archive tar

To create a TAR file, to list files in a TAR file, or to extract the files from a TAR file, use the **archive tar** command in privileged EXEC mode.

archive tar {/**create** *destination-url***flash:**/*file-url* | /**table** *source-url* | /**xtract** *source-url***flash:**/*file-url* [*dir*/*file***...**]}

Syntax Description

/**create** *destination-url* **flash:**/ *file-url*	Creates a new TAR file on the local or network file system. For *destination-url*, specify the destination URL alias for the local or network file system and the name of the TAR file to create. The following options are supported: • **flash:** --Syntax for the local flash file system. • **ftp:** [[// *username*[**:** *password*]**@** *location*]/ *directory*]/ *tar-filename.tar*-- Syntax for FTP. • **rcp:** [[// *username* **@** *location*]/ *directory*]/ *tar-filename.tar*--Syntax for Remote Copy Protocol (RCP). • **tftp:** [[// *location*]/ *directory*]/ *tar-filename.tar*--Syntax for TFTP. The *tar-filename.tar* is the name of the TAR file to be created. For **flash:**/ *file-url*, specify the location on the local flash file system from which the new TAR file is created. An optional list of files or directories within the source directory can be specified to write to the new TAR file. If none is specified, all files and directories at this level are written to the newly created TAR file.

/table *source-url*	Display the contents of an existing TAR file to the screen. For *source-url*, specify the source URL alias for the local or network file system. The following options are supported: • **flash:** --Syntax for the local flash file system. • **ftp:** [[// *username*[**:** *password*]**@** *location*]/ *directory*]/ *tar-filename.tar*-- Syntax for FTP. • **rcp:** [[// *username* **@** *location*]/ *directory*]/ *tar-filename.tar*--Syntax for Remote Copy Protocol (RCP). • **tftp:** [[// *location*]/ *directory*]/ *tar-filename.tar*--Syntax for TFTP. The *tar-filename.tar* is the name of the TAR file to be created.
/xtract *source-url* **flash:**/ *file-url* [*dir/file...*]	Extracts files from a TAR file to the local file system. For *source-url*, specify the source URL alias for the local file system. These options are supported: • **flash:** --Syntax for the local flash file system. • **ftp:** [[// *username*[**:** *password*]**@** *location*]/ *directory*]/ *tar-filename.tar*-- Syntax for FTP. • **rcp:** [[// *username* **@** *location*]/ *directory*]/ *tar-filename.tar*--Syntax for Remote Copy Protocol (RCP). • **tftp:** [[// *location*]/*directory*]/*tar-filename.tar*--Syntax for TFTP. The *tar-filename.tar* is the name of the TAR file to be created.

Command Default

The TAR archive file is not created.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(13)AY	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Release	Modification
12.4(22)YB	This command was integrated into Cisco IOS Release 12.4(22)YB.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

Filenames, directory names, and image names are case sensitive.

The TAR file is an archive file from which you can extract files by using the **archive tar**command.

Examples

The following example shows how to create a TAR file. The command writes the contents of the new-configs directory on the local flash device to a file named saved.tar on the TFTP server at 172.20.136.9.

```
Switch# archive tar /create tftp:172.20.136.9/saved.tar flash:/new-configs
```

The following example shows how to display the contents of the c2940-tv0-m.tar file that is in flash memory. The contents of the TAR file appear on the screen.

```
Switch# archive tar /table flash:c2940-tv0-m.tar

info (219 bytes)
c2940-tv0-mz-121/ (directory)
c2940-tv0-mz-121/html/ (directory)
c2940-tv0-mz-121/html/foo.html (0 bytes)
c2940-tv0-mz-121/vegas-tv0-mz-121.bin (610856 bytes)
c2940-tv0-mz-121/info (219 bytes)
info.ver (219 bytes)
```

The following example shows how to extract the contents of a TAR file on the TFTP server at 172.20.10.30. This command extracts only the new-configs directory into the root directory on the local flash file system. The remaining files in the saved.tar file are ignored.

```
Switch# archive tar /xtract tftp:/172.20.10.30/saved.tar flash:/ new-configs
```

boot system

To specify the system image that the router loads at startup, use one of the following **boot system** command in global configuration mode. To remove the startup system image specification, use the **no** form of this command.

Loading System Image from a URL or a TFTP File

boot system {*file-url* | *filename*}

no boot system {*file-url* | *filename*}

Booting from a System Image in Internal Flash

boot system flash [*flash-fs***:**] [*partition-number***:**] [*filename*]

no boot system flash [*flash-fs***:**] [*partition-number***:**] [*filename*]

Booting from a MOP Server

boot system mop *filename* [*mac-address*] [*interface*]

no boot system mop *filename* [*mac-address*] [*interface*]

Booting from ROM

boot system rom

no boot system rom

Booting a System Image from a Network, TFTP, or FTP Server

boot system {**rcp** | **tftp** | **ftp**} *filename* [*ip-address*]

no boot system {**rcp** | **tftp** | **ftp**} *filename* [*ip-address*]

Syntax Description

file-url	The URL of the system image to load at system startup.

filename	The TFTP filename of the system image to load at system startup.
flash	On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from internal flash memory. If you omit all arguments that follow this keyword, the system searches internal Flash for the first bootable image. On the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from the flash system specified by the *flash-fs* **:** argument. On the Cisco 1600 series and Cisco 3600 series routers, if you omit all optional arguments, the router searches internal flash memory for the first bootable image. On the Cisco 7000 family routers, when you omit all arguments that follow this keyword, the system searches the Personal Computer Memory Card Industry Association (PCMCIA) slot 0 for the first bootable image.
flash-fs **:**	(Optional) Flash file system containing the system image to load at startup. The colon is required. Valid file systems are as follows: • **flash:** --Internal flash memory on the Cisco 1600 series and Cisco 3600 series routers. For the Cisco 1600 series and Cisco 3600 series routers, this file system is the default if you do not specify a file system. This is the only valid file system for the Cisco 1600 series. • **bootflash:** --Internal flash memory in the Cisco 7000 family. • **slot0:** --First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers . For the Cisco 7000 family routers , this file system is the default if you do not specify a file system. • **slot1:** --Flash memory card in the second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. On the Cisco 2600 series routers, a file system should be specified. Otherwise, the router may attempt to load the Cisco IOS software twice with unexpected results.

partition-number **:**	(Optional) Number of the flash memory partition that contains the system image to boot, specified by the optional *filename* argument. If you do not specify a filename, the router loads the first valid file in the specified partition of flash memory. This argument is valid only on routers that can be partitioned.
filename	(Optional when used with the **boot system flash** command) Name of the system image to load at startup. This argument is case sensitive. If you do not specify a value for the *filename*argument, the router loads the first valid file in the following: • The specified flash file system • The specified partition of flash memory • The default flash file system if you also omitted the *flash-fs* **:** argument
mop	Boots the router from a system image stored on a DECNET Maintenance Operations Protocol (MOP) server. Do not use this keyword with the Cisco 3600 series or Cisco 7000 family routers .
mac-address	(Optional) MAC address of the MOP server containing the specified system image file. If you do not include the MAC address argument, the router sends a broadcast message to all MOP boot servers. The first MOP server to indicate that it has the specified file is the server from which the router gets the boot image.
interface	(Optional) Interface the router uses to send out MOP requests to the MOP server. The interface options are **async**, **dialer**, **ethernet**, **serial**, and **tunnel**. If you do not specify the *interface* argument, the router sends a request out on all interfaces that have MOP enabled. The interface that receives the first response is the interface the router uses to load the software.
rom	Boots the router from ROM. Do not use this keyword with the Cisco 3600 series or the Cisco 7000 family routers .
rcp	Boots the router from a system image stored on a network server using rcp.
tftp	Boots the router from a system image stored on a TFTP server.

ftp	Boots the router from a system image stored on an FTP server.
ip-address	(Optional) IP address of the server containing the system image file. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

Command Default

If you configure the router to boot from a network server but do not specify a system image file with the **boot system** command, the router uses the configuration register settings to determine the default system image filename. 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). Refer to the appropriate hardware installation guide for details on the configuration register and default filename. See also the **config-register** or **confreg** command.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

For this command to work, the **config-register** command must be set properly.

