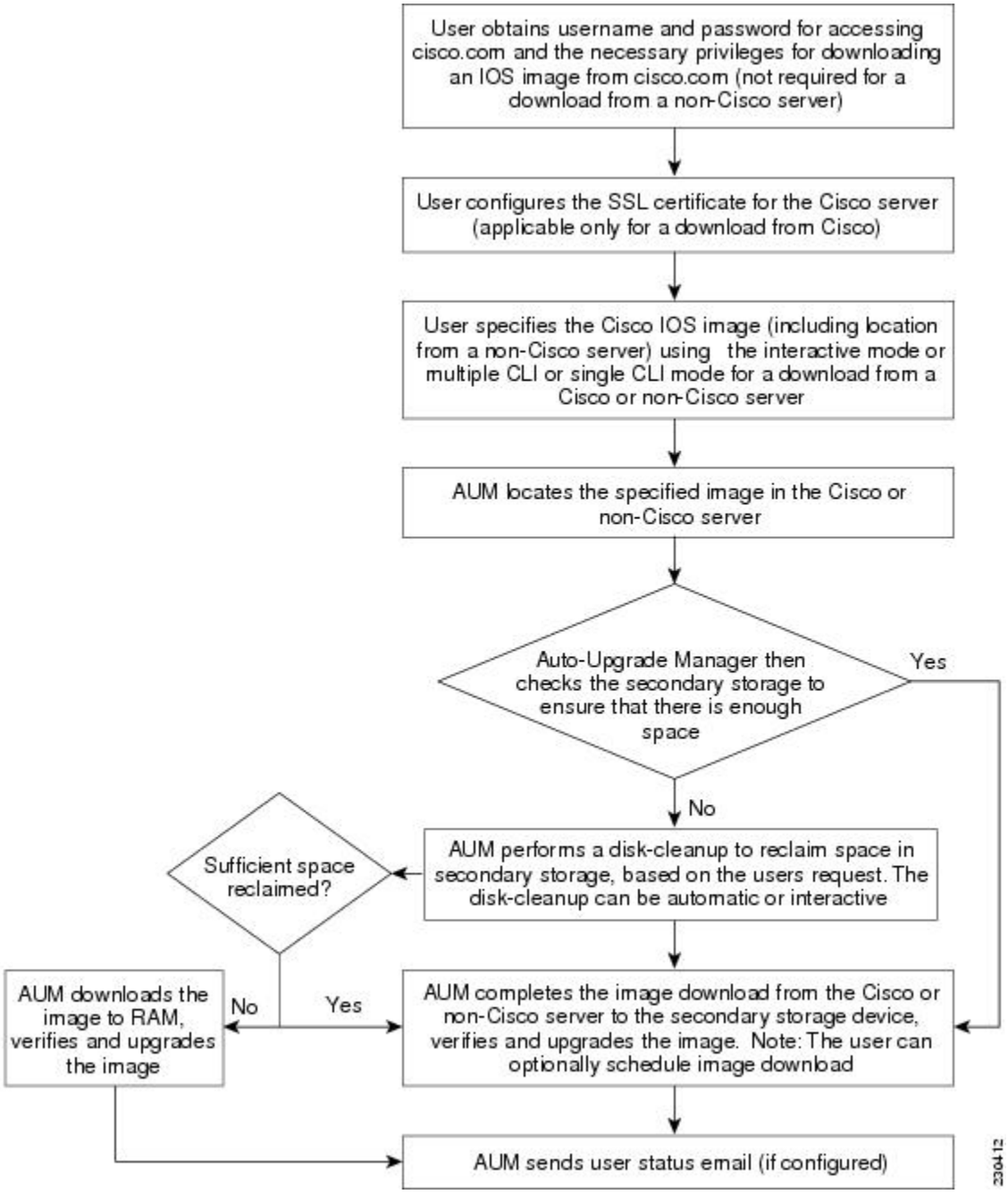
The Cisco IOS Auto-Upgrade Manager streamlines the process of upgrading to a new Cisco IOS software image. You can run the Cisco IOS Auto-Upgrade Manager through the command-line interface (CLI). AUM enables the router to connect to the Cisco website (www.cisco.com) and send the cisco.com username and password for authentication. After authentication, the router passes the name of the Cisco IOS software image that is specified by the user to the Cisco server. The Cisco server returns the complete URL of the Cisco IOS software image to the router.

The Cisco IOS Auto-Upgrade Manager configured on the router can then manage the entire process of upgrading to the Cisco IOS software image. AUM upgrades the router with the software image at the time specified by the user by performing the following tasks:

- Locating and downloading the Cisco IOS software image
- Checking all requirements
- Managing secondary storage space
- Validating the Cisco IOS software image
- Scheduling a warm-upgrade

The figure below illustrates the workflow of the Cisco IOS Auto-Upgrade Manager.

Figure 4: Cisco IOS Auto-Upgrade Manager Workflow



Note If the router fails to load the Cisco IOS software image that you have specified, it displays the error message in the console window and in the syslog buffers indicating the reason for the failure. If the user is not authorized to download encrypted software, an error message is generated requesting the user to register for this service. Similarly, if any CLI configuration statements are not understood by the parser at bootup, it generates an error message and stores the log of the invalid configuration lines in the nvram:invalid-config file. This error message indicates that the Cisco IOS software image that you have specified does not support the same feature set as the old Cisco IOS software image. If the router does not have sufficient secondary storage space to support both the images, but succeeds in the upgrade with the new image, it connects to the Cisco server again and downloads the Cisco IOS software image into a secondary storage. This process erases the existing image.

