

System Image and Configuration File Load Commands

This chapter provides detailed descriptions of the commands used to load and copy system images and configuration files. System images contain the system software. Configuration files contain commands entered to customize the functions of the access server.

For access server configuration information and examples, refer to the “Loading System Images and Configuration Files” chapter in the *Access and Communication Servers Configuration Guide*.

Note Commands in this chapter that have been replaced by new commands continue to perform their normal functions in the current release but are not longer documented. Support for these commands will cease in a future release.

Table 3-1 Mapping Old Commands to New Commands

Old Command	New Command
configure network	copy rcv running-config (for an rcv server) copy tftp running-config (for a TFTP server)
configure overwrite-network	copy rcv startup-config (for an rcv server) copy tftp startup-config (for a TFTP server)
copy erase flash	erase flash
copy verify or copy verify flash	verify flash
copy verify bootflash	verify bootflash
show configuration	show startup-config
tftp-server system	tftp-server
write erase	erase startup-config
write memory	copy running-config startup-config
write network	copy running-config rcv (for an rcv server) copy running-config tftp (for a TFTP server)
write terminal	show running-config

For access server configuration information and examples, refer to the “Loading System Images, Microcode Images, and Configuration Files” chapter in the *Access and Communication Servers Configuration Guide*.

async-bootp

Use the **async-bootp** command to enable support for extended BOOTP requests as defined in RFC 1084 when the access server is configured for SLIP. Use the **no** form of this command to restore the default.

```
async-bootp tag [:hostname] data
no async-bootp
```

Syntax Description

<i>tag</i>	Item being requested; expressed as filename, integer, or IP dotted-decimal address. See Table 3-2 for possible values.
<i>:hostname</i>	(Optional) This entry applies only to the host specified. The argument <i>:hostname</i> accepts both an IP address and a logical host name.
<i>data</i>	List of IP addresses entered in dotted-decimal notation or as logical host names, a number, or a quoted string.

Table 3-2 Async-BOOTP Tag Keywords

Keyword	Description
bootfile	Specifies use of a server boot file from which to download the boot program. Use the optional <i>:hostname</i> and <i>data</i> arguments to specify the filename.
subnet-mask <i>mask</i>	Dotted-decimal address specifying the network and local subnetwork mask (as defined by RFC 950).
time-offset <i>offset</i>	Signed 32-bit integer specifying the time offset of the local subnetwork in seconds from Universal Coordinated Time (UTC).
gateway <i>address</i>	Dotted-decimal address specifying the IP addresses of gateways for this subnetwork. A preferred gateway should be listed first.
time-server <i>address</i>	Dotted-decimal address specifying the IP address of time servers (as defined by RFC 868).
ien116-server <i>address</i>	Dotted-decimal address specifying the IP address of name servers (as defined by IEN 116).
dns-server <i>address</i>	Dotted-decimal address specifying the IP address of the Domain Name Server (DNS) (as defined by RFC 1034).
log-server <i>address</i>	Dotted-decimal address specifying the IP address of an MIT-LCS UDP log server.
quote-server <i>address</i>	Dotted-decimal address specifying the IP address of Quote of the Day servers (as defined in RFC 865).
lpr-server <i>address</i>	Dotted-decimal address specifying the IP address of Berkeley UNIX Version 4 BSD servers.
impress-server <i>address</i>	Dotted-decimal address specifying the IP address of Impress network image servers.
rlp-server <i>address</i>	Dotted-decimal address specifying the IP address of Resource Location Protocol (RLP) servers (as defined in RFC 887).

Keyword	Description
hostname <i>name</i>	The name of the client, which might or might not be domain qualified, depending upon the site.
bootfile-size <i>value</i>	A two-octet value specifying the number of 512-octet (byte) blocks in the default boot file.

Default

If no extended BOOTP commands are entered, the access server software generates a gateway and subnet mask appropriate for the local network.

Command Mode

Global configuration

Usage Guidelines

Use the EXEC command **show async bootp** to list the configured parameters. Use the **no async-bootp** command to clear the list.

Examples

The following example illustrates how to specify different boot files: one for a PC, and one for a Macintosh. With this configuration, a BOOTP request from the host on 172.30.1.1 results in a reply listing the boot filename as *pcboot*. A BOOTP request from the host named *mac* results in a reply listing the boot filename as *macboot*.

```
async-bootp bootfile :172.30.1.1 "pcboot"
async-bootp bootfile :mac "macboot"
```

The following example specifies a subnet mask of 255.255.0.0:

```
async-bootp subnet-mask 255.255.0.0
```

The following example specifies a negative time offset of the local subnetwork of -3600 seconds:

```
async-bootp time-offset -3600
```

The following example specifies the IP address of a time server:

```
async-bootp time-server 172.30.1.4
```

Related Command

show async bootp

b

To boot the access server manually, use the **b** ROM monitor command.

```
b  
b filename [ip-address]  
b flash [filename]  
b flash [device:][partition-number:][filename]
```

Syntax Description

<i>filename</i>	Name of the system image from which you want to netboot. The filename is case sensitive.
<i>ip-address</i>	(Optional) IP address of the network server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
flash <i>filename</i>	(Optional) Boots the access server from Flash memory with the optional filename of the image you want loaded. The filename is case sensitive. Without a filename, the first valid file in Flash memory will be loaded.
<i>device:</i>	(Optional) Valid value is flash . The colon (:) is required.
<i>partition-number:</i>	(Optional) Boots the access server from Flash memory with the optional filename of the image you want loaded from the specified Flash partition. If you do not specify a filename, the first valid file in the specified partition of Flash memory is loaded.
<i>filename</i>	(Optional) Boots the access server from Flash memory with the filename of the image you want loaded from the specified Flash partition, if a partition is specified. If a partition is not specified, the system boots with the filename from the first partition. The filename is case sensitive. If you do not specify a filename, the first valid file in the specified partition of Flash memory is loaded.

Default

If you enter the **b** command and press Return, the access server boots from ROM by default.

If you enter the **b flash** command without specifying a filename, the first valid file in Flash memory is loaded.

For other defaults, see the preceding Syntax Description section.

Command Mode

ROM monitor

boot bootstrap

To configure the filename that is used to boot a secondary bootstrap image, use the **boot bootstrap** global configuration command. Use the **no** form of the command to disable booting from a secondary bootstrap image.

```
boot bootstrap flash [filename]  
no boot bootstrap flash [filename]
```

```
boot bootstrap mop filename [mac-address] [interface]  
no boot bootstrap mop filename [mac-address] [interface]
```

```
boot bootstrap [tftp] filename [ip-address]  
no boot bootstrap [tftp] filename [ip-address]
```

Syntax Description

flash	Indicates that the access server will be booted from Flash memory.
mop	Indicates that the access server will be netbooted from a system image stored on a Digital MOP server.
tftp	(Optional) Indicates that the access server will be netbooted from a system image stored on a TFTP server.
<i>filename</i>	(Optional with flash) Name of the system image from which you want to netboot. If you omit the filename when booting from Flash, the access server uses the first system image stored in Flash memory.
<i>ip-address</i>	(Optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
<i>mac-address</i>	(Optional) MAC address of the MOP server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first MOP server to indicate that it has the file will be the server from which the access server gets the boot image.
<i>interface</i>	(Optional) Interface out which the access server should send MOP requests to reach the MOP server. The interface options are async , dialer , Ethernet , loopback , null , serial , and tunnel . If the <i>interface</i> argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface from which the first response is received will be used to load the software.

Default

No secondary bootstrap

Command Mode

Global configuration

Usage Guidelines

The **boot bootstrap** command, in conjunction with setting bit 9 on the configuration register of a access server, causes the access server to load a secondary bootstrap image over the network. The secondary bootstrap image then loads the specified system image file. The name of the secondary bootstrap file is *boot-csc3* or *boot-csc4*, depending on the access server model. See the appropriate hardware installation guide for details on the configuration register and secondary bootstrap filename.

Use this command when you have attempted to load a system image but have run out of memory even after compressing the system image. Secondary bootstrap allows you to load a larger system image through a smaller secondary image.

Example

In the following example, the system image file *sysimage-2* will be loaded by using a secondary bootstrap image:

```
boot bootstrap sysimage-2
```

boot buffersize

To modify the buffer size used to load configuration files, use the **boot buffersize** global configuration command. Use the **no** form of the command to return to the default setting.

boot buffersize *bytes*
no boot buffersize

Syntax Description

bytes Specifies the size of the buffer to be used. There is no minimum or maximum size that can be specified.

Default

Buffer size of the nonvolatile memory

Command Mode

Global configuration

Usage Guidelines

Normally, the access server uses a buffer the size of the system nonvolatile memory to hold configuration commands read from the network. You can increase this size if you have a very complex configuration. There is no minimum or maximum size that can be specified.

Example

The following example sets the buffer size to 64000:

```
boot buffersize 64000
```

boot host

To change the default name of the host configuration filename from which you want to load configuration commands, use the **boot host** global configuration command. Use the **no** form of the command to restore the host configuration filename to the default.

```
boot host mop filename [mac-address] [interface]
no boot host mop filename [mac-address] [interface]
```

```
boot host [tftp | rcp] filename [ip-address]
no boot host [tftp | rcp] filename [ip-address]
```

Syntax Description

mop	Indicates that the access server will be configured from a configuration file stored on a Digital MOP server.
tftp	(Optional) Indicates that the access server will be configured from a configuration file stored on a TFTP server.
rcp	(Optional) Indicates that the access server will be configured from a configuration file stored on an rcp server.
<i>filename</i>	Name of the file from which you want to load configuration commands.
<i>ip-address</i>	(Optional) IP address of the TFTP server on which the file resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
<i>mac-address</i>	(Optional) MAC address of the MOP server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first MOP server to indicate that it has the file will be the server from which the access server gets the boot image.
<i>interface</i>	(Optional) Interface out which the access server should send MOP requests to reach the MOP server. The interface options are async , dialer , ethernet , serial , and tunnel . If the <i>interface</i> argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface from which the first response is received will be used to load the software.

Default

The access server uses its host name to form a host configuration filename. To form this name, the access server converts its name to all lowercase letters, removes all domain information, and appends *-config*.