Create a comma-delimited list of several **boot system** commands to provide a fail-safe method for booting your router. The router stores and executes the **boot system** commands in the order in which you enter them in the configuration file. If you enter multiple boot commands of the same type--for example, if you enter two commands that instruct the router to boot from different network servers--the router tries them in the order in which they appear in the configuration file. If a **boot system** command entry in the list specifies an invalid device, the router omits that entry. Use the **boot system rom** command to specify use of the ROM system image as a backup to other **boot** system commands in the configuration.

Note After a list of several images are specified with the **boot system** command, running the command again results in the list being appended, not removed.

For some platforms, the boot image must be loaded before the system image is loaded. However, on many platforms, the boot image is loaded only if the router is booting from a network server or if the flash file system is not specified. If the file system is specified, the router will boot faster because it need not load the boot image first.

This section contains the following topics:

- Changing the List of Boot System Commands
- Booting Compressed Images
- Understanding rcp
- Understanding TFTP
- Understanding FTP
- Stopping Booting and Entering ROM Monitor Mode
- Cisco 1600 Series, Cisco 3600 Series, Cisco 7000 Family, and Cisco 7600 Series Router Notes

Changing the List of Boot System Commands

To remove a single entry from the bootable image list, use the **no** form of the command with an argument. For example, to remove the entry that specifies a bootable image on a flash memory card inserted in the second slot, use the **no boot system flash slot1:** *filename*] command. All other entries in the list remain.

To eliminate all entries in the bootable image list, use the **no boot system** command. At this point, you can redefine the list of bootable images using the previous **boot system** commands. Remember to save your changes to your startup configuration by issuing the **copy system:running-config nvram:startup-config** command.

Each time you write a new software image to flash memory, you must delete the existing filename in the configuration file with the **no boot system flash** *filename* command. Then add a new line in the configuration file with the **boot system flash** *filename* command.

Note If you want to rearrange the order of the entries in the configuration file, you must first issue the **no boot system** command and then redefine the list.

Booting Compressed Images

You can boot the router from a compressed image on a network server. When a network server boots software, both the image being booted and the running image must be able to fit into memory. Use compressed images to ensure that enough memory is available to boot the router. You can compress a software image on any UNIX platform using the **compress** command. Refer to your UNIX platform's documentation for the exact usage of the **compress** command. (You can also uncompress data with the UNIX **uncompress** command.)

Understanding rcp

The rcp requires that a client send the remote username in an rcp request to a server. When the router executes the **boot system rcp** command, the Cisco IOS software sends the hostname as both the remote and local usernames by default. Before the rcp can execute properly, an account must be defined on the network server for the remote username configured on the router.

If the server has a directory structure, the rcp software searches for the system image to boot from the remote server relative to the directory of the remote username.

By default, the router software sends the hostname as the remote username. You can override the default remote username by using the **ip rcmd remote-username** command. For example, if the system image resides in the home directory of a user on the server, you can specify that user's name as the remote username.

Understanding TFTP

You need a TFTP server running to retrieve the router image from the host.

Understanding FTP

You need an FTP server running to retrieve the router image from the host. You also need an account on the server or anonymous file access to the server.

Stopping Booting and Entering ROM Monitor Mode

During the first 60 seconds of startup, you can force the router to stop booting by pressing the Break key. The router will enter ROM monitor mode, where you can change the configuration register value or boot the router manually.

Cisco 1600 Series, Cisco 3600 Series, Cisco 7000 Family, and Cisco 7600 Series Router Notes

For the Cisco 3600 series and Cisco 7000 family, the **boot system** command modifies the BOOT variable in the running configuration. The BOOT variable specifies a list of bootable images on various devices.

Note When you use the **boot system** command on the Cisco 1600 series, Cisco 3600 series, Cisco 7000 family, and Cisco 7600 series, you affect only the running configuration. You must save the BOOT variable settings to your startup configuration to place the information under ROM monitor control and to have the variable function as expected. Use the **copy system:running-config nvram:startup-config** privileged EXEC command to save the variable from your running configuration to your startup configuration.

To display the contents of the BOOT variable, use the **show bootvar** EXEC command.

Examples

The following example illustrates a configuration that specifies two possible internetwork locations for a system image, with the ROM software being used as a backup:

```
Router(config)# boot system tftp://192.168.7.24/cs3-rx.90-1
Router(config)# boot system tftp://192.168.7.19/cs3-rx.83-2
Router(config)# boot system rom
```

The following example boots the system boot relocatable image file named igs-bpx-l from partition 2 of the flash device:

```
Router(config)# boot system flash:2:igs-bpx-l
```

The following example instructs the router to boot from an image located on the flash memory card inserted in slot 0:

```
Router(config)# boot system slot0:new-config
```

The following example specifies the file named new-ios-image as the system image for a Cisco 3600 series router to load at startup. This file is located in the fourth partition of the flash memory card in slot 0.

```
Router(config)# boot system slot0:4:dirt/images/new-ios-image
```

This example boots from the image fi le named c1600-y-l in part ition 2 of flash memory of a Cisco 1600 series router:

```
Router(config)# boot system flash:2:c1600-y-l
```

Related Commands

Command	Description
boot	Boots the router manually.
config-register	Changes the configuration register settings.
confreg	Changes the configuration register settings while in ROM monitor mode.
copy	Copies any file from a source to a destination.
copy system:running-config nvram:startup-config	Copies the running configuration to the startup configuration.
ip rcmd remote username	Configures the remote username to be used when requesting a remote copy using rcp.
show bootvar	Displays the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting.

copy

To copy any file from a source to a destination, use the **copy** command in privileged EXEC or diagnostic mode.

copy [**/erase**] [**/verify** | **/noverify**] *source-url destination-url*

Syntax Description

/erase	(Optional) Erases the destination file system before copying. **Note** This option is typically provided on platforms with limited memory to allow for an easy way to clear local flash memory space.
/verify	(Optional) Verifies the digital signature of the destination file. If verification fails, the file is deleted from the destination file system. This option applies to Cisco IOS software image files only.
/noverify	(Optional) If the file being copied is an image file, this keyword disables the automatic image verification that occurs after an image is copied. **Note** This keyword is often issued if the **file verify auto** command is enabled, which automatically verifies the digital signature of all images that are copied.
source-url	The location URL (or alias) of the source file or directory to be copied. The source can be either local or remote, depending upon whether the file is being downloaded or uploaded.
destination-url	The destination URL (or alias) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded.

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or a filename that follows the standard Cisco IOS file system syntax (*filesystem* :[/*filepath*][/*filename*]).

The table below shows two keyword shortcuts to URLs.

Table 1 Common Keyword Aliases to URLs

Keyword	Source or Destination
running-config	(Optional) Keyword alias for the **system:running-config** URL. The **system:running-config** keyword represents the current running configuration file. This keyword does not work in **more** and **show file** EXEC command syntaxes.
startup-config	(Optional) Keyword alias for the **nvram:startup-config**URL**.** The **nvram:startup-config** keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 family, which uses the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series cannot use the **copy running-config startup-config**command. This keyword does not work in **more** and **show file** EXEC command syntaxes.

The following tables list URL prefix keywords by file system type. The available file systems will vary by platform. If you do not specify a URL prefix keyword, the router looks for a file in the current directory.

