F through K

F through K

F through K

factory-reset all

To erase all the user-configured data, use the **factory-reset all** command in EXEC mode:

factory-reset all

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The command erases the following data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
Router>enable
Router>factory-reset all
```

factory-reset keep-licensing-info

To erase all the user-configured data except the licensing information, use the **factory-reset keep-licensing-info** command in EXEC mode:

factory-reset keep-licensing-info

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

This command erases the following user-configured data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials

Examples

The following example shows the configuration of the command:

```
enable
factory-reset keep-licensing-info
```

factory-reset all secure 3-pass

To erase all data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard, use the **factory-reset all secure 3-pass-DoD 5220-22-M** command in EXEC mode:

factory-reset all-secure 3-pass-DoD 5220-22-M

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The commands erases the following data

- All writable file systems and personal data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard:
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
enable
factory-reset all-secure 3-pass
DoD 5220-22-M
```

file privilege

To configure a new file privilege level for users use the **file privilege** command in global configuration mode. To reset the file privilege level of the files to the default and remove the file privilege level configuration from the running configuration file, use the **no** form of this command.

file privilege level *level*
no file privilege level *level*

Syntax Description

level	Specifies the file privilege level for the files. The level argument must be a number from 0 to 15. Users with privilege level equal to greater than the file privilege level can access the files under the file system.

Command Default

By default the privilege level is set to 15.

Command Modes

Global configuration (config#)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example, shows how to set the file privilege level to 3 and verify the change using the **show running-config** command.

```
Device(config)# file privilege ?
 <0-15>  Privilege level

Device(config)# file privilege 3
Device(config)# end

Device# show running-config | i file priv
file privilege 3
```

Related Commands

Command	Description
privilege level	Sets the default privilege level for a line.

file prompt

To specify the level of prompting, use the **file prompt**command in global configuration mode.

file prompt prompt [{**alert** | **noisy** | **quiet**}]

Syntax Description

alert	(Optional) Prompts only for destructive file operations. This is the default.
noisy	(Optional) Confirms all file operation parameters.
quiet	(Optional) Seldom prompts for file operations.

Command Default

alert

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to change the amount of confirmation needed for different file operations.

This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

Examples

The following example configures confirmation prompting for all file operations:

```
Router(config)# file prompt noisy
```

file verify auto

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

file verify auto
no file verify auto

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	Support was added for the Supervisor Engine 2.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

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

Examples

The following example shows how to enable automatic image verification:

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

Related Commands

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

format

To format a Class A, Class B, or Class C flash memory file system, use the **format** command in privileged EXEC or diagnostic mode.

Class B and Class C Flash File Systems
format *filesystem1:*

Class A Flash File System
format [**spare** *spare-number*] *filesystem1***:** [[*filesystem2***:**][*monlib-filename*]]

Syntax Description

spare	(Optional) Reserves spare sectors as specified by the *spare-number* argument when you format flash memory.
spare-number	(Optional) Number of the spare sectors to reserve in formatted flash memory. Valid values are from 0 to 16. The default value is 0.
filesystem1 **:**	Flash memory to format, followed by a colon. Valid values for use with the Cisco 7600 series router are **disk0: disk1:**, **bootflash:**, **slot0:**, **sup-slot0:**, and **sup-bootflash:**; see the "Usage Guidelines" section for additional information. Valid values for use with the ASR 1000 Series Routers are **bootflash:**, **harddisk:**, **stby-harddisk:**, **obfl:**, and **usb**[**0 1**]**;**.
filesystem2 **:**	(Optional) File system containing the monlib file to use for formatting the argument *filesystem1*followed by a colon.
monlib-filename	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the *filesystem1*argument. The default monlib file is the one bundled with the system software. Dual Route Switch Processors (RSP) High System Availability (HSA) Functionality When this command is used with Dual RSPs and you do not specify the *monlib-filename*argument, the system takes the ROM monitor library file from the secondary image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the secondary devices.

Command Default

spare-number : 0*monlib-filename:*The monlib file bundled with the system software

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(14)T	Support for Class B flash (USB flash and USB eToken) file systems was added as part of the USB Storage feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced: • This command was introduced in diagnostic mode for the first time. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers. • The **harddisk:**, **obfl:**, **stby-harddisk:**, **stby-usb**[**0-1**]**:** and **usb[0-1]:** *filesystem1* **:** options were introduced.
12.2YST	This command was integrated into Cisco IOS Release 12.2YST.