Command Mode

Global configuration

Usage Guidelines

Use the **service config** command to enable the loading of the specified configuration file at reboot time. Without this command, the access server ignores the **boot host** command and uses the configuration information in nonvolatile memory. If the configuration information in nonvolatile memory is invalid or missing, the **service config** command is enabled automatically.

The network server will attempt to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. The second is the host configuration file containing commands that apply to one network server in particular.

Example

The following example sets the host filename to *wilma-config* at address 172.30.7.19:

```
boot host /usr/local/tftpdire/wilma-config 172.30.7.19
```

Related Commands

boot network

service config

boot network

To change the default name of the network configuration file from which you want to load configuration commands, use the **boot network** global configuration command. Use the **no** form of this command to restore the network configuration filename to the default.

```
boot network mop filename [mac-address] [interface]
no boot network mop filename [mac-address] [interface]
```

```
boot network [tftp | rcp] filename [ip-address]
no boot network [tftp | rcp] filename [ip-address]
```

Syntax Description

mop	Configures the access server to download the configuration file from a network server using the Digital MOP protocol.
<i>filename</i>	Name of the file from which you want to load configuration commands. The default filename is <i>network-config</i> .
<i>mac-address</i>	(Optional) If MOP is specified, the MAC address of the network server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first server to indicate that it has the file will be the server from which the access server gets the boot image.
<i>interface</i>	(Optional) If MOP is specified, the interface out which the access server should send MOP requests to reach the server. The interface options are async , dialer , ethernet , serial , and tunnel . If the <i>interface</i> argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface from which the first response is received will be used to load the software.
rcp	(Optional) Configures the access server to download the configuration file from a network server using rcp. If omitted, defaults to tftp .
tftp	(Optional) Configures the access server to download the configuration file from a network server using tftp. If omitted and rcp is not specified, defaults to tftp .
<i>ip-address</i>	(Optional) If rcp or tftp is specified, the IP address of the network server on which the compressed image file resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

Default

The default filename is *network-config*. The default transfer protocol type is **tftp**, if neither **tftp** nor **rcp** is specified.

Command Mode

Global configuration

Usage Guidelines

When booting from a network server, access servers ignore routing information and static IP routes information. As a result, intermediate access servers are responsible for handling rcp or tftp requests correctly. Before booting from a network server, verify that a server is available by using the **ping** command.

Use the **service config** command to enable the loading of the specified configuration file at reboot time. Without this command, the access server ignores the **boot network** command and uses the configuration information in nonvolatile memory. If the configuration information in nonvolatile memory is invalid or missing, the **service config** command is enabled automatically.

The network server attempts to load two configuration files from remote hosts. The first is the network configuration file containing commands that apply to all network servers on a network. Use the **boot network** command to identify the network configuration file.

The rcp protocol requires that a client send the remote username on each rcp request to the network server. When the **boot network rcp** command is executed, the access server software sends the host name as the both the remote and local usernames. The rcp protocol implementation searches for the configuration files to be used relative to the account directory of the remote username on the network server.

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



Caution For rcp, if you do not explicitly specify a remote username by issuing the **ip rcmd remote-username** command and the access server host name is used, an account for the access server host name must be defined on the destination server. If the network administrator of the destination server did not establish an account for the access server host name, this command will not execute successfully.

If you copy the system image to a personal computer used as a file server, the remote host computer must support the remote shell protocol.

Examples

The following example changes the network configuration filename to *bridge_9.1* and uses the default broadcast address:

```
boot network bridge_9.1
service config
```

The following example changes the network configuration filename to *bridge_9.1*, specifies that rcp is to be used as the transport mechanism, and gives 172.30.1.111 as the IP address of the server on which the network configuration file resides.

```
boot network RCP bridge_9.1 172.30.1.111
service config
```

Related Commands

boot host
ip rcmd remote-username
service config

boot system

To change the filename of the system image that is loaded onto the access server when it reboots, use the **boot system** global configuration command. Use the **no boot system** command to remove the name.

```
boot system flash [device:][partition-number:][filename]  
no boot system flash [filename]
```

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

```
boot system rom  
no boot system rom
```

```
boot system [tftp | rcp] filename [ip-address]  
no boot system [tftp | rcp] filename [ip-address]
```

```
boot system flash [device:][partition-number:][filename]
```

```
no boot system
```

Syntax Description

flash	Indicates that the access server will be booted from Flash memory.
mop	Indicates that the access server will be netbooted from a system image stored on a Digital MOP server.
rom	Indicates that the access server will be booted from ROM.
rcp	(Optional) Indicates that the access server will be netbooted from a system image acquired from a network server using rcp. If omitted, the system defaults to tftp .
tftp	(Optional) Indicates that the access server will be booted from a system image stored on a network server using tftp. If omitted and rcp is not specified, the system defaults to tftp .
<i>filename</i>	(Optional with flash) Name of the system image file from which you want to netboot. It is case sensitive.
<i>ip-address</i>	(Optional) IP address of the network server on which the image file resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
<i>mac-address</i>	(Optional) If MOP is used, the MAC address of the server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first server to indicate that it has the file will be the server from which the access server gets the boot image.

<i>interface</i>	(Optional) Interface out which the access server should send MOP requests to reach the MOP server. The interface options are async , dialer , ethernet , serial , and tunnel . If the <i>interface</i> argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface from which the first response is received will be used to load the software.
<i>device:</i>	(Optional) Valid value is flash .
<i>partition-number:</i>	(Optional) Boots the access server from Flash memory with the optional filename of the image you want loaded from the specified Flash partition. If you do not specify a filename, the first valid file in the specified partition of Flash memory is loaded.
<i>filename</i>	(Optional) Boots the access server from Flash memory with the filename of the image you want loaded from the specified Flash partition. The filename is case sensitive. If you do not specify a filename, the first valid file in the specified partition of Flash memory will be loaded.

Default

If you do not specify a system image file with the **boot system** command, the access server uses the configuration register settings to determine the default system image filename for netbooting. The access server forms the default boot filename by starting with the word *cisco* and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen, and the processor-type name (*cisconn-cpu*). See the appropriate hardware installation guide for details on the configuration register and default filename. See also the command **config-register**. See also the Syntax Description section preceding this section.

If neither **tftp** or **rcp** is specified, the default transfer protocol type is **tftp**.

Command Mode

Global configuration

Usage Guidelines

In order for this command to work, the **config-register** command must be set properly.

Enter several **boot system** commands to provide a fail-safe method for booting your access server. Use the **boot system rom** command to specify use of the ROM system image as a backup to other **boot** commands in the configuration. The **boot system** commands are stored and executed on the order in which they are entered. If you enter multiple boot commands of the same type—for example, if you enter two commands that instruct the access server to boot from different network servers—then the access server tries them in the order they are entered.

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 The **no boot system** global configuration command disables all **boot system** configuration commands regardless of argument and keyword. Specifying the **flash** keyword or the *filename* argument with the **no boot system** command disables only the command specified by these arguments.

You can netboot from a compressed image. When a server netboots software, the image being booted and the running image must both fit into memory. Use compressed images to ensure that there is enough available memory to boot the access server. You can produce a compressed 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.)

The rcp protocol requires that a client send the remote username on an rcp request to a server. When the **boot system rcp** command is executed, by default the access server software sends the host name as the both the remote and local usernames. The rcp software searches for the system image to be booted from the remote server relative to the directory of the remote username, if the server has a directory structure, for example, as do UNIX systems.

Examples

The following example shows a list specifying two possible internetwork locations for a system image, with the ROM software being used as a backup. When the system image is booted from either of the internetwork locations, TFTP is used as the transport mechanism:

```
boot system cs3-rx.90-1 172.30.7.24
boot system cs3-rx.83-2 172.30.7.19
boot system rom
```

The following example boots the system boot relocatable image file *igs-bpx-1* from partition 2 of the Flash device.

```
boot system flash flash:2:igs-bpx-1
```

Related Commands

config-register
copy flash
copy rcp
copy tftp
ip rcmd remote-username

configure

To enter global configuration mode, use the **configure** privileged EXEC command.

```
configure { terminal | memory | network }
```

Syntax Description

- terminal** Executes configuration commands from the terminal.
- memory** Executes the configuration commands stored in nonvolatile memory.
- network** The **copy [rcp] tftp running-config** command replaces the **configure network** command. Use the appropriate keyword (**tftp** or **rcp**) for your application. Refer to the **copy rcp** or **copy tftp** command for more information.

Default

None

Command Mode

Privileged EXEC

Usage Guidelines

If you do not specify **terminal** or **memory** the access server prompts you for the source of configuration commands. After you enter the **configure** command, the system prompt changes from `Router-name#` to `Router-name(config)#`, indicating that you are in global configuration mode. To leave global configuration mode and return to the privileged EXEC prompt, press **Ctrl-Z**. If you specify **memory**, the access server executes the commands located in NVRAM.

Example

In the following example, the access server is configured from the terminal:

```
Router# configure

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
```

Related Commands

```
configure overwrite
copy running-config
show configuration
show running-config
```

configure overwrite

The **copy rcp startup-config** or **copy tftp startup-config** command replaces the **configure overwrite** command. If you use rcp, see the **copy rcp** command for more information. If you use TFTP, see the **copy tftp** command for more information.

config-register

To change the access server configuration register settings, use the **config-register** global configuration command.

config-register *value*

Syntax Description

value Hexadecimal or decimal value that represents the 16-bit configuration register value you want to use the next time the access server is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal).

Default

For the access server models without Flash memory, the default is 0x101, which causes the access server to boot from ROM and the Break key to be ignored. For access server models with Flash memory, the default is 0x10F, which causes the access server to boot from Flash memory and the Break key to be ignored.

Command Mode

Global configuration

Usage Guidelines

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the access server boots manually, from ROM, or from Flash or the network. Bit 8 controls the console Break key; when set to 1, it causes the Break key to be ignored. The remaining bits control other features of the access server and are typically set to 0.

To change the boot field value and leave all other bits set to their default values, follow these guidelines:

- If you set the configuration register value to 0x100, you must boot the operating system manually with the **b** command.
- If you set the configuration register value to 0x101, the access server boots using the default ROM software.
- If you set the configuration register to any value from 0x102 to 0x10F, the access server uses the boot field value to form a default boot filename for netbooting.