The table below lists URL prefix keywords for Special (opaque) file systems.

Table 2 URL Prefix Keywords for Special File Systems

Keyword	Source or Destination
cns:	Source URL for Cisco Networking Services files.
flh:	Source URL for flash load helper log files.
logging	Source URL which copies messages from the logging buffer to a file.
modem:	Destination URL for loading modem firmware on to supported networking devices.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.

Keyword	Source or Destination
obfl:	Source or destination URL for Onboard Failure Logging files.
stby-nvram:	Router NVRAM on the standby hardware. You can copy the startup configuration to NVRAM or from NVRAM.
stby-obfl:	Source or destination URL for Onboard Failure Logging files on the standby hardware.
system:	Source or destination URL for system memory, which includes the running configuration.
tar:	Source URL for the archive file system.
tmpsys:	Source or destination URL for the temporary system files.
xmodem:	Source or destination for a file from a network machine that uses the Xmodem protocol.
ymodem:	Source or destination for a file from a network machine that uses the Ymodem protocol.

The table belows lists URL prefix keywords for remote file systems.

Table 3 URL Prefix Keywords for Remote File Systems

Keyword	Source or Destination
ftp:	Source or destination URL for FTP network server. The syntax for this alias is as follows:**ftp:**[[[// username [:password]@]location]/directory]/ filename.
http://	Source or destination URL for an HTTP server (also called a web server). The syntax for this alias is as follows: http:// [[*username*:*password*]@] {*hostname* | *host-ip*}[/ *filepath*]/ *filename*
https://	Source or destination URL for a Secure HTTP (HTTPS) server. HTTPS uses Secure Socket Layer (SSL) encryption. The syntax for this alias is as follows:**https://**[[*username*:*password*]@]{*hostname* | *host-ip*}[/ *filepath*]/ *filename*
rcp:	Source or destination URL for a remote copy protocol (rcp) network server. The syntax for this alias is as follows:**rcp:**[[[//username@] location]/ directory]/filename

Keyword	Source or Destination
scp:	Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows:**scp://** *username@location*[/*directory*][/*filename*]
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is as follows:**tftp:** [[//location]/directory]/filename.

The table below lists URL prefix keywords for local writable storage file systems.

Table 4 URL Prefix Keywords for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of disk-based media.
flash:	Source or destination URL for flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that flash: is aliased to slot0:, allowing you to refer to the main flash memory storage area on all platforms.
harddisk:	Source or destination URL of the active harddisk file system.
slavebootflash:	Source or destination URL for internal flash memory on the slave RSP card of a router configured for HSA.
slaveram:	NVRAM on a slave RSP card of a router configured for HSA.
slaveslot0:	Source or destination URL of the first Personal Computer Memory Card International Association (PCMCIA) card on a slave RSP card of a router configured for HSA.
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.
slot0:	Source or destination URL of the first PCMCIA flash memory card.
slot1:	Source or destination URL of the second PCMCIA flash memory card.

Alias	Source or Destination
stby-bootflash:	Source or destination URL for boot flash memory in standby RP.
stby-harddisk:	Source or destination URL for the standby harddisk.
stby-usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the standby RP.
usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the active RP.
usbflash 0 9 :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router.
usbtoken [**0 9**] :	Source or destination URL for the USB eToken that has been plugged into the router.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
11.3T	This command was introduced.
12.3(2)T	• The **http://** and **https://** keywords were added as supported remote source locations (file system URL prefixes) for files. • This command was enhanced to support copying files to servers that support SSH and the scp.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)S	The /**verify**and /**noverify** keywords were added.
12.0(26)S	The /**verify**and /**noverify** keywords were integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	The /**verify**and /**noverify** keywords were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.3(7)T	The **http://** and **https://** keywords were enhanced to support file uploads.
12.3(14)T	The **usbflash 0 9 :**and **usbtoken 0 9 :**keywords were added to support USB storage.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	The Cisco ASR1000 series routers became available, and introduced the **copy** command in diagnostic mode.

Usage Guidelines

The fundamental function of the **copy** command is to allow you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file is specified using a Cisco IOS File System URL, which allows you to specify any supported local or remote file location. The file system being used (such as a local memory source, or a remote server) dictates the syntax used in the command.

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the **copy** command and have the router prompt you for any missing information.

For local file systems, two commonly used aliases exist for the **system:running-config** and **nvram:startup-config** files; these aliases are **running-config** and **startup-config**, respectively.

Timesaver

Aliases are used to reduce the amount of typing you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config**command). These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

The colon is required after the file system URL prefix keywords (such as **flash**). In some cases, file system prefixes that did not require colons in earlier software releases are allowed for backwards compatibility, but use of the colon is recommended.

In the URL syntax for **ftp:**, **http:**, **https:**, **rcp:**, **scp:** and **tftp:**, the location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers.

The following sections contain usage guidelines for the following topics:

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Understanding Character Descriptions

The table below describes the characters that you may see during processing of the **copy**command.

Table 5 copy Character Descriptions

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.
O	For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail.
e	For flash erasures, a lowercase e indicates that a device is being erased.
E	An uppercase E indicates an error. The copy process may fail.
V	A series of uppercase Vs indicates the progress during the verification of the image checksum.

Understanding Partitions

You cannot copy an image or configuration file to a flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available flash partitions by entering the **show file system** EXECcommand.

Using rcp

The rcp requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1 The remote username specified in the **copy** command, if a username is specified.
2 The username set by the **ip rcmd remote-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** command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that username 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, add an entry to the *.rhosts* file for the remote user on the rcp server. Suppose the router contains the following configuration lines:

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

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

```
Router1.company.com Rtr1
```

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

If you are using a personal computer as a file server, the computer must support the remote shell protocol (rsh).

Using FTP

The FTP protocol requires a client to send a username and password with each FTP request to a remote FTP server. Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a default username and password for all copy operations to or from an FTP server. Include the username in the **copy** command syntax if you want to specify a username for that copy operation only.

When you copy a file from the router to a server using FTP, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

Note The Syslog message will display 'xxxx' in place of the password entered in the syntax of the **copy** {**ftp:**} command.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that username as the remote username.

Refer to the documentation for your FTP server for details on setting up the server.

Using HTTP or HTTPS

Copying a file to or from a remote HTTP or HTTPS server, to or from a local file system, is performed using the embedded Secure HTTP client that is integrated in Cisco IOS software. The HTTP client is enabled by default.

Downloading files from a remote HTTP or HTTPS server is performed using the HTTP client integrated in Cisco IOS software.

If a username and password are not specified in the **copy** command syntax, the system uses the default HTTP client username and password, if configured.

When you copy a file from a remote HTTP or HTTPS server, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip http client username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip http client password** command, if the command is configured.
3. The router forms the password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Storing Images on Servers

Use the **copy flash:** *destination-url*command (for example, **copy flash: tftp:**) to copy a system image or boot image from flash memory to a network server. You can use the copy of the image as a backup copy. Also, you can also use the image backup file to verify that the image in flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the **copy** *destination-url* **flash:** command (for example, **copy tftp: flash:**) to copy an image from a server to flash memory.

On Class B file system platforms, the system provides an option to erase existing flash memory before writing onto it.

Note Verify the image in flash memory before booting the image.

Verifying Images

When copying a new image to your router, you should confirm that the image was not corrupted during the copy process. You can verify the integrity of the image in any of the following ways:

- Depending on the destination file system type, a checksum for the image file may be displayed when the **copy** command completes. You can verify this checksum by comparing it to the checksum value provided for your image file on Cisco.com.