Specific Cisco IOS Software Image Download from the Cisco Website

You can download a specific Cisco IOS software image from www.cisco.com. AUM uses Secure Socket Layer (SSL) for a secure connection, requiring the user to configure the certificate. The router passes the name of the Cisco IOS software image along with your username and password to log in to the www.cisco.com server. The Cisco server returns the complete URL for the specific Cisco IOS software image to the router.

The Cisco IOS Auto-Upgrade Manager can then automatically download the Cisco IOS software image that you have specified from www.cisco.com, verify it, and upgrade the router with the downloaded image.

Note The Intelligent Download Application (IDA) is the Cisco interface to AUM and is sometimes used interchangeably with the term *Cisco server* in the context of AUM.

Additionally, the Cisco IOS Auto-Upgrade Manager provides the following optional services:

- Disk clean-up utility
- Scheduling of upgrade

These services are available for download from a Cisco or non-Cisco server, both in the interactive and command line modes.

Specific Cisco IOS Software Image Download from a Non-Cisco Server

You can download a Cisco IOS software image that is present on a local or non-Cisco TFTP or FTP server. You can provide an FTP username and password using the **ipftpusername** and **ipftppassword**global configuration commands for an FTP download. The Cisco IOS Auto-Upgrade Manager automates the process of downloading the specific Cisco IOS software image from a non-Cisco server and warm upgrade services. It also provides the disk clean-up utility to delete the files if the space required to download the new Cisco IOS software image is not sufficient.

Interactive and Single Command Line Mode

You can download a specific Cisco IOS software image from www.cisco.com using the CLI or through the following user interfaces:

Interactive Mode

The Auto-Upgrade Manager guides you through the process of upgrading to a new Cisco IOS image in the interactive mode. When you choose automatic upgrade, you are required to answer a few questions in the interactive mode to complete the device upgrade. You can initiate interactive mode by issuing the **upgradeautomatic** command without any options. For more details, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

Single Command Line Mode

The non-interactive single line CLI is for advanced users. You can download and upgrade to a new Cisco IOS software image from a Cisco or non-Cisco server by using the **upgradeautomaticgetversion** command and specifying all the required arguments. For more details, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

The interactive mode and single line CLI mode are applicable to downloads from Cisco and non-Cisco servers.

How to Upgrade a Cisco IOS Software Image Using the Cisco IOS Auto-Upgrade Manager

Configuring the SSL Certificate for a Cisco Download

Perform this task to configure the SSL certificate for a Cisco download.

Before You Begin

The SSL certificate must be configured to download from cisco.com. The certificate is required for secure HTTP communication. You can obtain the SSL certificate from the Cisco website (www.cisco.com) to configure it on the router.

Perform the following task to obtain the SSL certificate from the Cisco website:

1. Pull down the Tools menu in Internet Explorer (IE) and select Internet Options.
2. Under the Advanced tab, select “Warn if changing between secure and not secure mode.”
3. Enter the URL https://www.cisco.com in IE. When a security alert pop-up box appears, click “No” for the question “You are about to leave a secure Internet connection. Do you want to continue?”.
4. Double-click the lock icon on the status bar of IE. This action opens a dialog box showing the details of the certificate.
5. Click the Certification Path tab. This tab displays the certification chain.

6 Select each CA certificate and click View Certificate. This action opens a details window for the certificate.

7 Select the Details tab of the certificate window displayed, and click Copy to File. This action opens the certificate export wizard.

8 Save the certificate in the Base-64 encoded format to a file (such as cisco.cert).

9 Open the cisco.cert file in a Notepad to get the certificate data that you need to configure on your router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal**
5. **revocation-check none**
6. **exit**
7. **crypto ca authenticate** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint cisco_ssl_cert`	Declares the certification authority (CA) and enters ca-trustpoint configuration mode.
Step 4	**enrollment terminal** **Example:** `Device(ca-trustpoint)# enrollment terminal`	Displays the certificate request on the console terminal and allows you to enter the issued certificate data on the terminal.

	Command or Action	Purpose
Step 5	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	Specifies that certificate checking is not required.
Step 6	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	**crypto ca authenticate** *name* **Example:** `Device(config)# crypto ca authenticate cisco_ssl_cert`	Authenticates the CA to your router by obtaining the self-signed certificate of the CA.

Configuring the Cisco IOS Auto-Upgrade Manager

Perform this task to configure the Cisco IOS Auto-Upgrade Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**}
4. **autoupgrade ida url** *url*
5. **autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**} **Example:** `Device(config)# autoupgrade disk-cleanup crashinfo`	Configures the Cisco IOS Auto-Upgrade Manager disk cleanup utility.
Step 4	**autoupgrade ida url** *url* **Example:** `Device(config)# autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl`	Configures the URL of the Cisco server running on www.cisco.com where the image download requests will be sent by Cisco IOS Auto-Upgrade Manager. **Note** This step is required only if the default URL has changed.
Step 5	**autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*} **Example:** `Device(config)# autoupgrade status email smtp-server smtpserver.abc.com`	Configures the email address and outgoing email server to which the router sends the status email.