For more information about the configuration register bit settings and default filenames, see the appropriate access server hardware installation guide.

Example

In the following example, the configuration register is set to boot the system image from Flash memory:

```
config-register 0x010F
```

Related Commands

boot system

o

show version

continue

To return to the EXEC mode from ROM monitor mode, use the **continue** ROM monitor command.

continue

Syntax Description

This command has no arguments or keywords.

Command Mode

ROM monitor

Usage Guidelines

Use this command when you are in ROM monitor mode, and you want to return to EXEC mode to use the system image instead of reloading. The angle bracket (>) indicates that you are in ROM monitor mode. You are in ROM monitor mode when you manually load a system image or perform diagnostic tests. Otherwise, you will most likely never be in this mode.



Caution While in ROM monitor mode, the Cisco IOS system software is suspended until you issue either a reset or the **continue** command.

Example

In the following example, the **continue** command takes you from ROM monitor to EXEC mode:

```
> continue  
Router#
```

copy flash

To copy a file from Flash memory to another destination, use one of the following **copy flash** EXEC commands:

```
copy flash {rcp | tftp}
```

Syntax Description

rcp	Specifies a copy operation to a network server using rcp.
tftp	Specifies a TFTP server as the destination of the copy operation.

Command Mode

EXEC

Usage Guidelines

To copy a system image from Flash memory to a network server that is using rcp, use the **copy flash rcp** EXEC command. To copy a system image from Flash memory to a network server that is using TFTP, use the **copy flash tftp** command.

You can use the copy of the system image as a backup copy. You can also use it to verify that the copy in Flash memory is the same as in the original file on disk.

The rcp protocol requires that a client send the remote username on each rcp request to the server. When you issue the **copy flash rcp** command, by default the access server software sends the remote username associated with the current TTY process, if that name is valid. For example, if the user is connected to the access server through Telnet and the user was authenticated through the **username** command, then the Cisco IOS software sends that username as the remote username.

If the TTY username is invalid, the Cisco IOS software uses the access server host name as the both the remote and local usernames.

Note For Cisco, TTYs are commonly used in communications servers. The concept of TTYs originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called TTY devices (which stands for teletype, the original UNIX terminal).

To specify that a different remote username be sent to the server, use the **ip rcmd remote-username** command. **rcp** copies the system image to the remote server relative to the directory of the remote username, if that server has a directory structure (for example, UNIX systems).



Caution The remote username must be associated with an account on the destination server. If you do not use the **ip rcmd remote-username** command to specify the name of a remote user associated with an account on the server, then the remote username associated with the current TTY process must be associated with an account on the server. If there is no username for the current TTY process, then the access server host name must be associated with an account on the server. If the network administrator of the destination server did not establish accounts for the remote username that is used, and if a default remote username is used, this command will not execute successfully.

copy mop flash

To copy a system image using MOP into Flash memory, use the **copy mop flash** EXEC command.

copy mop flash

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

The access server prompts for the MOP filename. It provides an option to erase existing Flash memory before writing onto it. The entire copying process takes several minutes and will differ from network to network.

Before booting from Flash memory, verify that the checksum of the image in Flash memory matches the checksum listed in the README file that was distributed with the system software image. The checksum of the image in Flash memory is displayed at the bottom of the screen when you issue the **copy mop flash** command.



Caution If the checksum value is not correct according to the value in the README file, do not reboot the access server. Issue the **copy mop flash** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original system software image back into Flash memory *before* you reboot the access server from Flash memory. If you have a bad image in Flash memory and try to boot from Flash, and netbooting is not configured, the access server will start the system image contained in ROM. If ROM does not contain a fully functional system image, the access server might not function and will have to be reconfigured through a direct console port connection.

Examples

The following example shows sample output of when copying a system image into a partition of Flash memory:

```
Router# copy mop flash
System flash directory:
File Length Name/status
  1  984   junk [deleted]
  2  984   junk
[2096 bytes used, 8386512 available, 8388608 total]
Source file name? junk
Destination file name [junk]?

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'junk' from server
  as 'junk' into Flash WITH erase? [yes/no]yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading junk from 1234.5678.9abc via Ethernet0: !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
```

```
Flash copy took 0:00:01 [hh:mm:ss]
```

The following example shows sample output of copying a system image into a partition of Flash memory. The system will prompt 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, ? for directory display of all partitions, or ?*number* for directory display of a particular partition. The default is the first read/write partition.

```
Router# copy mop 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]
```

If the partition is read-only and has dual Flash bank support in boot ROMs, the session continues as follows:

```
**** 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]
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```
Loading master/igs-bfpx.100-4.3 from 172.30.1.111: !
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from MOP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

If the partition is read-write, the session continues as follows:

```
System flash directory, partition 2:
File Length Name/status
  1  3459720 master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Source file name? master/igs-bfpx.100-4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```
Loading master/igs-bfpx.100-4.3 from 172.30.1.111: !
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from MOP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

Related Commands

boot system

copy verify

copy rcp

To copy a system image from a network server into Flash memory using rcp, use the **copy rcp** EXEC commands. The **copy rcp running-config** command replaces the **configure network** command. The **copy rcp startup-config** command replaces the **configure overwrite-network** command.

```
copy rcp {flash | running-config | startup-config}
```

Syntax Description

flash	Specifies internal Flash memory as the destination of the copy operation.
running-config	Specifies the currently running configuration as the destination of the copy operation.
startup-config	Specifies the configuration used for initialization as the destination of the copy operation.

Command Mode

EXEC

Usage Guidelines

The access server prompts you for the address of the rcp server and rcp filename. It provides an option to erase existing Flash memory before writing onto it. The entire copying process takes several minutes and will differ from network to network.

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



Caution If the checksum value is not correct according to the value in the README file, do not reboot the access server. Issue the **copy rcp flash** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original system software image back into Flash memory *before* you reboot the access server from Flash memory. If you have a bad image in Flash memory and try to boot from Flash, and netbooting is not configured, the access server will start the system image contained in ROM. If ROM does not contain a fully functional system image, the access server will not function and will have to be reconfigured through a direct console port connection.

The rcp protocol requires that a client send the remote username of an rcp request to the server. When you issue the **copy rcp flash** command, by default the software sends the username associated with the current TTY, if that name is valid. For example, if the user is connected to the access server through Telnet and the user was authenticated through the **username** command, then the Cisco IOS software sends that username as the remote username.

Note For Cisco, TTYs are commonly used in communications servers. The concept of TTYs originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called TTY devices (which stands for teletype, the original UNIX terminal).

If the TTY remote username is invalid, the Cisco IOS software uses the access server host name as the both the remote and local usernames. To specify that a different remote username be sent to the network server, use the **ip rcmd remote-username** command. The rcp protocol copies the system image from the remote server relative to the directory of the remote username, if the server has a directory structure (for example, UNIX systems).



Caution The remote username must be associated with an account on the destination server. If you do not use the **ip rcmd remote-username** command to specify the name of a remote user associated with an account on the server, then the remote username associated with the current TTY process must be associated with an account on the server. If there is no username for the current TTY process, then the access server host name must be associated with an account on the server. If the network administrator of the destination server did not establish accounts for the remote username used, and if a default remote username is used, this command will not execute successfully.

If you copy the system image from a PC used as a file server, the remote host computer must support the remote shell protocol.

Use the **copy rcp flash** to copy a system image from a network server to the access server's internal Flash memory using rcp. The access server prompts for the address of the rcp server and rcp filename. When you issue this command, the system provides an option to erase existing Flash memory before writing onto it. The entire copying process takes several minutes and will differ from network to network.

Before booting from Flash memory, verify that the checksum of the image in internal Flash memory matches the checksum listed in the README file that was distributed with the system software image. The checksum of the image in Flash memory is displayed at the bottom of the screen when you issue the **copy tftp flash** command. The README file was copied to the rcp server automatically when you installed the system software image.



Caution If the checksum value does not match the value in the README file, do not reboot the access server. Reissue the **copy rcp flash** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original system software image back into Flash memory *before* you reboot the access server from Flash memory. If you have a bad image in Flash memory and try to boot from Flash, and booting from a network server is not configured, the access server will start the system image contained in ROM. If ROM does not contain a fully functional system image, the access server will not function and will have to be reconfigured through a direct console port connection.

Use the **copy rcp running-config** command to copy a configuration file from a network server to the access server's running configuration environment using rcp. 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. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Note When using rcp, the **copy rcp running-config** command replaces the **configure network** command.

Use the **copy rcp startup-config** command to copy a host or network configuration file from a network server to the access server's startup configuration environment using rcp. Accept the default value of *host* to copy and store a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and store a network configuration file containing commands that apply to all network servers on a network. The **copy rcp startup-config** command copies a configuration file from the network server to NVRAM.

Note When using rcp, the **copy rcp startup-config** command replaces the **configure overwrite-network** command.

Examples

This example copies a system image named *IJ01030z* from the *netadmin1* directory on the remote server named *SERVER1.CISCO.COM* with an IP address of 131.108.101.101 to the access server's Flash memory. To ensure that enough Flash memory is available to accommodate the system image to be copied, the Cisco IOS software allows you to erase the contents of Flash memory first.

```
Router# configure terminal

commserver1(config)# rcmd remote-username netadmin1
Ctrl-Z
commserver1# copy rcp flash

System flash directory, partition 2:
File Length Name/status
  1  984   junk [deleted]
  2  984   junk
[2096 bytes used, 8386512 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 172.30.254.254
Source file name? junk
Destination file name [junk]?
Accessing file 'junk' on 172.30.254.254...
Loading dirt/ssangiah/junk .from 223.255.254.254 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'junk' from server
  as 'junk' into Flash WITH erase? [yes/no]yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading junk from 172.30.254.254 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

The following example shows sample output when copying a system image into a partition of Flash memory. The system prompts 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, *?* for directory display of all partitions, or *?number* for directory display of a particular partition. The default is the first read/write partition.