Caution If the checksum values do not match, do not reboot the router. Instead, reissue the **copy**command and compare the checksums again. If the checksum is repeatedly wrong, copy the original 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 memory, the router will start the system image contained in ROM (assuming booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

- Use the **/verify**keyword.
- Enable automatic image verification by default by issuing the **file verify auto** command. This command will automatically check the integrity of each file that is copied via the **copy** command (without specifying the **/verify**option) to the router unless the **/noverify** keyword is specified.
- Use the UNIX 'diff' command. This method can also be applied to file types other than Cisco IOS images. If you suspect that a file is corrupted, copy the suspect file and the original file to a UNIX server. (The file names may need to be modified if you try to save the files in the same directory.) Then run the UNIX 'diff' command on the two files. If there is no difference, then the file has not been corrupted.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy** {**ftp:** | **rcp:** | **scp:** | **tftp: running-config**command to load a configuration file from a network server to the running configuration of the router. (Note that **running-config** is the alias for the **system:running-config** keyword.) The configuration will be added to the running configuration as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** {**ftp:** | **rcp:** | **scp:** | **tftp:**} **nvram:startup-config**command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy system:running-config** {**ftp:** | **rcp:** | **scp:** | **tftp:**} command to copy the current configuration file to a network server using FTP, rcp, scp, or TFTP. Use the **copy nvram:startup-config** {**ftp:** | **rcp:** | **scp:** | **tftp:**} command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy system:running-config nvram:startup-config** command to copy the running configuration to the startup configuration.

Note Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the **copy system:running-config nvram:startup-config**command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to NVRAM.

On the Class A flash file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than **nvram:** (that is, **flash:**, **bootflash:**, **slot0:**, or **slot1:**), the software writes the current configuration to the specified device and filename, and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

For the Class A flash file system platforms, specifications are as follows:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOTLDR environment variable specifies the flash device and filename containing the rxboot image that ROM uses for booting.
- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the flash memory device and filename that are used as the boot helper; the default is the first system image in flash memory.

To view the contents of environment variables, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config**command.

When the destination of a **copy** command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

Using the Copy Command with the Dual RSP Feature

The Dual RSP feature allows you to install two Route Switch Processor (RSP) cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for Dual RSPs, if you copy a file to **nvram:startup-configuration** with automatic synchronization disabled, the system prompts whether you also want to copy the file to the slave startup configuration. The default answer is **yes**. If automatic synchronization is enabled, the system automatically copies the file to the slave startup configuration each time you use a **copy** command with **nvram:startup-configuration** as the destination.

Using the copy command with the ASR1000 Series Routers

The **copy** command is available in both privileged EXEC and diagnostic mode on the Cisco ASR1000 series routers. Because the **copy**command is available in diagnostic mode, it can be used to copy all types of files between directories and remote locations even in the event of an IOS failure.

Examples

The following examples illustrate uses of the **copy** command:

Verifying the Integrity of the Image Before It Is Copied Example

The following example shows how to specify image verification before copying an image:

```
Router# copy /verify tftp://10.1.1.1/cisco/c7200-js-mz disk0:
Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/cisco/c7200-js-mz...
Loading cisco/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]
19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-
mz  ....................................................
..........................................................................................
.........
..........................................................................................
.........
.......................................Done!
Embedded Hash         MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash                MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash                        MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

Copying an Image from a Server to Flash Memory Examples

The following examples use a **copy rcp:**, **copy tftp:**, or **copy ftp:** command to copy an image file from a server to flash memory:

Copying an Image from a Server to Flash Memory Example

The following example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of flash memory to ensure that enough flash memory is available to accommodate the system image.

```
Router#
copy rcp://netadmin@172.16.101.101/file1 flash:file1
Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
```

```
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]
Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual flash bank support in boot ROMs. If the partition entered is not valid, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?** *number*) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual flash bank support in boot ROM, so the system uses flash Load Helper.

```
Router# copy tftp: flash:

System flash partition information:
Partition   Size     Used    Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K   2048K   2048K       Read/Write  Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
                              **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                              ---- ******** ----
Proceed? [confirm]
System flash directory, partition 1:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [255.255.255.255]? 172.16.1.1

Source file name? master/igs-bfpx-100.4.3

Destination file name [default = source name]?
Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from TFTP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

Copying an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software prompts you to erase the files on the flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:
PCMCIA Slot0 flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3068K     1027K     4096K      Read/Write     Direct
  2         4096K   1671K     2424K     4096K      Read/Write     Direct
  3         4096K      0K     4095K     4096K      Read/Write     Direct
  4         4096K   3825K      270K     4096K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
```

```
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   3142288  c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz

Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/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/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no]
yes

Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-
mz: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]
```

Saving a Copy of an Image on a Server Examples

The following examples use **copy** commands to copy image files to a server for storage:

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from flash Memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```
Router#
copy flash: rcp:
IP address of remote host [255.255.255.255]? 172.16.13.110
Name of file to copy? gsxx
writing gsxx - copy complete
```

Copy an Image from Flash Memory to an SSH Server Using scp Example

The following example shows how to use scp to copy a system image from flash memory to a server that supports SSH:

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/

Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Before you can use the server-side functionality, SSH, authentication, and authorization must be properly configured so the router can determine whether a user is at the right privilege level. The scp server-side functionality is configured with the **ip scp server enable** command.

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?** *number*) for a directory display of a particular partition. The default is the first partition.

```
Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:
System flash partition information:
Partition   Size     Used     Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K    2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K    2048K   2048K       Read/Write  Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]?
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying an Image from a Flash Memory File System to an FTP Server Example

The following example copies the file c3600-i-mz from partition 1 of the flash memory card in slot 0 to an FTP server at IP address 172.23.1.129:

```
Router# show slot0: partition 1
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]
Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)...  OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
  as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

Copying an Image from Boot Flash Memory to a TFTP Server Example

The following example copies an image from boot flash memory to a TFTP server:

```
Router#
copy bootflash:file1 tftp://192.168.117.23/file1
Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
  as 'file1'? [yes/no]y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying a Configuration File from a Server to the Running Configuration Example

The following example copies and runs a configuration filename host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```
Router#
copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copying a Configuration File from a Server to the Startup Configuration Example

The following example copies a configuration file host2-confg from a remote FTP server to the startup configuration. The IP address is 172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router#
copy ftp://netadmin1:ftppass@172.16.101.101/host2-confg nvram:startup-config
Configure using rtr2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-confg:![OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by
FTP from 172.16.101.101
```

Copying the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named rtr2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

```
Router# configure terminal

Router(config)# ip rcmd remote-username netadmin1

Router(config)#
end

Router#
copy system:running-config rcp:

Remote host[]? 172.16.101.101

Name of configuration file to write [Rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
```

Copying the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

```
Router#
copy nvram:startup-config tftp:
Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Saving the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE variable.

```
copy system:running-config nvram:startup-config
```

The following example shows the warning that the system provides if you try to save configuration information from bootstrap into the system:

```
Router(boot)# copy system:running-config nvram:startup-config
Warning: Attempting to overwrite an NVRAM configuration written
by a full system image. This bootstrap software does not support
the full configuration command set. If you perform this command now,
some configuration commands may be lost.
Overwrite the previous NVRAM configuration?[confirm]
```

Enter no to escape writing the configuration information to memory.