Usage Guidelines

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the flash memory card can still be used. Otherwise, you must reformat the flash card after some of the sectors fail.

Use this command to format Class A, B, or C flash memory file systems. The Cisco 7600 series router supports only Class A and Class C flash file systems.

In some cases, you might need to insert a new Personal Computer Memory Card Industry Association (PCMCIA) flash memory or flash PC card and load images or backup configuration files onto it. Before you can use a new flash memory or flash PC card, you must format it.

Sectors in flash memory or flash PC cards can fail. Reserve certain flash memory or flash PC sectors as "spares" by using the optional spare-number argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the flash memory or flash PC card. If you specify 0 spare sectors and some sectors fail, you must reformat the flash memory or flash PC card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the flash file system. The Cisco IOS system software contains a monlib file. Use the **show disk0: all**command to display monlib file details.

When this command is used with HSA and you do not specify the *monlib-filename argument*, the system takes the ROM monitor library file from the secondary image bundle. If you specify the *monlib-filename argument*, the system assumes that the files reside on the secondary devices.

In the command syntax, the *filesystem1* **:**argumentspecifies the device to format and the *filesystem2* **:**argumentspecifies the optional device containing the monlib file used to format the *filesystem1* **:**argument. The device determines which monlib file to use, as follows:

- If you omit the optional *filesystem2* **:** and *monlib-filename* arguments, the system formats the *filesystem1* **:** argument using the monlib file already bundled with the system software.
- If you omit only theoptional *filesystem2* **:** argument, the system formats the *filesystem1* **:** argumentusing the monlib file from the device you specified with the **cd** command.
- If you omit only the optional *monlib-filename* argument, the system formats *filesystem1* **:** using the *filesystem2* **:** monlib file.
- When you specify both arguments--*filesystem2* **:** and *monlib-filename*-- the system formats the *filesystem1* **:** argumentusing the monlib file from the specified device.
- You can specify the *filesystem1* **:**arguments's own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

Note Most platforms do not support booting from images stored on flash memory cards . You should reboot your device only from integrated memory locations, such as NVRAM.

Cisco 7600 Series Router Notes

The **bootflash:**, **slot0:**, **sup-slot0:**, and **sup-bootflash:** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Use the **format** command to format Class A or C flash memory file systems.

- The **disk0:** and **disk1:** keywords are for Class C file systems.
- The **bootflash:**, **slot0:**, **sup-slot0:**, and **sup-bootflash:** keywords are for Class A file systems.

The **disk0:** keyword is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

Cisco ASR 1000 Series Routers Notes

This command is available in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 Series Routers.

Examples

The following example shows how to format a flash memory card that is inserted in slot 0:

```
Router# format slot0:
Running config file on this device, proceed? [confirm] y
All sectors will be erased, proceed? [confirm] y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the privileged EXEC prompt, the new flash memory card is formatted and ready for use.

This following example shows how to format a CompactFlash PC card that is inserted in slot 0:

```
Router# format disk0:
Running config file on this device, proceed? [confirm] y
All sectors will be erased, proceed? [confirm] y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device disk0 completed
When the console returns to the EXEC prompt, the new CompactFlash PC card is formatted and
 ready for use.
```

This follwing example shows how a format operation cleans up the disk and writes the monitor library on the disk filesystem:

```
Router# format formatdisk:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "bootdisk:".  Continue? [confirm]
Hash Computation:    100%Done!
Computed Hash   SHA2: DFBA87256310DC8A7B7BF8158451F7F4
                      0AC333C9B396D9D0E42DDBD542C30E08
                      F3946DDE692AF04F0B20F29BE51C49C4
                      1B631790A542D81F9A7C90ABC2426960
```

```
Embedded Hash   SHA2: DFBA87256310DC8A7B7BF8158451F7F4
                      0AC333C9B396D9D0E42DDBD542C30E08
                      F3946DDE692AF04F0B20F29BE51C49C4
                      1B631790A542D81F9A7C90ABC2426960

Digital signature successfully verified in file Monlib
Writing Monlib sectors....
Monlib write complete
Format: All system sectors written. OK...
Format: Total sectors in formatted partition: 1000881
Format: Total bytes in formatted partition: 512451072
Format: Operation completed successfully.
Format of bootdisk: complete
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
delete	Deletes a file on a flash memory device.
show disk0: all	Displays ATA MONLIB file information for disk0.
show file systems	Lists available file systems.
squeeze	Permanently deletes flash files by squeezing a Class A flash file system.
undelete	Recovers a file marked “deleted” on a Class A or Class B flash file system.

fsck

To check a File Allocation Table (FAT)-based disk, a flash file system, or a Class C file system for damage and to repair any problems, use the **fsck**command in privileged EXEC or diagnostic mode.