```
Router# copy rcp 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]
```

If the partition is read-only and has dual Flash bank support in boot ROM, the session continues as follows:

```

                **** 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]? 172.30.1.1
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```

Loading master/igs-bfpx.100-4.3 from 172.30.1.111: !
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
```

If the partition is read-write, the session continues as follows:

```

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 [255.255.255.255]? 172.30.1.1
Source file name? master/igs-bfpx.100-4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```

Accessing file 'master/igs-bfpx.100-4.3' on ABC.CISCO.COM...
Loading master/igs-bfpx.100-4.3 from 172.30.1.111: !
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
```

The following example specifies a remote username of *netadmin1*. Then it copies and runs a host configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.30.101.101.

```

Router# configure terminal
Router# ip rcmd remote-username netadmin1
Ctrl-Z
Router# copy rcp running-config
```

```
Host or network configuration file [host]?
Address of remote host [255.255.255.255]? 172.30.101.101
Name of configuration file [cs-config]? host1-config
Configure using host1-config from 172.30.101.101? [confirm]
Connected to 172.30.101.101
Loading 1112 byte file host1-config:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.30.101.101
```

The following example shows how to copy a configuration file to a Cisco 2500 system using rcp. This example specifies a remote username of *netadmin1*. Then it copies and stores a host configuration file *host2-config* from the *netadmin1* directory on the remote server with an IP address of 172.30.101.101:

```
cs2# configure terminal
cs2# ip rcmd remote-username netadmin1
Ctrl-Z
cs2# copy rcp startup-config
Host or network configuration file [host]?
Address of remote host [255.255.255.255]? 172.30.101.101
Name of configuration file[cs2-config]? host2-config
Configure using cs2-config from 172.30.101.101? [confirm]
Connected to 172.30.101.101
Loading 1112 byte file cs2-config:![OK]
[OK]
cs2#
%SYS-5-CONFIG_NV:Non-volatile store configured from cs2-config by rcp from
172.30.101.101
```

Related Commands

- boot system**
- copy flash**
- copy running-config**
- copy running-config startup-config**
- copy startup-config rcp**
- ip rcmd remote-username**
- verify flash**

copy running-config

To copy the running configuration file from the access server to a network server using rcp, use the **copy running-config EXEC** commands. The **copy running-config startup-config** command replaces the **write memory** command. The **copy running-config rcp** or **copy running-config tftp** command replaces the **write network** command.

```
copy running-config { rcp | startup-config | tftp }
```

Syntax Description

rcp	Specifies a copy operation to a network server using rcp.
startup-config	Specifies the configuration used for initialization as the destination of the copy operation.
tftp	Specifies a TFTP server as the destination of the copy operation.

Command Mode

EXEC

Usage Guidelines

(Cisco 2500 only.) Use the **copy running-config { rcp | tftp }** command to copy the current configuration file to a network server using rcp or TFTP. The configuration file copy can serve as a backup copy. You are prompted for a destination host and filename.

The rcp protocol requires that a client send the remote username of an rcp request to the server. When you issue the **copy running-config rcp** command, by default the Cisco IOS software sends the username associated with the current TTY, if that name is valid. For example, if the user is connected to the access server through Telnet and the user was authenticated through the **username** command, then the Cisco IOS software sends that username as the remote username.

If the TTY username is invalid, the Cisco IOS software uses the access server host name as the both the remote and local usernames.

Note For Cisco, TTYs are commonly used in communication servers. The concept of TTYs originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called TTY devices (which stands for teletype, the original UNIX terminal).

To specify that a different remote username be sent to the server, use the **ip rcmd remote-username** command. The rcp software copies the running configuration file to the remote server relative to the directory of the remote username that you specify, if the server has a directory structure (for example, UNIX systems).



Caution The remote username must be associated with an account on the destination server. If you do not use the **ip rcmd remote-username** command to specify the name of a remote user associated with an account on the server, then the remote username associated with the current TTY process must be associated with an account on the server. If there is no username for the current TTY process, then the access server host name must be associated with an account on the server. If the network administrator of the destination server did not establish accounts for the remote username that is used, and if a default remote username is used, this command will not execute successfully.

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

To run this command, the access server must contain Flash memory.

The **copy running-config startup-config** command copies the currently running configuration to NVRAM. Use this command in conjunction with the **reload** command to restart the access server with the configuration information stored in NVRAM.

If you issue the **copy running-config startup-config** command from a bootstrap system image, you receive a warning instructing you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands 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.

Example

The following example specifies a remote username of *netadmin1*. Then it copies the running configuration file, named *cs2-config* to the *netadmin1* directory on the remote host with an IP address of 172.30.101.101:

```
cs2# configure terminal
cs2# ip rcmd remote-username netadmin1
Ctrl-Z
cs2# copy running-config rcp
Remote host[]? 172.30.101.101
Name of configuration file to write [cs2-config]?
Write file cs2-config on host 172.30.101.101?[confirm]
###! [OK]
Connected to 172.30.101.101
cs2#
```

The following is an example of the **copy running-config startup-config** command and the warning the system provides if you are trying to save configuration information from bootstrap into the system:

```
cs2(boot)# copy running-config 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.

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

copy rcp running-config
ip rcmd remote-username †
copy rcp startup-config
copy startup-config
reload †

copy startup-config

To copy a startup configuration file to a network server using rcp, use the **copy startup-config EXEC** commands.

```
copy startup-config {rcp | running-config | tftp}
```

Syntax Description

rcp	Specifies a copy operation to a network server using rcp.
running-config	Specifies the currently running configuration as the destination of the copy operation.
tftp	Specifies a TFTP server as the destination of the copy operation.

Command Mode

EXEC

Usage Guidelines

Use this command to copy the contents of the configuration file in nonvolatile memory to a network server.

The rcp protocol requires that a client send the remote username of an rcp request to the server. When you issue the **copy startup-config rcp** command, by default the Cisco IOS software sends the username associated with the current TTY, if that name is valid. For example, if the user is connected to the access server through Telnet and the user was authenticated through the **username** command, then the Cisco IOS software sends that username as the remote username.

If the TTY username is invalid, the Cisco IOS software uses the access server host name as the both the remote and local usernames.

Note For Cisco, TTYs are commonly used in communication servers. The concept of TTYs originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called TTY devices (which stands for teletype, the original UNIX terminal).

To specify that a different remote username be sent to the server, use the **ip rcmd remote-username** command. The rcp software copies the system image to the remote server relative to the directory of the remote username, if the server has a directory structure (for example, UNIX systems).



Caution The remote username must be associated with an account on the destination server. If you do not use the **ip rcmd remote-username** command to specify the name of a remote user associated with an account on the server, then the remote username associated with the current TTY process must be associated with an account on the server. If there is no username for the current TTY process, then the access server host name must be associated with an account on the server. If the network administrator of the destination server did not establish accounts for the remote username used, and if a default remote username is used, this command will not execute successfully.

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

To run this command, the access server must contain Flash memory.

Example

The following example shows how to copy a startup configuration file to a network server using rcp:

```
Router# configure terminal
Router# ip rcmd remote-username netadmin2
Ctrl-Z
Router# copy startup-config rcp
Remote host[]? 172.30.101.101
Name of configuration file to write [cs2-config]?
Write file cs2-config on host 172.30.101.101?[confirm]
! [OK]
```

Related Commands

copy rcp startup-config

copy running-config

ip rcmd remote-username

copy tftp

To copy a file from a TFTP server to the access server or to another destination, use one of the following **copy tftp** EXEC commands. The **copy tftp running-config** command replaces the **configure network** command. The **copy tftp startup-config** command replaces the **configure overwrite-network** command.

```
copy tftp { flash | running-config | startup-config }
```

Syntax Description

flash	Specifies internal Flash memory as the destination of the copy operation.
running-config	Specifies the currently running configuration as the destination of the copy operation.
startup-config	Specifies the configuration used for initialization as the destination of the copy operation.

Command Mode

EXEC

Usage Guidelines

The access server prompts for the address of the network server and TFTP filename. It provides an option to erase existing Flash memory before writing onto it. The entire copying process takes several minutes and will differ from network to network.

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



Caution If the checksum value is not correct according to the value in the README file, do not reboot the access server. Issue the **copy tftp flash** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original system software image back into Flash memory *before* you reboot the access server from Flash memory. If you have a bad image in Flash memory and try to boot from Flash, and netbooting is not configured, the access server will start the system image contained in ROM (assuming). If ROM does not contain a fully functional system image, the access server will not function and will have to be reconfigured through a direct console port connection.

Note When using TFTP, the **copy tftp running-config** command replaces the **configure network** command and the **copy tftp startup-config** command replaces the **configure overwrite-network** command.

Example

The following example shows sample output of copying a system image named *IJ01030Z* into Flash memory:

```
Router# copy tftp flash
System flash directory, partition 2:
File Length Name/status
  1  984   junk [deleted]
  2  984   junk
[2096 bytes used, 8386512 available, 8388608 total]
Address or name of remote host [255.255.255.255]?172.30.254.254
Source file name? junk
Destination file name [junk]?
Accessing file 'junk' on 172.30.254.254...
Loading dirt/ssangiah/junk .from 172.30.254.254 (via Ethernet0): - [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'junk' from server
  as 'junk' into Flash WITH erase? [yes/no]yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Loading junk from 223.255.254.254 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

The series of Vs in the sample output indicates that a checksum verification of the image is occurring after the image is written to Flash memory.

The following example shows sample output when copying a system image into a partition of Flash memory. The system will prompt 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 to enter a partition number, ? for directory display of all partitions, or ?*number* for directory display of a particular partition. The default is the first read/write partition.