Downloading the Cisco IOS Software Image

Perform this task to download the Cisco IOS software image from the Cisco website (www.cisco.com) or from a non-Cisco server.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic getversion** {**ciscousername***username***password***password***image***image* | *url*} [**at***hh***:***mm* | **now** | **in***hh***:***mm*] [**disk-management** {**auto** | **confirm** | **no**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**upgrade automatic getversion** {**ciscousername***username***password***password***image***image* | *url*} [**at***hh*:*mm* | **now** | **in***hh*:*mm*] [**disk-management** {**auto** | **confirm** | **no**}] **Example:** `Device# upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin at now disk-management auto`	Downloads the image directly from www.cisco.com or a non-Cisco server.

Reloading the Router with the New Cisco IOS software Image

Perform this task to reload the router with the new Cisco IOS software image.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic runversion** [**at***hh*:*mm* | **now** | **in***hh*:*mm*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**upgrade automatic runversion** [**at***hh*:*mm* | **now** | **in***hh*:*mm*] **Example:** `Device# upgrade automatic runversion at 7:30`	Reloads the router with the new image. **Note** You can also use the **upgradeautomaticgetversion** command to reload the router with the new Cisco IOS software image. But, if you have already downloaded the Cisco IOS software image using the **upgradeautomaticgetversion** command, you must use the **upgradeautomaticrunversion** command to reload the router.

Canceling the Cisco IOS Software Image Reload

Perform this task to cancel a scheduled reload of a specific Cisco IOS software image.

You can cancel an image reload under the following conditions:

- When the scheduled time to reload the router is not sufficient.
- When you do not want to upgrade the router to the new image.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic abortversion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**upgrade automatic abortversion** **Example:** `Device# upgrade automatic abortversion`	Cancels the Cisco IOS software image upgrade.

Configuration Examples for Cisco IOS Auto-Upgrade Manager

Configuring the DNS Server IP Address Example

You should configure the DNS server IP address on the router before configuring the Cisco IOS Auto-Upgrade Manager. This sequence of events enables the router to use the **ping** command with a hostname rather than an IP address. You can successfully ping the Cisco website (www.cisco.com) after configuring the DNS server IP address on the router. This action also ensures that the router is connected to the Internet.

The following example shows how to configure the DNS server IP address on your router. After configuring the DNS server IP address, you should be able to ping www.cisco.com successfully.

```
configure terminal
 ip domain name mycompany.com
 ip name-server 10.2.203.1
```

```
 end
  ping www.cisco.com
```

Configuring the SSL Certificate for a Cisco Download Example

You should configure the SSL certificate of the Cisco server on the router before using the Cisco IOS Auto-Upgrade Manager to download an image from the Cisco website.

The following example shows how to configure the SSL certificate:

```
configure terminal
 crypto pki trustpoint cisco_ssl_cert
  enrollment terminal
  revocation-check none
  exit
 crypto ca authenticate cisco_ssl_cert
!Enter the base 64 encoded CA certificate and end this with a blank line or the word quit
. !The console waits for the user input. Paste the SSL certificate text and press Return.

-----BEGIN CERTIFICATE-----


<The content of the certificate>

-----END CERTIFICATE-----


!Trustpoint 'cisco_ssl_cert' is a subordinate CA and holds a non self signed cert
!Trustpoint 'cisco_ssl_cert' is a subordinate CA.
!but certificate is not a CA certificate.
!Manual verification required
!Certificate has the following attributes:
      ! Fingerprint MD5: 49CE9018 C0CC41BA 1D2FBEA7 AD3011EF
      ! Fingerprint SHA1: A88EAA5D 73D63CB7 BF25197B 9C35ED97 023BB57B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Configuring the Cisco IOS Auto-Upgrade Manager Example

The following example shows how to configure the Cisco IOS Auto-Upgrade Manager on the router:

```
configure terminal
autoupgrade disk-cleanup crashinfo
autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl
autoupgrade status status email smtp-server
```

Additional References

The following sections provide references related to the Cisco IOS Auto-Upgrade Manager.

Related Documents

Related Topic	Document Title
Cisco IOS Auto-Upgrade Manager commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	Cisco IOS Configuration Fundamentals Command Reference
Configuring DNS on Cisco routers	Configuring DNS on Cisco Routers technical note
Warm Upgrade	Warm Upgrade feature module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS Auto-Upgrade Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 3: Feature Information for Cisco IOS Auto-Upgrade Manager

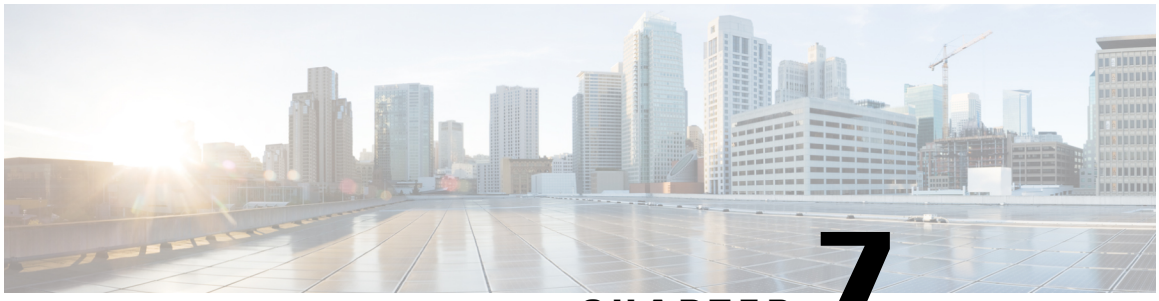
Feature Name	Releases	Feature Information
Cisco IOS Auto-Upgrade Manager	12.4(15)T Cisco IOS XE Release 3.9S	The Cisco IOS Auto-Upgrade Manager simplifies the software image upgrade process by providing a simple interface to specify, download, and upgrade a new Cisco IOS image. In 12.4(15)T, this feature was introduced on the Cisco 1800, Cisco 2800, and Cisco 3800 series routers. This feature was integrated into Cisco IOS XE Release 3.9S. The following commands were introduced or modified by this feature: **autoupgrade disk-cleanup**,**autoupgrade ida url**, **autoupgrade status email**, **debug autoupgrade**, **show autoupgrade configuration unknown**, **upgrade automatic abortversion**, **upgrade automatic getversion**, **upgrade automatic runversion**.

Glossary

CLI --command-line interface

IDA or Cisco server --Intelligent Download Application

Cisco IOS --Cisco Internetworking Operating System



CHAPTER 7

Digitally Signed Cisco Software

The Digitally Signed Cisco Software feature describes how to identify digitally signed Cisco software, gather software authentication information related to digitally signed images, and perform key revocation. Digitally Signed Cisco software is software that is digitally signed using secure asymmetrical (public-key) cryptography.

The purpose of digitally signed Cisco software is to ensure that customers are confident that the software running within their systems is secure and has not been tampered with, and that the software running in those systems originated from the trusted source as claimed.

For customers concerned about software updates involving digitally signed Cisco software--no action is necessary for customers to take advantage of the increased protection. The system operation is largely transparent to existing practices. Some minor changes in system displays reflect the use of digitally signed Cisco software.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Digitally Signed Cisco Software

The Cisco Catalyst 4500 E+Series switches running Cisco IOS XE software include the functionality described in this document, except for Digitally Signed Software Key Revocation and Replacement.

Information About Digitally Signed Cisco Software

Features and Benefits of Digitally Signed Cisco Software

Three main factors drive digitally signed Cisco software and software integrity verification:

- The U.S. government is introducing a new version of the Federal Information Processing Standard (FIPS) 140. FIPS-140-3 is the latest draft and is scheduled for ratification in 2010 and to be effective in 2011. This standard requires software to be digitally signed and to be verified for authenticity and integrity prior to load and execution.
- The focus on product security provides increased protection from attacks and threats to Cisco products. Digitally signed Cisco software offers increased protection from the installation and loading of software that has been corrupted or modified.
- Digitally signed Cisco software provides counterfeit protection, which provides further assurance for customers that the equipment they purchase is as claimed.

Digitally Signed Cisco Software Identification

Digitally signed Cisco IOS software is identified by a three-character extension in the image name. The Cisco software build process creates a Cisco IOS image file that contains a file extension based on the signing key that was used to sign images. These file extensions are:

- .SPA
- .SSA

The significance of each character in the file extension is explained in the table below.

Table 4: Digitally Signed Cisco Software Images File Extension Character Meanings

File Extension Character	Character Meaning
S (first character)	Stands for digitally signed software.
P or S (second character)	P and S stand for a production and special (development) image, respectively. A production image is Cisco software approved for general release; a special image is development software provided under special conditions for limited use.

File Extension Character	Character Meaning
A (third character)	Indicates the key version used to digitally sign the image. A key version is identified by an alphabetical character - for example, A,B,C...

Digitally Signed Cisco Software Key Types and Versions

Digitally signed Cisco software keys are identified by the type and version of the key. A key can be a special, production, or rollover key type. Special and production keys can be revoked. A rollover key is used to revoke a production or special key. The second character in the file extension indicates whether the key type is a special or production key. The key type can be “P” for a production key or an “S” for a special key.

Production and special key types have an associated key version. The key version is defined by the third character in the file extension, in the form of an alphabetical character; for example A, B or C. When a key is replaced, the key version is incremented alphabetically. For example, after a key revocation of a key type “P” (production key) with a key version of “A”, the new image will be signed with key version “B”. Key type and key version are stored as part of the key record in the key storage of the router.

Digitally Signed Cisco Software Key Revocation and Replacement

Note Key revocation and replacement is not supported on Catalyst 4500 E+Series switches running IOS XE software.

Key Revocation

Key revocation is the process of removing a key from operational use in digitally signed Cisco software.

Key revocation takes place when a key becomes compromised or is no longer used. Key revocation and replacement is only necessary in the event of a certain type of vulnerability or catastrophic loss to Cisco's secure key infrastructure. Operational steps to remedy the situation would only be necessary if notified and directed by Cisco. Notification and direction would occur through posting of advisories or field notices on www.cisco.com.

There are two different key revocation processes depending on the type of key to be revoked:

- Production key replacement uses a revocation image and a production image
- Special key replacement uses a production image

Key Replacement

Key replacement is the process of providing a new key to replace a compromised key. The new key is added before the compromised key is revoked. Key replacement is a two-step process:

1 A new key is added to the key storage to replace the revoked key.

2 After the image is verified as operating correctly with the new key, the compromised key is revoked from the key storage.

Key Revocation Image

A revocation image is a basic version of the normal image whose function is to add a new production key to the key storage area. A revocation image has no other capabilities. When a key is to be revoked and replaced, one revocation image per key is provided.

A revocation image contains a new production key bundled within it.

A rollover key stored on the platform is used to verify the signature of the revocation image--a valid revocation image is signed using the same rollover key.

Note A revocation image can be used only in production key revocation.

Important Tasks Concerning the Revocation Image

There are two important tasks concerning the revocation image:

- Adding the new production key to the key storage area.
- Performing a production key upgrade check. For more information, see Step 2 in the "Production Key Revocation".

Adding the New Production Key to the Key Storage Area:

The revocation image adds the bundled production key to the key storage. The key is written to the primary and backup key storage areas after the revocation image checks that the key is already not part of the existing set of keys in the key storage.

Performing a Key Upgrade Check:

After the new key is added and the customer has upgraded the software (Cisco IOS and ROMmon), the show software authenticity upgrade-status command should be run. The user can review the command output to determine if the production key is successfully upgraded, and can be selected for the next boot.

Production Key Revocation

A production key (also called the release key) is revoked and replaced using a revocation image signed with a rollover key, because the images signed using the compromised production key cannot be trusted. The ROMmon can boot any image signed using a rollover key. The production key revocation and replacement process involves four steps:

1 Add the new production key to the key storage. The new production key is bundled within the revocation image.

2 Perform a software upgrade check using the show software authenticity upgrade-status command to verify the following:

- The new production key version is installed.

- The new production key is added to the primary key storage (if not, issue the software authenticity key add production command again with the existing revocation image).
- The new production key is added to the backup key storage (if not, issue the software authenticity key add production command again with the existing revocation image).
- The image is configured for autoboot (with the boot system command) signed with the new production key (if not, make sure the new production image is copied into the box and modify the boot system command to point to the new image).
- The upgradable ROMmon is signed with the new production key (if not, upgrade the ROMmon to the one signed with the new production key).

3. Once everything is verified, the user may load the production image signed with the new production key by using the reload command.
4. Once the new production image is loaded, the user may revoke the compromised key using the software authenticity key revoke production command.

Steps 1 and 2 are done using the special revocation image. It is important for the user to do verifications in Step 2 because after a reboot (in Step 3), an old key will not be revoked if any of the software is still using the old key. The verifications help to ensure that the new key is fully installed and the next reboot (in Step 3) will use the new release software and new ROMmon. Revoking the old production key (Step 4) can be done only after the new key and the new software are installed to the system.

Special Key Revocation

A special key is revoked using a production image signed with a production key. Each production image used for special key revocation has a bundled special key that is the latest at the time of building the production image. The special key revocation and replacement process involves three steps:

1. Add the bundled new special key to the key storage area.
2. Upgrade the ROMmon that is signed using the compromise special key, to the new ROMmon signed with the new special key.
3. Revoke the compromised key from the key storage.

Note that Step 3 does not require any reboot and will be done using the production image itself. This is because the customer is already running a production image and invalidation itself happens from the running production image. Special images do not have the capability to add or invalidate any key.

How to Work with Digitally Signed Cisco Software Images

Identifying Digitally Signed Cisco Software

Perform this task to identify digitally signed Cisco software by examining the image filename in the command output from the show version command, and judging it on the criteria described in the “Digitally Signed Cisco Software Identification” section.

Note If the image file has been renamed by the user, it may not be possible to identify the image because the user may have overwritten the criteria used to indicate that the image is digitally signed.

SUMMARY STEPS

1. **enable**
2. **show version**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show version** **Example:** `Device# show version`	Displays information about the Cisco IOS software version running on a routing device, the ROM Monitor and Bootflash software versions, and the hardware configuration, including the amount of system memory.

Displaying Digitally Signed Cisco Software Signature Information

Perform this task to display information related to software authentication for the current ROMmon and the Cisco IOS image file used for booting. The display includes image credential information, the key type used for verification, signature information, and other attributes in the signature envelope.

SUMMARY STEPS

1. **enable**
2. **show software authenticity running**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show software authenticity running** **Example:** `Device# show software authenticity running`	Displays software authenticity-related information for the current ROMmon and the Cisco IOS image file used for booting.

Displaying Digital Signature Information for a Specific Image File

Perform this task to display the digital signature information related to software authentication for a specific image file.

SUMMARY STEPS

1. **enable**