Moving Configuration Files to Other Locations Examples

On some routers, you can store copies of configuration files on a flash memory device. Five examples follow:

Copying the Startup Configuration to a Flash Memory Device Example

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a flash memory card inserted in slot 0:

```
Router# copy nvram:startup-config slot0:router-confg
```

Copying the Running Configuration to a Flash Memory Device Example

The following example copies the running configuration from the router to the flash memory PC card in slot 0:

```
Router# copy system:running-config slot0:berlin-cfg

Building configuration...

5267 bytes copied in 0.720 secs
```

Copying to the Running Configuration from a Flash Memory Device Example

The following example copies the file named ios-upgrade-1 from the flash memory card in slot 0 to the running configuration:

```
Router# copy slot0:4:ios-upgrade-1 system:running-config
Copy
'ios-upgrade-1
' from flash device
  as 'running-config' ? [yes/no] yes
```

Copying to the Startup Configuration from a Flash Memory Device Example

The following example copies the router-image file from the flash memory to the startup configuration:

```
Router# copy flash:router-image nvram:startup-config
```

Copying a Configuration File from one Flash Device to Another Example

The following example copies the file running-config from the first partition in internal flash memory to the flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

```
Router# copy flash: slot1:
System flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/images/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]
PCMCIA Slot1 flash directory:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'running-config' from flash: device
  as 'running-config' into slot1: device WITH erase? [yes/no] yes

Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!
 [OK - 850/4194304 bytes]
Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

Copying a File from a Remote Web Server Examples

In the following example, the file config1 is copied from a remote server to flash memory using HTTP:

```
Router# copy
http://
www.example.com:8080/configs/config1 flash:config1
```

In the following example, a default username and password for HTTP Client communications is configured, and then the file sample.scr is copied from a secure HTTP server using HTTPS:

```
Router# configure terminal

Router(config)# ip http client username joeuser
Router(config)# ip http client password letmein

Router(config)# end

Router# copy https://www.example_secure.com/scripts/sample.scr flash:
```

In the following example, an HTTP proxy server is specified before using the copy http:// command:

```
Router# configure terminal

Router(config)# ip http client proxy-server edge2 proxy-port 29

Router(config)# end

Router# copy
http://
www.example.com/configs/config3 flash:/configs/config3
```

Copying an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the router-image file from the flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

```
Router# copy slot1:router-image slaveslot0:
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
cd	Changes the default directory or file system.
copy xmodem: flash:	Copies any file from a source to a destination.
copy ymodem: flash:	Copies any file from a source to a destination.
delete	Deletes a file on a flash memory device.
dir	Displays a list of files on a file system.
erase	Erases a file system.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.
ip scp server enable	Enables scp server-side functionality.
reload	Reloads the operating system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show (flash file system)	Displays the layout and contents of a flash memory file system.
slave auto-sync config	Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.
verify bootflash:	File system or directory containing the files to list, followed by a colon.

define interface-range

To create an interface-range macro, use the **define interface-range** command in global configuration mode. To remove an interface-range macro, use the **no** form of this command.

define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface-range macro.
interface-range	Type of interface range. • For a list of valid values, see the "Usage Guidelines" section.

Command Default

Interface-range macro is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced.
12.2(17d)SXB	This command was integrated into Cisco IOS XE Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

- The **define interface-range** command applies a particular configuration on multiple interfaces and creates multiple logical, and sub interfaces.
- An interface range macro name can comprise up to 32 characters.
- An interface range for a macro can accept a maximum of five ranges. However, the subinterface range for a macro accepts only one range.
- An interface range cannot span slots.
- Use the *interface-type slot/first-interface last-interface* format to enter the interface range.
- Valid values for the *interface-type* argument are as follows:
  - **atm** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **ethernet**
  - **fastethernet**
  - **ge-wan** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **gigabitethernet**
  - **loopback**
  - **port-channel** *interface-number* —Valid values are from 1 to 256
  - **pos** —Supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2
  - **tengigabitethernet**
  - **tunnel**
  - **vlan** *vlan-id* —Valid values are from 1 to 4094

Examples

The following example shows how to create a multiple-interface macro:

```
Device(config)# define interface-range macro1 ethernet 1/2 - 5, fastethernet 5/5 - 10
```

The following example shows how to create multiple loopback interfaces:

```
Device(config)# define interface-range loopback1-10
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.

enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the **enable** command in either user EXEC, privileged EXEC, or diagnostic mode.

enable [**privilege-level**] [**view** [*view-name*]]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. **Note** This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Command Default

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
12.3(7)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **view** keyword and *view-name* argument were integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(22)SB.
Cisco IOS XE Release 2.1	This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.

Usage Guidelines

By default, using the **enable** command without the *privilege-level* argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOSSecurity Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the **enable** command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first
Password:
00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
Router# show ?
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
```

The following example shows how to use the **enable view** command to switch from the root view to the CLI view “first”:

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view
Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all
Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
```

```
Router# enable view first

Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view “first.”
Router# show parser view
Current view is 'first'
```

Related Commands

Command	Description
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.
privilege level (line)	Sets a privilege level for a command for a specific line.

erase

To erase a file system or all files available on a file system, use the **erase**command in privileged EXEC or diagnostic mode.

erase {**/all nvram:** | **/no-squeeze-reserve-space** *filesystem***:** | *filesystem*: | **startup-config**}

Cisco 7600 Series Routers and Cisco ASR 1000 Series Routers

erase {**/all nvram:** | *filesystem***:** | **startup-config**}

Syntax Description

/all	Erases all files in the specified file system.
nvram:	Erases all files in the NVRAM.
*file-system***:**	File system name, followed by a colon. For example, **flash:** or **nvram:**. **Note** This argument may not be used if the device memory contains logging persistent files.
/no-squeeze-reserve-space	Disables the squeeze operation to conserve memory and makes the **erase** command compatible with older file systems.
startup-config	Erases the contents of the configuration memory.

Command Modes

Privileged EXEC (#) Diagnostic (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(11)T	This command was modified. The **/no-squeeze-reserve-space**keyword was added.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was modified. The command was introduced in diagnostic mode on the Cisco ASR 1000 Series Routers, and the /**all** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The *file-system* **:** argument was added.

Usage Guidelines

The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

Caution When you use the **erase** command to erase a file system, you cannot recover the files in the file system.

The *word help* feature is disabled for the **erase** command. You must enter the complete command name to enable the command. The parser does not complete the command name if you enter partial syntax of the command and press the Tab key. For more information on the word help feature, refer to the Using the Cisco IOS Command-Line Interface feature guide.

The **erase**command can be used on Class B and Class C flash file systems only.

Class A flash file systems cannot be erased. You can delete individual files using the **delete** command and then reclaim the space using the **squeeze** command. You can use the **format**command to format the flash file system. The **format** command when used on ATA disk clears the File Allocation Table (FAT) and root directory entries only. The data is not erased.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in flash memory, the specified file will be marked “deleted.”

The **erase /all nvram:** command erases all files on NVRAM, including private NVRAM.

The **/no-squeeze-reserve-space** keyword is available on systems with small amounts of flash memory in order to conserve memory. When a squeeze operation is performed, the last two erase sectors are permanently reserved for the squeeze logs and squeeze buffer. The **/no-squeeze-reserve-space**keyword prevents the reservation of space that guarantees the ability to run the squeeze command. Disabling the squeeze operation keeps these memory sectors free. If any sectors using squeeze data are detected, they will be erased when the **/no-squeeze-reserve-space** keyword is used. The **/no-squeeze-reserve-space** keyword increases the available amount of usable flash space, but you may not be able to run the **squeeze** command.

This is typically fine if the file system (such as flash) is used to store a single, large file. For example, an IOS image.

On Class C flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinitialize a Class C flash file system.

Note Use the context-sensitive help to determine which file systems can be used for the **erase** command. The output will vary based on the platform.

Examples

The following example shows how to erase the NVRAM, including the startup configuration located there:

```
Router# erase nvram:
```

The following example shows how to erase all of partition 2 in internal flash memory:

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]
Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]:
yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

The following example shows how to erase flash memory when flash is partitioned, but no partition is specified in the command:

```
Router# erase flash:
System flash partition information:
Partition   Size     Used    Free    Bank-Size   State       Copy-Mode
    1       4096K    2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K    2048K   2048K   2048K       Read/Write  Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?** *number*) for directory display of a particular partition. The default is the first read/write partition.

```
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Erase flash device, partition 2? [confirm] <Return>
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).

Command	Description
delete	Deletes a file on a flash memory device.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Removes all deleted files from the flash file system and recovers the memory space used by deleted files.
undelete	Recovers a file marked “deleted” on a Class A or Class B flash file system.
write erase	The **write erase** command is replaced by the **erase nvram:**command. See the description of the **erase** command for more information

errdisable detect cause

To enable error-disable detection, use the **errdisable detect cause** command in global configuration mode. To disable error-disable detection, use the **no** form of this command.

errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **packet-buffer-error** | **pagp-flap** | **rootguard** | **udld**}

no errdisable detect cause {**all** | **bpduguard** | **dtp-flap** | **l2ptguard** | **link-flap** | **pagp-flap** | **rootguard** | **udld**}

Syntax Description

all	Specifies error-disable detection for all error-disable causes.
bpduguard	Specifies detection for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
dtp-flap	Specifies detection for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
l2ptguard	Specifies detection for the Layer 2 Protocol Tunneling guard error-disable cause.
link-flap	Specifies detection for the link flap error-disable cause.
packet-buffer-error	Causes the packet buffer error to error-disable the affected port.
pagp-flap	Specifies detection for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
rootguard	Specifies detection for the root-guard error-disable cause.

udld	Specifies detection for the Unidirectional Link Detection (UDLD) error-disable cause.

Command Default

Error-disable detection is enabled for all causes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. Support was added for the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. The **packet-buffer-error** keyword was added.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Entering the **no errdisable detect cause packet-buffer-error** command allows you to detect the fault that triggers a power cycle of the affected module.

A cause (bpduguard, dtp-flap, link-flap, pagp-flap, root-guard, udld) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similiar to the link-down state).

You must enter the **shutdown** and then the **no shutdown** commands to recover an interface manually from the error-disable state.

Examples

The following example shows how to enable error-disable detection for the Layer 2 protocol-tunnel guard error-disable cause:

```
Router(config)#
errdisable detect cause l2ptguard
```

Related Commands

Command	Description
show errdisable detect	Displays the error-disable detection status.
show interfaces status	Displays the interface status or a list of interfaces in an error-disable state on LAN ports only.
shutdown	Disables an interface.

errdisable recovery

To configure recovery mechanism variables, use the **errdisable recovery** command in global configuration mode. To return to the default state, use the **no** form of this command.

errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}

no errdisable recovery {**cause** {**all** | **arp-inspection** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **dtp-flap** | **gbic-invalid** | **l2ptguard** | **link-flap** | **pagp-flap** | **psecure-violation** | **security-violation** | **rootguard** | **udld** | **unicast-flood**} | **interval** *seconds*}

Syntax Description

cause	Enables error-disable recovery from a specific cause.
all	Enables the recovery timers for all error-disable causes.
arp-inspection	Enables error-disable recovery from an Address Resolution Protocol (ARP) inspection cause.
bpduguard	Enables the recovery timer for the Bridge Protocol Data Unit (BPDU)-guard error-disable cause.
channel-misconfig	Enables the recovery timer for the channel-misconfig error-disable cause.
dhcp-rate-limit	Enables the recovery timer for the Dynamic Host Configuration Protocol (DHCP)-rate-limit error-disable cause.
dtp-flap	Enables the recovery timer for the Dynamic Trunking Protocol (DTP)-flap error-disable cause.
gbic-invalid	Enables the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.
l2ptguard	Enables the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.

link-flap	Enables the recovery timer for the link-flap error-disable cause.
pagp-flap	Enables the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
psecure-violation	Enables the recovery timer for the psecure-violation error-disable cause.
security-violation	Enables the automatic recovery of ports that were disabled because of 802.1X security violations.
rootguard	Enables the recovery timer for the root-guard error-disable cause.
udld	Enables the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.
unicast-flood	Enables the recovery timer for the unicast-flood error-disable cause.
interval *seconds*	Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.

Command Default

The recovery mechanisms are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command was implemented on the Supervisor Engine 2.
12.2(18)SXD	This command was modified. The **arp-inspection** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A cause (bpduguard, channel-misconfig, dhcp-rate-limit, dtp-flap, l2ptguard, link-flap, pagp-flap, psecure-violation, security-violation, rootguard, udld, or unicast-flood) is defined as the reason why the error-disable state occurred. When a cause is detected on an interface, the interface is placed in an error-disable state (an operational state that is similar to the link-down state). If you do not enable error-disable recovery for the cause, the interface stays in the error-disable state until a shutdown and no shutdown occur. If you enable recovery for a cause, the interface is brought out of the error-disable state and allowed to retry operation once all the causes have timed out.

You must enter the **shutdown** command and then the **no shutdown** command to manually recover an interface from the error-disable state.

Note A separate line is required each time you want to enter the **errdisable recovery cause** command to add a new reason for recovery; each new reason does not get appended to the original single line. This means you must enter each new reason separately.

Examples

This example shows how to enable the recovery timer for the BPDU-guard error-disable cause:

```
Router(config)#
 errdisable recovery cause bpduguard
```

This example shows how to set the recovery timer to 300 seconds:

```
Router(config)#
 errdisable recovery interval 300
```

Related Commands

Command	Description
show errdisable recovery	Displays the information about the error-disable recovery timer.
show interfaces status	Displays the interface status or a list of interfaces in an error-disabled state on LAN ports only.
shutdown	Disables an interface.

file verify auto

To enable automatic image verification, use the **file verify auto** command in global configuration mode. To disable automatic image verification, use the **no** form of this command.

file verify auto

no file verify auto

Syntax Description

This command has no arguments or keywords.

Command Default

Image verification is not automatically applied to all images that are copied or reloaded onto a router.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support was added for the Supervisor Engine 2.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Image verification is accomplished by verifying the compressed Cisco IOS image checksum.

Image verification allows users to automatically verify the integrity of all Cisco IOS images. Thus, users can be sure that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The **file verify auto** command enables image verification globally; that is, all images that are to be copied (via the **copy** command) or reloaded (via the **reload** command) are automatically verified. Although both the **copy** and **reload** commands have a **/verify** keyword that enables image verification, you must issue the keyword each time you want to copy or reload an image. The **file verify auto** command enables image verification by default so you no longer have to specify image verification multiple times.

If you have enabled image verification by default but prefer to disable verification for a specific image copy or reload, the **/noverify** keyword along with either the **copy** or the **reload** command will override the **file verify auto** command.

Examples

The following example shows how to enable automatic image verification:

```
Router(config)# file verify auto
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
copy/noverify	Disables the automatic image verification for the current copy operation.
reload	Reloads the operating system.
verify	Verifies the checksum of a file on a Flash memory file system or computes an MD5 signature for a file.

hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Release	Modification
15.0(1)M4	This command was integrated into Cisco IOS Release 15.0(1)M4 and support for numeric hostnames added.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer* .

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```
Router(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names--Implementation and Specification* .

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Router,” you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.