```
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]
```

If the partition is read-only and has dual Flash bank support in boot ROM, the session continues as follows:

```
**** 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]? 131.108.1.1
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```
Loading master/igs-bfpx.100-4.3 from 131.108.1.111: !
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
```

If the partition is read-write, the session continues as follows:

```
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 [255.255.255.255]? 131.108.1.1
Source file name? master/igs-bfpx.100-4.3
Destination file name [default = source name]?
```

The file will be copied into the partition given by the user earlier:

```
Accessing file 'master/igs-bfpx.100-4.3' on ABC.CISCO.COM...
Loading master/igs-bfpx.100-4.3 from 172.30.1.111: !
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
```

Related Commands

boot system flash

copy flash tftp

verify flash

copy verify

The **verify flash** command replaces the **copy verify** command. Refer to the description of the **verify flash** command for more information.

erase

To erase a saved configuration, use one of the following **erase** EXEC commands. The **erase startup-config** command replaces the **write erase** command.

erase startup-config

Syntax Description

startup-config Erases the startup configuration in NVRAM.

Command Mode

EXEC

Usage Guidelines

Use the **erase startup-config** command on all platforms to erase the startup configuration. This command erases the configuration stored in NVRAM.

Example

The following example illustrates how to erase the configuration located in NVRAM :

```
Gouda#erase startup-config
```

Related Commands

show startup-config

erase flash

To erase internal Flash memory, use the **erase flash** EXEC command. This command replaces the **copy erase flash** command.

erase flash

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

This command performs the same action as the **copy erase flash** command.

Example

The following example illustrates how to use this command. Note that this example reflects the dual Flash bank feature only available on Cisco 2500 series.

```
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, **?** for directory display of all partitions, or **?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-bfx.103.1
[3459784 bytes used, 734520 available, 4194304 total]

Erase flash device, partition 2? [confirm] <Return>
```

ip rarp-server

Use the **ip rarp-server** interface configuration command to allow the access server to act as a Reverse Address Resolution Protocol (RARP) server. Use the **no** form of the command to restore the interface to the default of no RARP server support.

```
ip rarp-server ip-address  
no ip rarp-server ip-address
```

Syntax Description

ip-address IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This feature makes diskless booting of clients possible between network subnets where the client and server are on separate subnets.

RARP server support is configurable on a per interface basis, so that the access server does not interfere with RARP traffic on subnets that do not need RARP assistance from the access server.

The access server answers incoming RARP requests only if both of the following conditions are met:

- The **ip rarp-server** command has been configured for the interface on which the request was received.
- There is a static entry found in the IP ARP table that maps the MAC address contained in the RARP request to an IP address.

Use the **show ip arp EXEC** command to display the contents of the IP ARP cache.

Sun Microsystems, Inc., makes use of RARP and UDP-based network services to facilitate network-based booting of SunOS on their workstations. By bridging RARP packets and using both the **ip helper-address** interface configuration command and the **ip forward-protocol** global configuration command, the access server should be able to perform the necessary packet switching to enable booting of Sun workstations across subnets. Unfortunately, some Sun workstations assume that the sender of the RARP response, in this case the access server, is the host the client can contact to TFTP load the bootstrap image. This causes the workstations to fail to boot.

By using the **ip rarp-server** feature, the access server can be configured to answer these RARP requests, and the client machine should be able to reach its server by having its TFTP requests forwarded through the access server that acts as the RARP server.

In the case of RARP responses to Sun workstations attempting to diskless boot, the IP address specified in the **ip rarp-server** interface configuration command should be the IP address of the TFTP server. In addition to configuring RARP service, the access server must also be configured to forward UDP-based Sun portmapper requests to completely support diskless booting of Sun workstations. This can be accomplished using configuration commands of the form:

```
ip forward-protocol udp 111
interface interface name
ip helper-address target-address
```

RFC 903 documents the Reverse Address Resolution Protocol.

Examples

The following partial example configures the access server to act as a RARP server. The access server is configured to use the primary address of the specified interface in its RARP responses.

```
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
ip address 172.30.3.100 255.255.255.0
ip rarp-server 172.30.3.100
```

In the following example, the access server is configured to act as a RARP server, with TFTP and portmapper requests forwarded to the Sun server:

```
! Allow the communication server to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the communication server with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface ethernet 0
! Configure the communication server to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ip forward-protocol †

ip helper-address †

ip rcmd domain-lookup

Use the **ip rcmd domain-lookup** global configuration command to enable DNS security for rcp and rsh. To bypass DNS security for rcp and rsh, use the **no** form of this command.

ip rcmd domain-lookup
no ip rcmd domain-lookup

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

If you do not want to use DNS for rcmd queries, but DNS has been enabled with the **ip domain-lookup** command, use the **no ip rcmd domain-lookup** command.

This command will turn off DNS lookups for rsh and rcp only. The **no ip domain-lookup** command takes precedence over the **ip rcmd domain-lookup** command. If **ip domain-lookup** is disabled using the **no ip domain-lookup** command, DNS will be bypassed for rcp and rsh, even if **ip rcmd domain-lookup** is enabled.

Note In Cisco IOS Release 10.3, the **ip** keyword has been added to **rcmd** commands. If you are upgrading from Cisco IOS Release 10.2 to 10.3, this keyword will automatically be added to any **rcmd** commands you have in your Cisco IOS Release 10.2 configuration files.

Example

In the following example, DNS security is enabled for rcp and rsh.

```
ip rcmd domain-lookup
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

ip domain-lookup †

ip rcmd rcp-enable

To configure the access server to allow remote users to copy files to and from the access server, use the **ip rcmd rcp-enable** global configuration command. Use the **no rcp-enable** command to disable a access server that is enabled for rcp.

ip rcmd rcp-enable
no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

Default

To ensure security, the access server is not enabled for rcp by default.

Command Mode

Global configuration

Usage Guidelines

To allow a remote user to execute rcp commands on the access server, you must also create an entry for the remote user in the local access server's authentication database.

The **no ip rcmd rcp-enable command** does not prohibit a local user from using rcp to copy system images and configuration files to and from the access server.

To protect against undesirable users copying the system image or configuration files without consent, the access server is not enabled for rcp by default.

Note In Cisco IOS Release 10.3, the **ip** keyword has been added to **rcmd** commands. If you are upgrading from Cisco IOS Release 10.2 to 10.3, this keyword will automatically be added to any **rcmd** commands you have in your Cisco IOS Release 10.2 configuration files.

Example

The following example shows how to enable the access server for rcp:

```
ip rcmd rcp-enable
```

Related Command

ip rcmd remote-host

ip rcmd remote-host

To allow remote users to execute commands on the access server using rsh or rcp, use the **ip rcmd remote-host** global configuration command to create an entry for the remote user in a local authentication database. Use the **no ip rcmd remote-host** command to remove an entry for a remote user from the local authentication database.

```
ip rcmd remote-host local-username {ip-address | host} remote-username [enable]
no ip rcmd remote-host local-username {ip-address | host} remote-username [enable]
```

Syntax Description

<i>local-username</i>	Name of the user on the local access server. You can specify the access server host name as the username. This name needs to be communicated to the network administrator or the user on the remote system. To be allowed to remotely execute commands on the access server, the remote user must specify this value correctly.
<i>ip-address</i>	IP address of the remote host from which the local access server will accept remotely executed commands. Either the IP address or the host name is required.
<i>host</i>	Name of the remote host from which the local access server will accept remotely executed commands. Either the host name or the IP address is required.
<i>remote-username</i>	Name of the user on the remote host from which the access server will accept remotely executed commands.
enable	(Optional) Enables the remote user to execute privileged EXEC commands using rsh. This keyword does not apply to rcp.

Command Mode

Global configuration

Default

No entries are automatically created in the authentication database.

Usage Guidelines

A TCP connection to a access server is established using an IP address. Using the host name is valid only when you are initiating an rcp or rsh command from a local access server. The host name is converted to an IP address using DNS or host-name aliasing.

To allow a remote user to execute rcp or rsh commands on a local access server, you must create an entry for the remote user in the local access server's authentication database. You must also enable the access server to act as an rsh or rcp server.

To enable the access server to act as an rsh server, issue the **ip rcmd rsh-enable** command. To enable the access server to act as an rcp server, issue the **ip rcmd rcp-enable** command. The access server cannot act as a server for either of these protocols unless you explicitly enable the capacity.

A local authentication database, which is similar to a UNIX *.rhosts* file, is used to enforce security on the access server through access control. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user. To permit a remote user of *rsh* to execute commands in privileged EXEC mode, specify the **enable** keyword.

The difference between an entry that you configure in the access server authentication database and an entry in a UNIX *.rhost* file is that because the *.rhosts* file on a UNIX system resides in the home directory of a local user account, an entry in a UNIX *.rhosts* file does not need to include the local username. The local username is determined from the user account. To provide equivalent support on a access server, specify the local username along with the remote host and remote username in each authentication database entry that you configure.

For a remote user to be able to execute commands on the access server in its capacity as a server, the local username, host address or name, and remote username sent with the remote client request must match values configured in an entry in the local authentication file.

A remote client host should be registered with DNS. The Cisco IOS software uses DNS to authenticate the remote host's name and address. Because DNS can return several valid IP addresses for a host name, the Cisco IOS software checks the address of the requesting client against all of the IP addresses for the named host returned by DNS. If the address sent by the requester is considered invalid in that it does not match any address listed with DNS for the host name, then the Cisco IOS software will reject the remote-command execution request.

Note that if no DNS servers are configured for the access server, then the access server cannot authenticate the host in this manner. In this case, the Cisco IOS software will send a broadcast request to attempt to gain access to DNS services on another server. If DNS services are not available, you must use the **no ip domain-lookup** command to disable the access server's attempt to gain access to a DNS server by sending a broadcast request.

If DNS services are not available and, therefore, you bypass the DNS security check, the Cisco IOS software will accept the request to remotely execute a command *only if* all three values sent with the request match exactly the values configured for an entry in the local authentication file.

Note In Cisco IOS Release 10.3, the **ip** keyword has been added to *rcmd* commands. If you are upgrading from Cisco IOS Release 10.2 to 10.3, this keyword will automatically be added to any *rcmd* commands you have in your Cisco IOS Release 10.2 configuration files.

Example

The following example allows the remote user *netadmin3* on a remote host with the IP address 131.108.101.101 to execute commands on *cs1* using the *rsh* protocol. For *rsh*, user *netadmin3* is allowed to execute commands in privileged EXEC mode.

```
ip rcmd remote-host cs1 172.30.101.101 netadmin3 enable
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

ip rcmd rcp-enable

ip rcmd rsh-enable

no ip domain-lookup†

ip rcmd remote-username

To configure the remote username to be used when requesting a remote copy using rcp, use the **ip rcmd remote-username** global configuration command. To remove the remote username from the configuration, use the **no ip rcmd remote-username** command.

```
ip rcmd remote-username username  
no ip rcmd remote-username username
```

Syntax Description

username Name of the remote user on the server. This name is used for rcp copy requests. If the server has a directory structure, such as UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user's account.