2. **show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | usbflash0:filename | usbflash1:filename}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | usbflash0:filename | usbflash1:filename}** **Example:** `Device# show software authenticity file usbflash0:c3900-universalk9-mz.SPA`	Displays digital signature and software authenticity-related information for a specific image file.

Displaying Digitally Signed Cisco Software Key Information

Perform this task to display digitally signed Cisco software key information. The information details the software public keys that are in storage with the key types.

SUMMARY STEPS

1. **enable**
2. **show software authenticity keys**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show software authenticity keys** **Example:** `Device# show software authenticity keys`	Displays the software public keys that are in storage with the key types for digitally signed Cisco software.

Performing Production Key Revocation for Digitally Signed Cisco Software

Perform this task to perform production key revocation for digitally signed Cisco software.

Before You Begin

This task must be performed with a dedicated revocation image.

SUMMARY STEPS

1. **enable**
2. **sof tware authenticity key add production**
3. **show sof tware authenticity upgrade-status**
4. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
5. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
6. **upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path]
7. reload [/verify | /noverify] [line | in [hhh:mm | mmm [text]] | at hh:mm [text] | reason [reason string] | cancel]
8. **sof tware authenticity key revoke production**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**sof tware authenticity key add production** **Example:** `Device# software authenticity key add production`	Adds the bundled production key to the key storage of a router with digitally signed Cisco software when run from a revocation image. • An error message will be displayed if this command is used with a special or production image.
Step 3	**show sof tware authenticity upgrade-status** **Example:** `Device# show software authenticity upgrade-status`	Displays software authentication upgrade-status information about the Cisco IOS digitally signed image file and the ROMMON file.
Step 4	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* **Example:** `Device# copy tftp: usbflash0:`	Copies an image from a TFTP server to the selected router storage area. • The new production ROMmon image signed with a new production key is copied to the selected router storage with this command.
Step 5	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* **Example:** `Device# copy /verify tftp: usbflash0:`	Copies an image from a TFTP server to the selected router storage area. • The new production image signed with a new production key is copied to the selected router storage with this command. • It is recommended to use the /verify option in order to verify the signature of the new image during the copy process.
Step 6	**upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path] **Example:** `Device# upgrade rom-monitor file flash0:C3900_ROMMON_RM2.srec.SPB`	Upgrades the ROM monitor (ROMMON) image.

	Command or Action	Purpose
Step 7	reload [/verify | /noverify] [line | in [hhh:mm | mmm [text]] | at hh:mm [text] | reason [reason string] | cancel] **Example:** `Device# reload`	Reloads the software on the router. **Note** The warm upgrade functionality does not support key revocation.
Step 8	**sof tware authenticity key revoke production** **Example:** `Device# software authenticity key revoke production`	Revokes or invalidates the old production key from the key storage when run from a production image. • An error message will be displayed if this command is used with a special image. **Note** This step must be performed after the reload is complete. It is important to be aware of this in the event of a scheduled reload.

Performing Special Key Revocation for Digitally Signed Cisco Software

Perform this task to perform special key revocation for digitally signed Cisco software.

Before You Begin

This task must be performed with a production image.

SUMMARY STEPS

1. **enable**
2. **sof tware authenticity key add special**
3. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
4. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
5. **upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path]
6. **sof tware authenticity key revoke special**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**sof tware authenticity key add special** **Example:** `Device# software authenticity key add production`	Adds a new special key to the key storage area of a router loaded with digitally signed Cisco software. • An error message will be displayed if this command is used with a revocation or special image.
Step 3	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* **Example:** `Device# copy tftp: usbflash0:`	Copies an image from a TFTP server to the selected router storage area. • The new special ROMmon image signed with a new special key is copied to the selected router storage area in this line.
Step 4	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* **Example:** **Example:** **Example:** **Example:** `Device# copy /verify tftp: usbflash0:`	Copies an image from a TFTP server to the selected router storage area. • The new special image signed with a new special key is copied to the selected router storage area in this line. • It is recommended to use the /verify option in order to verify the signature of the new image during the copy process.
Step 5	**upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path] **Example:** `Device# upgrade rom-monitor file flash0:C3900_ROMMON_RM2.srec.SSB`	Upgrades the ROM monitor (ROMmon) image in privileged EXEC mode.
Step 6	**sof tware authenticity key revoke special** **Example:** `Device# software authenticity key revoke special`	Revokes or invalidates the old special key from the key storage when run from a production image. • An error message will be displayed if run from a special or revocation image.

Troubleshooting Digitally Signed Cisco Software Images

Perform this task to troubleshoot digitally signed Cisco software images.

SUMMARY STEPS

1. **enable**
2. **debug software authenticity {envelope | errors | key | revocation | show | verbose}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug software authenticity {envelope | errors | key | revocation | show | verbose}** **Example:** `Device# debug software authenticity errors`	Enables the display of debug messages for digitally signed Cisco software.

Configuration Examples for Digitally Signed Cisco Software

Identifying Digitally Signed Cisco Software Example

The following example displays the digitally signed Cisco software image filename and allows a user to identify it based on the digitally signed Cisco software identification criteria:

```
Device# show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M),
12.4(20090904:044027) [i12 577]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 04-Sep-09 09:22 by xxx
ROM: System Bootstrap, Version 12.4(20090303:092436)
C3900-2 uptime is 8 hours, 41 minutes
System returned to ROM by reload at 08:40:40 UTC Tue May 21 1901!
System image file is "xxx.SPA"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
```

```
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco xxx (revision 1.0) with CISCxxx with 987136K/61440K bytes of memory.
Processor board ID xxx
3 Gigabit Ethernet interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
1 cisco Integrated Service Engine(s)
DRAM configuration is 72 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
1020584K bytes of USB Flash usbflash0 (Read/Write)
1020584K bytes of USB Flash usbflash1 (Read/Write)
500472K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
xx        xxx                   xxxx
Technology Package License Information for Module:'xxx'
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
Configuration register is 0x2102
```

Note the digitally signed image file is identified in the following line:

```
System image file is "xxx.SPA"
```

The image has a three-character extension in the filename (.SPA) characteristic of digitally signed Cisco software. Based on the guidelines in the “Digitally Signed Cisco Software Identification” section the first character in the file extension “S” indicates that the image is a digitally signed software image, the second character “P” indicates that the image is digitally signed using a production key, and the third character “A” indicates that the key version is version A.

Displaying Digitally Signed Cisco Software Signature Information Example

The following example shows how to display information related to software authentication for the current ROMmon and Cisco IOS image file used for booting:

```
Device# show software authenticity running
SYSTEM IMAGE
-------------------
Image type                  : Development
    Signer Information
        Common Name         : xxx
        Organization Unit   : xxx
        Organization Name   : xxx
    Certificate Serial Number : xxx
    Hash Algorithm          : xxx
    Signature Algorithm     : 2048-bit RSA
    Key Version             : xxx

    Verifier Information
        Verifier Name       : ROMMON 2
        Verifier Version    :  System Bootstrap, Version 12.4(20090409:084310)
ROMMON 2
```

```
---------------
Image type                  : xxx
    Signer Information
        Common Name         : xxx
        Organization Unit   : xxx
        Organization Name   : xxx
    Certificate Serial Number : xxx
    Hash Algorithm          : xxx
    Signature Algorithm     : 2048-bit RSA
    Key Version             : xx

    Verifier Information
        Verifier Name       : ROMMON 2
        Verifier Version    :  System Bootstrap, Version 12.4(20090409:084310) [
```

The table below describes the significant fields shown in the display.

Table 5: show software authenticity running Field Descriptions

Field	Description
SYSTEM IMAGE	Section of the output displaying the system image information.
Image type	Displays the type of image.
Common Name	Displays the name of the software manufacturer.
Organization Unit	Displays the hardware the software image is deployed on.
Organization Name	Displays the owner of the software image.
Certificate Serial Number	Displays the certificate serial number for the digital signature.
Hash Algorithm	Displays the type of hash algorithm used in digital signature verification.
Signature Algorithm	Displays the type of signature algorithm used in digital signature verification.
Key Version	Displays the key version used for verification.
Verifier Name	Name of the program responsible for performing the digital signature verification.
Verifier Version	Version of the program responsible for performing the digital signature verification.
ROMMON 2	Section of the output displaying the current ROMmon information.

Displaying the Digital Signature Information for a Specific Image File Example

The following example shows how to display the digital signature information related to software authentication for a specific image file:

Device# **showsoftwareauthenticityfileflash0:**c3900-universalk9-mz.SSA

```
File Name                     : flash0:c3900-universalk9-mz.SSA
Image type                    : Development
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

The table below describes the significant fields shown in the display.

Table 6: show software authenticity file Field Descriptions

Field	Description
File Name	Name of the filename in the memory. For example, flash0:c3900-universalk9-mz.SSA refers to filename c3900-universalk9-mz.SSA in flash memory (flash0:).
Image type	Displays the type of image.
Signer Information	Signature information.
Common Name	Displays the name of the software manufacturer.
Organization Unit	Displays the hardware the software image is deployed on.
Organization Name	Displays the owner of the software image.
Certificate Serial Number	Displays the certificate serial number for the digital signature.
Hash Algorithm	Displays the type of hash algorithm used in digital signature verification.
Signature Algorithm	Displays the type of signature algorithm used in digital signature verification.
Key Version	Displays the key version used for verification.

Displaying Digitally Signed Cisco Software Key Information Example

The following example displays digitally signed Cisco software key information. The information details the software public keys that are in storage, including their key types.

```
Device# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release  (Primary)
Public Key Algorithm : RSA
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ...
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development  (Primary)
Public Key Algorithm : RSA
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ....
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version           : A
```

The table below describes the significant fields shown in the display.

Table 7: show software authenticity keys Field Descriptions

Field	Description
Public Key #	Public key number.
Key Type	Displays the key type used for image verification.
Public Key Algorithm	Displays the name of the algorithm used for public key cryptography.
Modulus	Modulus of the public key algorithm.
Exponent	Exponent of the public key algorithm
Key Version	Displays the key version used for verification.