The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **hostname**, results in incorrect translation:

```
Router(config)#
Router(config)#hostname \99
% Hostname contains one or more illegal characters.
```

Examples

The following example changes the hostname to “host1”:

```
Router(config)# hostname host1
host1(config)#
```

Related Commands

Command	Description
setup	Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

reload

To reload the operating system, use the **reload** command in privileged EXEC or diagnostic mode.

reload [**/verify** | **/noverify**] [[**warm file**] [**line** | **in** [*hhh*:*mm* | *mmm* [*text*]] | **at** *hh*:*mm* [*day month*] [*text*]] | **reason** [*reason-string*] | **cancel**]

Syntax Description

/verify	(Optional) Verifies the digital signature of the file that will be loaded onto the operating system.
/noverify	(Optional) Does not verify the digital signature of the file that will be loaded onto the operating system. **Note** This keyword is often issued if the **file verify auto** command is enabled, which automatically verifies the digital signature of all images that are copied.
warm	(Optional) Specifies warm rebooting.
file	(Optional) Specifies the image file for warm rebooting.
line	(Optional) Reason for reloading; the string can be from 1 to 255 characters long.
in *hhh* **:** *mm* | *mmm*	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
text	(Optional) Reason for reloading; the string can be from 1 to 255 characters long.

at *hh* **:** *mm*	(Optional) 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. The reload must take place within 24 days.
day	(Optional) Number of the day in the range from 1 to 31.
month	Month of the year.
reason *reason-string*	(Optional) Specifies a reason for reloading.
cancel	(Optional) Cancels a scheduled reload.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.3(2)T	This command was modified. The **warm** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The /**verify**and **/noverify** keywords were added.
12.2(20)S	This command was modified. Support was added for the Cisco 7304 router. The Cisco 7500 series router in not supported in Cisco IOS Release 12.2(20)S.
12.0(26)S	This command was modified. The /**verify**and **/ noverify** keywords were integrated into Cisco IOS Release 12.0(26)S.

Release	Modification
12.3(4)T	This command was modified. The /**verify**and / **noverify** keywords were integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(11)T	This command was modified. The **file** keyword and *url* argument were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **reason** keyword and *reason-string*argument were added.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Router and was made available in diagnostic mode.

Usage Guidelines

The **reload** command halts the system. If the system is set to restart on error, it reboots itself. Use the **reload** command after configuration information is entered into a file and saved to the startup configuration.

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This restriction prevents the system from using an image stored in the ROM monitor and taking the system out of the remote user's control.

If you modify your configuration file, the system prompts you to save the configuration. During a save operation, the system prompts whether you want to proceed with the save if the CONFIG_FILE variable points to a startup configuration file that no longer exists. If you respond "yes" in this situation, the system enters setup mode upon reload.

When you schedule a reload to occur at a later time (using the **in** keyword), it must take place within 24 days.

The **at** keyword can be used only if the system clock has been set on the router (either through Network Time Protocol [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, synchronize the time on each router with NTP.

When you specify the reload time using the **at** keyword, if you specify the month and day, the reload takes 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. The reload must take place within 24 days.

To display information about a scheduled reload, use the **show reload** command.

The /verify and /noverify Keywords

If the /**verify** keyword is specified, the integrity of the image will be verified before it is reloaded onto a router. If verification fails, the image reload will not occur. Image verification is important because it assures the user that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

The **/noverify** keyword overrides any global automatic image verification that may be enabled via the **file verify auto** command.

The warm Keyword

If you issue the **reload** command after you have configured the **warm-reboot** global configuration command, a cold reboot will occur. Thus, if you want to reload your system, but do not want to override the warm reboot functionality, you should specify the **warm** keyword with the **reload** command. The warm reboot functionality allows a Cisco IOS image to reload without ROM monitor intervention. That is, read-write data is saved in RAM during a cold startup and restored during a warm reboot. Warm rebooting allows the router to reboot quicker than conventional rebooting (where control is transferred to ROM monitor and back to the image) because nothing is copied from flash to RAM.

Examples

The following example shows how to immediately reload the software on the router:

```
Router# reload
```

The following example shows how to reload the software on the router in 10 minutes:

```
Router# reload in 10
Router# Reload scheduled for 11:57:08 PDT Fri Apr 21 1996 (in 10 minutes)
Proceed with reload? [confirm]
```

The following example shows how to reload the software on the router at 1:00 p.m. on that day:

```
Router# reload at 13:00
Router# Reload scheduled for 13:00:00 PDT Fri Apr 21 1996 (in 1 hour and 2 minutes)
Proceed with reload? [confirm]
```

The following example shows how to reload the software on the router on April 21 at 2:00 a.m.:

```
Router# reload at 02:00 apr 21
Router# Reload scheduled for 02:00:00 PDT Sat Apr 21 1996 (in 38 hours and 9 minutes)
Proceed with reload? [confirm]
```

The following example shows how to cancel a pending reload:

```
Router# reload cancel
%Reload cancelled.
```

The following example shows how to perform a warm reboot at 4:00 a.m. on that day:

Router# **reload warm at 04:00**

The following example shows how to specify a reason for the reload:

Router# **reload reason** *reloaded with updated version*

The following example shows how to specify image verification via the **/verify** keyword before reloading an image onto the router:

```
Router# reload /verify
Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
```

```
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-
mz ..................................................................
.....................................................Done!
Embedded Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash     MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
Proceed with reload? [confirm]n
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
file verify auto	Enables automatic image verification.
show reload	Displays the reload status on the router.
warm-reboot	Enables router reloading with reading images from storage.

remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

remote-span

no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

setup

To enter Setup mode, use the **setup** command in privileged EXEC mode.

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Setup mode gives you the option of configuring your system without using the Cisco IOS Command Line Interface (CLI). For some tasks, you may find it easier to use Setup than to enter Cisco IOS commands individually. For example, you might want to use Setup to add a protocol suite, to make major addressing scheme changes, or to configure a newly installed interface. Although you can use the CLI to make these changes, Setup provides you with a high-level view of the configuration and guides you through the configuration process.

If you are not familiar with Cisco products and the CLI, Setup is a particularly valuable tool because it prompts you for the specific information required to configure your system.

Note If you use the Setup mode to modify a configuration because you have added or modified the hardware, be sure to verify the physical connections using the **show version** EXEC command. Also, verify the logical port assignments using the **show running-config** EXEC command to ensure that you configure the correct port. Refer to the hardware documentation for your platform for more information on physical and logical port assignments.

Before using the Setup mode, you should have the following information so that you can configure the system properly:

- Which interfaces you want to configure
- Which routing protocols you wish to enable
- Whether the router is to perform bridging
- Network addresses for the protocols being configured
- Password strategy for your environment

When you enter the **setup** EXEC command after first-time startup, an interactive dialog called the *System Configuration Dialog* appears on the system console screen. The System Configuration Dialog guides you through the configuration process. It prompts you first for global parameters and then for interface parameters. The values shown in brackets next to each prompt reflect either the default settings or the last configured setting.

The prompts and the order in which they appear on the screen vary depending on the platform and the interfaces installed in the device.

You must progress through the System Configuration Dialog until you come to the item that you intend to change. To accept default settings for items that you do not want to change, press the **Return** or **Enter** key. The default choice is indicated by square brackets (for example, [yes]) before the prompt colon (:).

To exit Setup mode and return to privileged EXEC mode without making changes and without progressing through the entire System Configuration Dialog, press **Ctrl-C**

The facility also provides help text for each prompt. To access help text, press the question mark (**?**) key at a prompt.

When you complete your changes, the system will automatically display the configuration file that was created during the Setup session. It also asks you if you want to use this configuration. If you answerYes, the configuration is saved to NVRAM as the startup configuration file. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

Examples

The following example displays the **setup** command facility to configure serial interface 0 and to add ARAP and IP/IPX PPP support on the asynchronous interfaces:

```
Router# setup
         --- System Configuration Dialog
 ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to
abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes]:
First, would you like to see the current
interface summary? [yes]:
Interface          IP-Address      OK?  Method    Status                Protocol
Ethernet0          172.16.72.2     YES  manual    up                    up
```

```
Serial0            unassigned      YES  not set   administratively down  down
Serial1            172.16.72.2     YES  not set   up                     up
Configuring global parameters:
  Enter host name [Router]:
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
  Enter enable secret [<Use current secret>]:


The enable password is used when there is no enable secret
and when using older software and some boot images.