Command Mode

Global configuration

Default

If you do not issue this command, the Cisco IOS software sends the remote username associated with the current TTY process for rcp copy commands, if the username is valid. For example, if the user is connected to the access server through Telnet and the user was authenticated through the **username** command, then the Cisco IOS software sends that username as the remote username.

If the username for the current TTY process is not valid, the Cisco IOS software sends the host name as the remote username. For rcp boot commands, the Cisco IOS software sends the access server host name by default.

Note For Cisco, TTYs are commonly used in access servers. The concept of TTYs originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called TTY devices (which stands for teletype, the original UNIX terminal).

Usage Guidelines

The rcp protocol requires that a client send the remote username on an rcp request to the server. Use this command to specify the remote username to be sent to the server for an rcp copy request. All files and images to be copied are searched for or written relative to the directory of the remote user's account, if the server has a directory structure, for example, as do UNIX systems.

Note In Cisco IOS Release 10.3, the **ip** keyword has been added to rcmd commands. If you are upgrading from Cisco IOS Release 10.2 to 10.3, this keyword will automatically be added to any **rcmd** commands you have in your Cisco IOS Release 10.2 configuration files.



Caution The remote username must be associated with an account on the destination server.

Example

The following example shows how to use this command:

```
Router# configure terminal  
Router(config)# ip rcmd remote-username netadmin1  
Router(config)# Ctrl-Z
```

Related Commands

- boot network**
- boot system**
- copy flash**
- copy rcp**
- copy rcp running-config**
- copy rcp startup-config**
- copy running-config**
- copy startup-config**

ip rcmd rsh-enable

To configure the access server to allow remote users to execute commands on the access server using rsh, use the **ip rcmd rsh-enable** global configuration command. Use the **no ip rcmd rsh-enable** command to disable a access server that is enabled for rsh.

ip rcmd rsh-enable
no rsh-enable

Syntax Description

This command has no arguments or keywords.

Default

To ensure security, the access server is not enabled for rsh by default.

Command Mode

Global configuration

Usage Guidelines

Use this command to enable the access server to receive rsh requests from remote users. In addition to issuing this command, to allow a remote user to execute rsh commands on the access server, you must create an entry for the remote user in the local access server's authentication database.

The **no rsh-enable command** does not prohibit a local user of the access server from executing a command on other access servers and UNIX hosts on the network using rsh.

Note In Cisco IOS Release 10.3, the **ip** keyword has been added to **rcmd** commands. If you are upgrading from Cisco IOS Release 10.2 to 10.3, this keyword will automatically be added to any **rcmd** commands you have in your Cisco IOS Release 10.2 configuration files.

Example

The following example shows how to enable the access server as an rsh server:

```
ip rcmd rsh-enable
```

Related Command

ip rcmd remote-host

mop device-code

To identify the type of device sending MOP sysid messages and request program messages, use the **mop device-code** global configuration command. Use the **no** form of the command to set the identity to the default value.

```
mop device-code { cisco | ds200 }  
no mop device-code { cisco | ds200 }
```

Syntax Description

cisco	Denotes a Cisco device code.
ds200	Denotes a DECserver 200 device code.

Default

Cisco device code

Command Mode

Global configuration

Usage Guidelines

The sysid messages and request program messages use the identity information indicated by this command.

Example

The following example identifies a DECserver 200 device as sending MOP sysid and request program messages:

```
mop device-code ds200
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

mop sysid †

mop retransmit-timer

To configure the length of time the access server waits before retransmitting boot requests to a MOP server, use the **mop retransmit-timer** global configuration command. Use the **no** form of the command to reinstate the default value.

```
mop retransmit-timer seconds  
no mop retransmit-timer
```

Syntax Description

seconds Sets the length of time, in seconds, that the access server waits before retransmitting a message. The value is a number from 1 to 20.

Default

4 seconds

Command Mode

Global configuration

Usage Guidelines

By default, when the access server transmits a request that requires a response from a MOP boot server and the server does not respond, the message will be retransmitted after 4 seconds. If the MOP boot server and access server are separated by a slow serial link, it might take longer than 4 seconds for the access server to receive a response to its message. Therefore, you might want to configure the access server to wait longer than 4 seconds before retransmitting the message if you are using such a link.

Example

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

```
mop retransmit-timer 10
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

```
mop device-code  
mop retries  
mop enabled †
```

mop retries

To configure the number of times a access server will retransmit boot requests to a MOP server, use the **mop retries** global configuration command. Use the **no** form of the command to reinstate the default value.

mop retries *count*
no mop retries

Syntax Description

count Indicates the number of times a access server will retransmit a MOP boot request. The value is a number from 3 to 24.

Default

8 times

Command Mode

Global configuration

Example

In the following example, the access server will attempt to retransmit a message to an unresponsive host 11 times before declaring a failure:

```
mop retries 11
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

mop device-code
mop retransmit-timer
mop enabled †

o

To list the value of the boot field (bits 0-3) in the configuration register, use the ROM monitor **o** command. To reset the value of the boot field so that the access server boots from ROM, use the ROM monitor **o/r** command.

o
o/r

Syntax Description

This command has no arguments or keywords.

Default

Refer to the appropriate hardware installation guide for default values.

Command Mode

ROM monitor

Usage Guidelines

To get to the ROM monitor prompt at a access server, use the **reload EXEC** command if the configuration register has a boot value of 0. (For systems with a software configuration register, a value can be included on the **o/r** command line.) Use the **i** command in conjunction with the **o/r** command to initialize the access server. (The **i** command is documented in the hardware installation and maintenance publication for your product.) The **o/r** command resets the configuration register to 0x141, which disables the Break key, ignores the nonvolatile memory configuration, and boots the default system image from ROM.

Examples

The following is an example of the **o** command:

```
> o
Bit# Configuration register option settings:
15 Diagnostic mode disabled
14 IP broadcasts do not have network numbers
13 Do not boot default ROM software if network boot fails
12-11 Console speed is 9600 baud
10 IP broadcasts with ones
09 Do not use secondary bootstrap
08 Break enabled
07 OEM disabled
06 Ignore configuration disabled
03-00 Boot to ROM monitor

>
```

The following is an example of the **o/r** and **i** commands used to reset and boot the default system image from ROM:

```
> o/r
> i
```

Related Command
config-register

partition flash

To partition Flash memory into two partitions, use the **partition flash** global configuration command. Use the **no** form of this command to undo partitioning, and restore Flash memory to one partition.

```
partition flash partitions [size1 size2]  
no partition flash
```

Syntax Description

<i>partitions</i>	Number of partitions in Flash memory. Can be 1 or 2.
<i>size1</i>	(Optional) Size of the first partition in megabytes.
<i>size2</i>	(Optional) Size of the second partition in megabytes.

Default

Flash memory consists of one partition.

If this command is entered but partition size is not specified, two partitions of equal size will be created.

Command Mode

Global configuration

Usage Guidelines

To undo partitioning, use either the **partition flash 1** or **no partition flash** command. If one or more files exist in the second partition, the second partition must be erased manually, using the **erase** command, before reverting to a single partition.

When creating two partitions, you must not truncate a file or cause the spillover of a file into the second partition.

Example

The following example creates two partitions of 4 MB each in Flash memory:

```
partition flash 2 4 4
```

reload

To reload the operating system, use the **reload** EXEC command.

reload

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

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

You cannot reload from a virtual terminal if the system is not set up for automatic booting. This prevents the system from dropping to the ROM monitor and thereby 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 asks you if you want to proceed with the save if the `CONFIG_FILE` environment variable points to a startup configuration file that no longer exists. If you say "yes" in this situation, the system goes to **setup** mode upon reload.

Example

The following example illustrates how to enter the **reload** command at the privileged EXEC prompt:

```
Router# reload
```

Related Command

copy running-config

rsh

To execute a command remotely on a remote rsh host, use the **rsh EXEC** command.

```
rsh {ip-address | host} [/user username] remote-command
```

Syntax Description

<i>ip-address</i>	IP address of the remote host on which to execute the rsh command. Either the IP address or the host name is required.
<i>host</i>	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
/user <i>username</i>	(Optional) Remote username. If you do not specify a remote username, the access server software uses the configured remote username, if one exists. Otherwise, the Cisco IOS software uses the username associated with the current TTY, if it is a valid name. If this name is invalid, the Cisco IOS software uses the host name as the username.
<i>remote-command</i>	Command to be executed remotely. This is a required parameter. Unlike UNIX, the Cisco IOS software does not default to a remote login. Instead, the access server provides telnet and connect services.

Command Mode

EXEC

Default

If you do not specify the **/user** keyword and argument, the access server sends a default remote username unless you override the default by configuring a remote username. As the default value of the remote username, the Cisco IOS software sends the remote username associated with the current TTY process, if that name is valid. If the TTY remote username is invalid, the Cisco IOS software uses the access server host name as the both the remote and local usernames.

Note For UNIX systems, each physical device is represented in the file system. Terminals, or serial lines, are called TTY devices (which stands for teletype, the original UNIX terminal).

Usage Guidelines

Use the rsh command to execute commands remotely. The host on which you remotely execute the command must support the remote shell (rsh) protocol, and the *.rhosts* files on the rsh host must include an entry that permits you to remotely execute commands on that host.

Example

The following example shows how to execute a command remotely on a remote rsh host:

```
Router# rsh mysys.cisco.com /u sharon ls -a
```

```
.  
..  
.alias  
.cshrc  
.emacs  
.exrc  
.history  
.login  
.mailrc  
.newsrc  
.oldnewsrc  
.rhosts  
.twmrc  
.xsession  
jazz
```

Related Command

ip rcmd remote-username

service compress-config

To compress configuration files on access servers that are equipped with nonvolatile memory, use the **service compress-config** global configuration command. To disable compression, use the **no** form of this command.