Performing Special Key Revocation for Digitally Signed Cisco Software Example

The following example displays a special key revocation process:

```
Device# software authenticity key add special
Validating running image...
Validating new special key...
```

```
Adding the key to Primary
Checking for duplicate keys
Writing the key...e.Success
Adding the key to Backup
Checking for duplicate keys
Writing the key...e.Success
Done!
```

The software authenticity key add special command adds the new special key to the primary and backup storage areas of the router and verifies that a duplicate key is not present.

```
Device# copy tftp: usbflash0:
Address or name of remote host []? 209.165.200.226
Source filename []? rommon_image_location/ C3900_rom-monitor.srec.SSB
```

The new ROMmon special image file with a new special key is copied to the ROMmon storage area (usbflash0:).

```
Device# copy /verify tftp: usbflash0:
Address or name of remote host []? 209.165.200.225
Source filename []? image_location/c3900-universalk9-mz.SSB
Destination filename [c3900-universalk9-mz.SSB]?
Accessing tftp:// 209.165.200.225/image_location/c3900-universalk9-mz.SSB...
Loading image_location/c3900-universalk9-mz.SSB from 209.165.200.225 (via GigabitEthernet0/0):

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 52291428 bytes]

52291428 bytes copied in 124.804 secs (418988 bytes/sec)

Starting image verification
Hash Computation:    100% Done!
Computed Hash   SHA2: 7F54083493EB6B06234CFC5266E538E7
                      .....
                      .....
                      0B17572E9A33735ADCEE26A4E3FDB662

Embedded Hash   SHA2: 7F54083493EB6B06234CFC5266E538E7
                      .....
                      .....
                      0B17572E9A33735ADCEE26A4E3FDB662

CCO Hash        MD5 : 966D4092FA8F5F2E0F74BDCF46511CF7
Digital signature successfully verified in file usbflash0:/c3900-universalk9-mz.SSB
```

The new special image file with a new special key is copied to the image storage area in the router (usbflash0:) and the signature of the image is verified successfully.

```
Device# upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
Platform Field Upgradeable ROMMON LOAD test
___________________________________________
RSA Signature Verification Passed ...
ROM: Digitally Signed Development Software

This command will result in a  'power-on reset' of the router!
Continue? [yes/no]: yes
ROMMON image upgrade in progress.

Erasing boot flash eeeeeeeeeeeeeeeeeeeeeeee
Programming boot flash .......................
Now Reloading
FPGA System Reset Fail; Performing IOCTRL System reset

System Bootstrap, Version 15.0(1r)M3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2009 by cisco Systems, Inc.

Total memory size = 1024 MB - DIMM0 = 512 MB, DIMM1 = 512 MB

 Running new upgrade for first time

System Bootstrap, Version 12.4(20090921:163953) [image-rommon 152], DEVELOPMENT SOFTWARE
```

```
Copyright (c) 1994-2009 by cisco Systems, Inc.

Total memory size = 1024 MB - DIMM0 = 512 MB, DIMM1 = 512 MB
Field Upgradeable ROMMON Integrity test
_____________________________________
ROM: Digitally Signed Development Software
CISCO3945 with CISCO3900-MPE140 with 1048576 Kbytes of main memory
Main memory is configured to 72/72(dimm 0/1) bit mode with ECC enabled
Upgrade ROMMON initialized
program load complete, entry point: 0x4000000, size: 0x3f520
Continue to reload the same Production image
```

The ROMmon file is upgraded to the new ROMmon file in the router.

```
Device# software authenticity key revoke special
Finding the new special key in the key storage
Validating running image...
Revoking keys with version less than B
Validating upgradable rommon...
Scanning the keys in Primary
Revoking the key with version A...e.Success
Scanning the keys in Backup
Revoking the key with version A...e.Success
Done!

Device#
*Mar  8 10:29:17.219 PST: %DIGISIGN-4-DEV_IMAGE:
Upgradable rommon software signed using special key version B
```

The old special key (Rev A) is revoked from the primary and backup key storage areas.

Enabling Debugging of Digitally Signed Cisco Software Image Key Information Example

The following example shows how to enable debugging of software authentication events relating to key information for digitally signed Cisco software:

```
Device# debug software authenticity key
```

Additional References

The following sections provide references related to the Digitally Signed Cisco Software feature.

Related Documents

Related Topic	Document Title
Overview of Cisco IOS software activation	Cisco IOS Software Activation Conceptual Overview
Commands related to Cisco IOS software activation	Cisco IOS Software Activation Tasks and Commands

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Digitally Signed Cisco Software

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 8: Feature Information for Digitally Signed Cisco Software

Feature Name	Releases	Feature Information
Digitally Signed Cisco Software	Cisco IOS 15.0(1)M Cisco IOS 15.0(1)M2 Cisco IOS 15.1(1)T Cisco IOS XE 3.1.0SG	The Digitally Signed Cisco Software feature describes how to identify digitally signed Cisco software, gather software authentication information related to digitally signed images, and perform key revocation. Digitally Signed Cisco software is software that is digitally signed using secure asymmetrical (public-key) cryptography. The following commands were introduced or modified: **debug software authenticity, show software authenticity file, show software authenticity keys, show software authenticity running.**
Key Revocation Feature Support	Cisco IOS 15.0(1)M2 Cisco IOS 15.1(1)T	Key revocation feature support was added. Key revocation removes a key from a platform's key storage. A platform can host a production or special image, and a production key (from a production image) or special key (from a special image) may be revoked during key revocation. The following section provides information about this feature: • Digitally Signed Cisco Software Key Revocation and Replacement The following commands were introduced or modified: **debug software authenticity, show software authenticity upgrade-status, software authenticity key add, software authenticity key revoke, upgrade rom-monitor file.**