  Enter enable password [ww]:
  Enter virtual terminal password [ww]:
  Configure SNMP Network Management? [yes]:
    Community string [public]:
  Configure DECnet? [no]:
  Configure AppleTalk? [yes]:
    Multizone networks? [no]: yes
  Configure IPX? [yes]:
  Configure IP? [yes]:
    Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [15]:
  Configure Async lines? [yes]:
    Async line speed [9600]: 57600
    Configure for HW flow control? [yes]:
    Configure for modems? [yes/no]: yes
      Configure for default chat script? [yes]: no
    Configure for Dial-in IP SLIP/PPP access? [no]: yes
      Configure for Dynamic IP addresses? [yes]: no

      Configure Default IP addresses? [no]: yes
      Configure for TCP Header Compression? [yes]: no
      Configure for routing updates on async links? [no]:
    Configure for Async IPX? [yes]:
    Configure for Appletalk Remote Access? [yes]:
      AppleTalk Network for ARAP clients [1]: 20
      Zone name for ARAP clients [ARA Dialins]:
Configuring interface parameters:
Configuring interface Ethernet0:
  Is this interface in use? [yes]:
  Configure IP on this interface? [yes]:
    IP address for this interface [172.16.72.2]:
    Number of bits in subnet field [8]:
    Class B network is 172.16.0.0, 8 subnet bits; mask is /24
  Configure AppleTalk on this interface? [yes]:
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [1]:
    AppleTalk ending cable range [1]:
    AppleTalk zone name [Sales]:
    AppleTalk additional zone name:
  Configure IPX on this interface? [yes]:
    IPX network number [1]:
Configuring interface Serial0:
  Is this interface in use? [no]: yes
  Configure IP on this interface? [no]: yes
  Configure IP unnumbered on this interface? [no]: yes
    Assign to which interface [Ethernet0]:
  Configure AppleTalk on this interface? [no]: yes
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]: 3
    AppleTalk ending cable range [3]: 3
    AppleTalk zone name [myzone]: ZZ Serial
    AppleTalk additional zone name:
  Configure IPX on this interface? [no]: yes
    IPX network number [2]: 3
Configuring interface Serial1:
  Is this interface in use? [yes]:
  Configure IP on this interface? [yes]:
  Configure IP unnumbered on this interface? [yes]:
    Assign to which interface [Ethernet0]:
  Configure AppleTalk on this interface? [yes]:
```

```
    Extended AppleTalk network? [yes]:
    AppleTalk starting cable range [2]:
    AppleTalk ending cable range [2]:
    AppleTalk zone name [ZZ Serial]:
    AppleTalk additional zone name:
  Configure IPX on this interface? [yes]:
    IPX network number [2]:
Configuring interface Async1:
    IPX network number [4]:
    Default client IP address for this interface [none]: 172.16.72.4
Configuring interface Async2:
    IPX network number [5]:
    Default client IP address for this interface [172.16.72.5]:
Configuring interface Async3:
    IPX network number [6]:
    Default client IP address for this interface [172.16.72.6]:
Configuring interface Async4:
    IPX network number [7]:
    Default client IP address for this interface [172.16.72.7]:
Configuring interface Async5:
    IPX network number [8]:
    Default client IP address for this interface [172.16.72.8]:
Configuring interface Async6:
    IPX network number [9]:
    Default client IP address for this interface [172.16.72.9]:
Configuring interface Async7:
    IPX network number [A]:
    Default client IP address for this interface [172.16.72.10]:
Configuring interface Async8:
    IPX network number [B]:
    Default client IP address for this interface [172.16.72.11]:
Configuring interface Async9:
    IPX network number [C]:
    Default client IP address for this interface [172.16.72.12]:
Configuring interface Async10:
    IPX network number [D]:
    Default client IP address for this interface [172.16.72.13]:
Configuring interface Async11:
    IPX network number [E]:
    Default client IP address for this interface [172.16.72.14]:
Configuring interface Async12:
    IPX network number [F]:
    Default client IP address for this interface [172.16.72.15]:
Configuring interface Async13:
    IPX network number [10]:
    Default client IP address for this interface [172.16.72.16]:
Configuring interface Async14:
    IPX network number [11]:
    Default client IP address for this interface [172.16.72.17]:
Configuring interface Async15:
    IPX network number [12]:
    Default client IP address for this interface [172.16.72.18]:
Configuring interface Async16:
    IPX network number [13]:
    Default client IP address for this interface [172.16.72.19]:
The following configuration command script was created:
hostname Router
enable secret 5 $1$krIg$emfYm/1OwHVspDuS8Gy0K1
enable password ww
line vty 0 4
password ww
snmp-server community public
!
no decnet routing
appletalk routing
ipx routing
ip routing
!
line 1 16
speed 57600
flowcontrol hardware
modem inout
!
```

```
arap network 20 ARA Dialins
line 1 16
arap enable
autoselect
!
! Turn off IPX to prevent network conflicts.
interface Ethernet0
no ipx network
interface Serial0
no ipx network
interface Serial1
no ipx network
!
interface Ethernet0
ip address 172.16.72.2 255.255.255.0
appletalk cable-range 1-1 1.204
appletalk zone Sales
ipx network 1
no mop enabled
!
interface Serial0
no shutdown
no ip address
ip unnumbered Ethernet0
appletalk cable-range 3-3
appletalk zone ZZ Serial
ipx network 3
no mop enabled
!
interface Serial1
no ip address
ip unnumbered Ethernet0
appletalk cable-range 2-2 2.2
appletalk zone ZZ Serial
ipx network 2
no mop enabled
!
Interface Async1
ipx network 4
ip unnumbered Ethernet0
peer default ip address 172.16.72.4
async mode interactive
!
Interface Async2
ipx network 5
ip unnumbered Ethernet0
peer default ip address 172.16.72.5
async mode interactive
!
Interface Async3
ipx network 6
ip unnumbered Ethernet0
peer default ip address 172.16.72.6
async mode interactive
!
Interface Async4
ipx network 7
ip unnumbered Ethernet0
peer default ip address 172.16.72.7
async mode interactive
async dynamic address
!
Interface Async5
ipx network 8
ip unnumbered Ethernet0
peer default ip address 172.16.72.8
async mode interactive
!
Interface Async6
ipx network 9
ip unnumbered Ethernet0
peer default ip address 172.16.72.9
async mode interactive
```

```
!
Interface Async7
ipx network A
ip unnumbered Ethernet0
peer default ip address 172.16.72.10
async mode interactive
!
Interface Async8
ipx network B
ip unnumbered Ethernet0
peer default ip address 172.16.72.11
async mode interactive
!
Interface Async9
ipx network C
ip unnumbered Ethernet0
peer default ip address 172.16.72.12
async mode interactive
!
Interface Async10
ipx network D
ip unnumbered Ethernet0
peer default ip address 172.16.72.13
async mode interactive
!
Interface Async11
ipx network E
ip unnumbered Ethernet0
peer default ip address 172.16.72.14
async mode interactive
!
Interface Async12
ipx network F
ip unnumbered Ethernet0
peer default ip address 172.16.72.15
async mode interactive
!
Interface Async13
ipx network 10
ip unnumbered Ethernet0
peer default ip address 172.16.72.16
async mode interactive
!
Interface Async14
ipx network 11
ip unnumbered Ethernet0
peer default ip address 172.16.72.17
async mode interactive
!
Interface Async15
ipx network 12
ip unnumbered Ethernet0
peer default ip address 172.16.72.18
async mode interactive
!
Interface Async16
ipx network 13
ip unnumbered Ethernet0
peer default ip address 172.16.72.19
async mode interactive
!
router igrp 15
network 172.16.0.0
!
end
Use this configuration? [yes/no]: yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.


Router#
```

Related Commands

Command	Description
erase nvram:	Erases a file system.
show running-config	Displays the running configuration file. Command alias for the **more system:running-config** command.
show startup-config	Displays the startup configuration file. Command alias for the **more system:startup-config**command.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.