```
service compress-config
no service compress-config
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

If the file compression completes successfully, the following message is displayed:

```
Compressing configuration from configuration-size to compressed-size
[OK]
```

If the boot ROMs do not recognize a compressed configuration, the following message is displayed:

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

If the file compression fails, the following message is displayed:

```
Error trying to compress nvram
```

One way to determine whether a configuration file will compress enough to fit into nonvolatile memory is to use a text editor to enter the configuration, then use the UNIX **compress** command to check the compressed size. To get a closer approximation of the compression ratio, use the UNIX command **compress -b12**.

Once the configuration file has been compressed, the access server functions normally. A **show configuration** command would uncompress the configuration before displaying it. At boot time, the system would recognize that the configuration file was compressed, uncompress it, and proceed normally.

To disable compression of the configuration file, enter configuration mode and specify the **no service compress-config** command. Then enter the **write memory** command. The access server displays an OK message if it is able to successfully write the uncompressed configuration to nonvolatile memory. Otherwise, the access server displays an error message indicating that the configuration is too large to store. If the configuration file is larger than the physical nonvolatile memory, the following message is displayed:

```
###Configuration too large to fit uncompressed in NVRAM Truncate configuration? [confirm]
```

To truncate and save the configuration, type **Y**. To not truncate and not save the configuration, type **N**.

Example

In the following example, the configuration file is compressed:

```
service compress-config
```

Related Command

show startup-config

service config

To enable automatic loading of configuration files from a network server, use the **service config** global configuration command. Use the **no** form of the command to restore the default.

service config
no service config

Syntax Description

This command has no arguments or keywords.

Default

Disabled, except on systems without nonvolatile memory or with invalid or incomplete information in nonvolatile memory. In these cases, autoloading of configuration files from a network server is enabled automatically.

Command Mode

Global configuration

Usage Guidelines

Usually, the **service config** command is used in conjunction with the **boot host** or **boot network** command. You must enter the **service config** command to enable the access server to automatically configure the system from the file specified by the **boot host** or **boot network** command.

The **service config** command can also be used without the **boot host** or **boot network** command. If you do not specify host or network configuration filenames, the access server uses the default configuration files. The default network configuration file is *network-config*. The default host configuration file is *host-config*, where *host* is the host name of the access server. If the access server cannot resolve its host name, the default host configuration file is *cs-config*.

Example

In the following example, the access server is configured to automatically load the default host configuration file:

```
boot host
service config
```

Related Commands

boot host
boot network

show async bootp

Use the **show async bootp** privileged EXEC command to display the parameters that have been configured for SLIP extended BOOTP requests.

show async bootp

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is a sample output of the **show async bootp** command:

```
Router# show async bootp

The following extended data will be sent in BOOTP responses:

bootfile (for address 172.30.1.1) "pcboot"
bootfile (for address 1172.30.1.111) "dirtboot"
subnet-mask 255.255.0.0
time-offset -3600
time-server 172.30.1.1
```

Table 3-3 describes significant fields shown in the display.

Table 3-3 Show Async BOOTP Field Descriptions

Field	Description
bootfile... "pcboot"	Boot file for address 172.30.1.1 is named pcboot
subnet-mask 255.255.0.0	Subnet mask
time-offset -3600	Local time is one hour (3600 seconds) earlier than UTC time
time-server 128.128.1.1	Address of the time server for the network

Related Command

async-bootp

show configuration

The **show startup-config** command replaces this command. Refer to the description of the **show startup-config** command for more information.

show flash

Use the **show flash** EXEC command to verify Flash memory. The **show flash** command displays the type of Flash memory present, any files that might currently exist in Flash memory, and the amounts of Flash memory used and remaining.

```
show flash [all | chips | detailed | err | partition number [all | chips | detailed | err] |  
summary]
```

Syntax Description

all	(Optional) Shows complete information about Flash memory, including information about the individual ROM devices in Flash memory and the names and sizes of all system image files stored in Flash memory, including those that are invalidated.
chips	(Optional) Shows information per partition and per chip, including which bank the chip is in, its code, size, and name.
detailed	(Optional) Shows detailed information per partition, including file length, address, name, Flash checksum, computer checksum, bytes used, bytes available, total bytes, and bytes of system Flash memory.
err	(Optional) Shows write or erase failures in the form of number of retries.
partition number	(Optional) Shows output for the specified partition number. If you specify the partition keyword, you must specify a partition number. You can use this keyword only when Flash memory has multiple partitions.
summary	(Optional) Shows summary information per partition, including the partition size, bank size, state, and method by which files can be copied into a particular partition. You can use this keyword only when Flash memory has multiple partitions.

Command Mode

EXEC

Sample Display

The following is sample output from the **show flash** command on the Cisco 2500 series:

```
Router# show flash  
  
System flash directory:  
  
File      name/status  
0        ahp4/igs-bfpx.940705  
1        micro/eip1-0  
2        micro/sp1-3  
3        micro/trip1-1  
4        micro/hip1-0  
5        micro/fip1-1  
6        fsipucode  
7        spucode  
8        tripucode  
9        fipucode
```

```

10  eipucode
11  hipucode
12  sipucode
13  sp_q160-1
14  ahp4/sp160-3 [deleted]
15  ahp4/sp160-3
[4008468 bytes used, 185836 bytes available]

```

Table 3-3 describes the **show flash** display fields for the Cisco 2500 series.

Table 3-3 Show Flash Field Descriptions

Field	Description
File	Number of file in Flash memory.
name/status	Files that currently exist in Flash memory.
[deleted]	Flag indicating that another file exists with the same name or that process has been aborted.
bytes used/available	Amount of Flash memory used/amount remaining.

As the display shows, the Flash memory can store and display multiple, independent software images for booting itself or for TFTP server software for other products. This feature is useful for storing default system software. These images can be stored in compressed format (but cannot be compressed by the access server).

To eliminate any files from Flash (invalidated or otherwise) and free up all available memory space, the entire Flash memory must be erased; individual files cannot be erased from Flash memory.

The following is a sample output from the **show flash all** command on the Cisco 2500 Series. The format of your display might differ.

```

Router# show flash all

System flash directory:

File  name/status
      addr      length  fcksum  ccksum
  1  achopra/igs-bfpx.940705
      0x40      4008404  0x35B3  0x35B3
[4008468 bytes used, 185836 bytes available]
4096K bytes of processor board System flash. (Read only mode)
System flash chips could not be identified.
Check the Vpp (12V) jumper installation (if present)
and/or the chips/SIMMs installed.

Flash chips supported by system :
Code  Chip-Sz  Cmd-grp  Chip-name
89B4  0x20000  1        INTEL 28F010
89BD  0x40000  1        INTEL 28F020
01A7  0x20000  1        AMD 28F010
012A  0x40000  1        AMD 28F020
1CD0  0x40000  1        MSM 28F101P
89A2  0x100000 2        INTEL 28F008SA

```

Table 3-4 describes the **show flash all** display fields for the Cisco 2500 series.

Table 3-4 Show Flash All Field Descriptions

Field	Description
File	Number of the system image file. If no filename is specified in the boot system flash command, the access server boots the system image file with the lowest file number.
name/status	Filename and status of a system image file. The status (invalidated) appears when a file has been rewritten (recopied) into Flash memory. The first (now invalidated) copy of the file is still present within Flash memory, but it is rendered unusable in favor of the newest version. The [invalidated] status can also indicate an incomplete file that results from the user aborting the copy process, a network time-out, or a Flash memory overflow.
addr	Address of the file in Flash memory.
length	Size of the system image file (in bytes).
fcksum	Checksum recorded in Flash memory.
ccksum	Computer checksum.
bytes used/available	Amount of Flash memory used/amount of Flash memory available.
bytes of flash memory	Total amount of Flash memory present.
Code	Vendor code identifying the vendor of the ROM unit.
Chip-Sz	Size of the ROM unit (in hex bytes).
Chip-name	Vendor name and chip part number of the ROM unit.

Note When the security jumper is not installed, you cannot write to Flash memory. If you enter the **show flash all** command when the security jumper is not installed, the system returns a message reminding you that the security jumper is not installed, and that the Flash memory is read-only.

The following is sample output from the **show flash** command on the Cisco 2500 series:

```
Router# show flash

System flash directory:

File      name/status
 0      ahp4/igs-bfpx.940705
 1      micro/eip1-0
 2      micro/sp1-3
 3      micro/trip1-1
 4      micro/hip1-0
 5      micro/fip1-1
 6      fsipucode
 7      spucode
 8      tripucode
 9      fipucode
10      eipucode
11      hipucode
12      sipucode
13      sp_q160-1
14      ahp4/sp160-3 [deleted]
```

```

15    ahp4/sp160-3
[4008468 bytes used, 185836 bytes available]

```

Table 3-5 describes the **show flash** display fields.

Table 3-5 Show Flash Field Descriptions

Field	Description
File	Number of file in Flash memory.
name/status	Files that currently exist in Flash memory.
bytes free	Amount of Flash memory remaining.
[deleted]	Flag indicating that another file exists with the same name or that process has been aborted.

As the display shows, the Flash memory can store and display multiple, independent software images for booting itself or for TFTP server software for other products. This feature is useful for storing default system software. These images can be stored in compressed format (but cannot be compressed by the access server).

To eliminate any files from Flash memory (invalidated or otherwise) and free up all available memory space, the entire Flash memory must be erased; individual files cannot be erased from Flash memory.

The following is a sample output from the **show flash** command on a access server that has Flash memory partitioned:

```

Router# show flash
System flash directory, partition 1:
  File Length Name/status
  1 3459720 master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
4096K bytes of processor board System flash (Read Only)

System flash directory, partition 2:
  File Length Name/status
  1 3459720 igs-kf
[3459784 bytes used, 734520 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)

```

In the following example, the security jumper is not installed and you cannot write to Flash memory until the security jumper is installed:

```

Router> show flash all
4096K bytes of flash memory on embedded flash (in RP1).
security jumper(12V) is not installed,
flash memory is read-only.

file      offset length  name
00xDCD0  1903892  igs-k [deleted]
10x1DEA24 1903912  igs-k
[329908/4194304 bytes free]

```

Table 3-6 describes the additional fields in the display.

Table 3-6 Show Flash All Fields for Partitioned Flash Memory

Field	Description
Partition	Partition number in Flash memory.
Size	Size of partition in bytes.
Used	Number of bytes used in partition.
Free	Number of bytes free in partition.
Bank-Size	Size of bank in bytes.
State	State of the partition. It can be one of the following values: <ul style="list-style-type: none"> • Read-Only—indicates the partition that is being executed from. • Read/Write—is a partition that can be copied to.
Copy-Mode	Method by which the partition can be copied to: <ul style="list-style-type: none"> • RXBOOT-FLH—indicates copy via Flash Load Helper. • Direct—indicates that a user can copy directly into Flash memory. • None—indicates that it is not possible to copy into that partition.
Chip	Chip number.
Bank	Bank number.
Code	Code number.
Size	Size of chip.
Name	Name of chip.

The following is sample output for the **show flash chips** command on a access server that has Flash memory partitioned.

```
Router# show flash chips
System flash partition 1:
4096K bytes of processor board System flash (Read ONLY)

  Chip   Bank   Code   Size   Name
  ----   -
  1      1      89A2   1024KB INTEL 28F008SA
  2      1      89A2   1024KB INTEL 28F008SA
  3      1      89A2   1024KB INTEL 28F008SA
  4      1      89A2   1024KB INTEL 28F008SA
Executing current image from System flash [partition 1]

System flash partition 2:
4096K bytes of processor board System flash (Read/Write)

  Chip   Bank   Code   Size   Name
  ----   -
  1      2      89A2   1024KB INTEL 28F008SA
  2      2      89A2   1024KB INTEL 28F008SA
  3      2      89A2   1024KB INTEL 28F008SA
  4      2      89A2   1024KB INTEL 28F008SA
```

The following is sample output for the **show flash detailed** command on a access server that has Flash memory partitioned.

```
Router# show flash detailed
System flash directory, partition 1:
File Length Name/status
```

```

      addr      fcksum  ccksum
1  3224008  igs-kf.100
      0x40      0xEE91  0xEE91
[3224072 bytes used, 970232 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)

```

```

System flash directory, partition 2:
File Length Name/status
      addr      fcksum  ccksum
1  3224008  igs-kf.100
      0x40      0xEE91  0xEE91
[3224072 bytes used, 970232 available, 4194304 total]
4096K bytes of processor board System flash (Read/Write)

```

The following is sample output for the **show flash summary** command on a access server that has Flash memory partitioned. The partition that indicates a state of “Read Only” is the partition that is being executed from.

```

Router# show flash summary
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

```

The following are possible values for Copy-Mode:

- **RXBOOT-MANUAL**—User can copy manually by reloading to the boot ROM image.
- **RXBOOT-FLH**—User can copy via Flash load helper.
- **Direct**—User can copy directly into Flash memory.
- **None**—Copy not allowed into that partition.

show flh-log

To view the system console output generated during the Flash load helper operation, use the **show flh-log** privileged EXEC command.

show flh-log

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

If you are a remote Telnet user performing the Flash upgrade without a console connection, this command allows you to retrieve console output when your Telnet connection has terminated due to switching to the ROM image. The output indicates what happened during the download, and is particularly useful if the download fails.

Sample Display

The following is sample output from the **show flh-log** command:

```
Router# show flh-log
%FLH: abc/igs-kf.103 from 172.30.1.111 to flash ...

System flash directory:
File Length Name/status
  1 2251320 abc/igs-kf.103

[2251384 bytes used, 1942920 available, 4194304 total]
Accessing file 'abc/igs-kf.103' on 172.30.1.111...
Loading from 172.30.13.111:

Erasing device... .. erased
Loading from 131.108.13.111:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK -
2251320/4194304 bytes]

Verifying checksum... OK (0x97FA)
Flash copy took 79292 msecs
%FLH: Re-booting system after download
Loading abc/igs-kf.103 at 0x3000040, size = 2251320 bytes [OK]

F3: 2183364+67924+259584 at 0x3000060
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted --More--

Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

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

Cisco Internetwork Operating System Software
Cisco IOS (tm) GS Software (GS7), Version 10.3
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Tue 06-Dec-94 14:01 by smith
Image text-base: 0x00001000, data-base: 0x005A9C94

cisco 2500 (68030) processor (revision 0x00) with 4092K/2048K bytes of
memory.
Processor board serial number 00000000
DDN X.25 software, Version 2.0, NET2 and BFE compliant.
ISDN software, Version 1.0.
Bridging software.
Enterprise software set supported. (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
--More--

1 ISDN Basic Rate interface.
32K bytes of non-volatile configuration memory.

4096K bytes of processor board System flash (Read ONLY)

Related Command

copy tftp

show running-config

To display the configuration information currently running on the terminal, use the **show running-config** EXEC command. This command replaces the **write terminal** command.

show running-config

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in NVRAM.

Example

The following example illustrates how to display the running configuration:

```
show running-config
```

Related Commands

configure
copy running-config startup-config
show startup-config

show startup-config

To display the contents of NVRAM (if present and valid), use the **show startup-config EXEC** command. This command replaces **show configuration** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

NVRAM stores the configuration information on the network server in text form as configuration commands. The **show startup-config** command shows the version number of the software used when you last executed the **copy running-config startup-config** command.

Sample Displays

The following is sample output from the **show startup-config** command. It shows the access server displaying the contents of NVRAM.

```
Router# show startup-config

Using 5057 out of 32768 bytes
!
version 10.3
!
enable-password xxxx
service pad
!
boot system dross-system 131.108.13.111
boot system dross-system 131.108.1.111
!
exception dump 131.108.13.111
!
no ip ipname-lookup
!
decnet routing 13.1
decnet node-type area
decnet max-address 1023
!
interface Ethernet 0
ip address 131.108.1.1 255.255.255.0
ip helper-address 131.120.1.0
ip accounting
ip gdp
decnet cost 3
!
ip domain-name CISCO.COM
ip name-server 255.255.255.255
!
end
```

Related Commands

A dagger (†) indicates that the command is documented in another chapter.

configure

description †

service compress-config

copy running-config startup-config

show running-config

show version

Use the **show version** EXEC command to display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

show version

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show version** command from a Cisco 2500 series:

```
Router> show version

3000 Software (IGS-BFPX), Version 10.2
Copyright (c) 1986-1994 by cisco Systems, Inc.
Compiled Tue 05-Jul-94 16:14

System Bootstrap, Version (3.3), SOFTWARE

cs1 uptime is 6 days, 20 hours, 46 minutes
System restarted by reload
System image file is "achopra/igs-bfpx.940705", booted via flash

cisco 2500 (68030) processor (revision A) with 1024K/1024K bytes of memory.
Processor board serial number 01244583
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Bridging software.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
Authorized for Enterprise software set. (0x0)
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
16 terminal lines.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash. (Read only mode)
Configuration register is 0x0
```

Table 3-7 describes significant fields shown in the display.

Table 3-7 Show Version Field Descriptions

Field	Description
software version	Information identifying the software by name and version number, including the date and time it was compiled. Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 10.2.
System Bootstrap, Version...	Bootstrap version string.
Cs1 uptime is...	The amount of time the system has been up and running.

show version

Field	Description
System restarted by...	Also displayed is a log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is generally the result of an attempt to access a nonexistent address, as follows: System restarted by bus error at PC 0xC4CA, address 0x210C0C0
System image file is ...	If the software was booted over the network, the IP address of the boot host is shown. If the software was loaded from onboard ROM, this line reads "running default software." In addition, the names and sources of the host and network configuration files are shown.
cisco 2500 (68030) processor...	The remaining output shows the hardware configuration and any nonstandard software options. The configuration register contents are displayed in hexadecimal notation.

The output of the **show version EXEC** command can also provide certain messages, such as bus error messages. If such error messages appear, report the complete text of this message to your technical support specialist.

tftp-server

To specify that the access server operate as a TFTP server, use the **tftp-server** global configuration command. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no tftp-server system** command with the appropriate filename and, optionally, the IP access list number.

```
tftp-server flash [partition-number:]filename1 [alias filename2] [access-list-number]
```

```
tftp-server rom alias filename2 [access-list-number]
```

```
no tftp-server {flash [partition-number:]filename1 | rom alias filename2}
```

Syntax Description

flash	Specifies TFTP service of a file in Flash memory.
rom	Specifies TFTP service of a file in ROM.
<i>filename1</i>	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
<i>filename2</i>	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.
<i>access-list-number</i>	(Optional) Basic IP access-list number. Valid values are 0 to 99.
<i>partition-number:</i>	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

You can specify multiple filenames by repeating the **tftp-server** command. The system sends a copy of the system image contained in ROM or one of the system images contained in Flash memory to any host that issues a TFTP read request with this filename.

If the specified *filename1* or *filename2* exists in Flash memory, a copy of the Flash image is sent. On systems that contain a complete image in ROM, the system sends the ROM image if the specified *filename1* or *filename2* is not found in Flash memory.

Images that run from ROM cannot be loaded over the network. Therefore, it does not make sense to use TFTP to offer the ROMs on these images.

Examples

In the following example, the system uses TFTP to send a copy of the *version-10.3* file located in Flash memory in response to a TFTP Read Request for that file. The requesting host is checked against access list 22.

```
tftp-server flash version-10.3 22
```

In the following example, the system uses TFTP to send a copy of the ROM image *flash:2:igs-bpx-1* in response to a TFTP Read Request for the *flash:2:igs-bpx-1* file:

```
tftp-server rom alias gs3-k.101
```

Related Command

A dagger (†) indicates that the command is documented in another chapter.

access-list[†]

verify flash

The system will prompt only if there are two or more read/write partitions. 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 partition.

```
File Length Name/status
  1 3459720 master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]

Name of file to verify? master/igs-bfpx.100-4.3
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
```

write erase

The **erase startup-config** command replaces this command. Refer to the description of the **erase** command for more information on **erase startup-config**.

write memory

The **copy running-config startup-config** command replaces this command. Refer to the description of the **copy running-config** command for more information on **copy running-config startup-config**.

write network

The **copy running-config rcp** or **copy running-config tftp** command replaces this command. Refer to the description of the **copy running-config** command for more information on **copy running-config rcp** or **copy running-config tftp**.

write terminal

The **show running-config** command replaces this command. Refer to the description of **show running-config** for more information.