Supported Platforms Other than the Cisco 7600 Series and Cisco ASR1000 Series Routers
fsck [/**nocrc**] [/**automatic**] [/**all**] [/**force**] [*filesystem***:**]

Cisco 7600 Series Routers
fsck [/**automatic**] [/**all**] [/**force**] [*filesystem***:**]

Cisco ASR 1000 Series Routers
fsck [/**all**] [/**force**] [*filesystem***:**]

Syntax Description

/nocrc	(Optional) This keyword is available for Class C flash file systems only. Omits cyclic redundancy checks (CRCs).
/automatic	(Optional) This keyword is available for Advanced Technology Attachment (ATA) FAT-based disks only. Specifies that the check and repair actions should proceed automatically. This option can be used to skip the prompts for each check and repair action. **Note** This command also specifies the automatic mode for the Cisco 7600 series router; see the “Usage Guidelines” section for additional information.

/ all	(Optional) Specifies that all partitions on the disk be checked for problems.
/force	(Optional) Ensures forced termination of simultaneous file operations on the same device.
filesystem **:**	The file system prefix indicating the disk to be checked. The colon (:) is required. Typically, the file system prefix will be **disk0:** or **disk1:**. In case of dual processors, the file system on the redundant supervisor engine can also be specified.

Command Default

A FAT-based disk, flash file system, or Class C file system is not checked for damage and repaired. If you do not enter the **/automatic** keyword, command-line interface (CLI) prompts for actions are issued. For the Cisco 7600 series router, if you do not specify the **disk0:** keyword, the current file system is checked.

This command is available in both privileged EXEC and diagnostic mode on the Cisco ASR1000 series routers.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
11.3 AA	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7000 family of routers and on the Cisco 10000 series router and the Gigabit Switch Router (GSR) to support ATA disks.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)SX	This command was modified. Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers and the following enhancements were introduced: • This command was introduced in diagnostic mode for the first time. The command can be entered in both privileged EXEC and diagnostic mode on the Cisco ASR 1000 series routers. • The **/all** option was introduced. • The **harddisk:**, **obfl:**, **stby-harddisk:**, **stby-usb**[**0**-**1**]**:**,and **usb**[**0**-**1**]**:** *filesystem* **:** options were introduced.
15.0(1)M	This command was modified. The **/force** keyword was added.

Usage Guidelines

Supported Platforms Other than Cisco 7600 Series Router

This command performs all steps necessary to remove corrupted files and reclaim unused disk space. Changes include checking for incorrect file sizes, cluster loops, and so on. The default form of this command issues

multiple prompts to confirm each of the changes. However, you can skip these prompts by using the **/automatic** keyword when issuing the command.

When you use the **/automatic**keyword you are prompted to confirm that you want the automatic option. Prompts for actions will be skipped, but all actions performed are displayed to the terminal (see the example below).

This command works with ATA Personal Computer Memory Card Industry Association (PCMCIA) cards formatted in Disk Operating System (DOS), or for Class C flash file systems.

Note Only one partition (the active partition) is checked in the ATA disk.

Cisco 7600 Series Router

The disk0: or slavedisk0: file systems are the only file systems in the Cisco 7600 series routers on which you can run the File-System-Check (fsck) utility. The slavedisk0**:** file system appears in redundant supervisor engine systems only.

This command is valid only on Class C flash file systems and only on PCMCIA ATA flash disks and CompactFlash disks.

The output for the **fsck slavedisk0:** command is similar to the **fsck disk0:** command output.

If you do not enter any arguments, the current file system is used. Use the **pwd** command to display the current file system.

If you enter the **disk0:** or **slavedisk0:** keyword, the fsck utility checks the selected file system for problems. If a problem is detected, a prompt is displayed asking if you want the problem fixed.

If you enter the **/automatic** keyword, you are prompted to confirm that you want the automatic mode. In automatic mode, problems are fixed automatically and you are not prompted to confirm.

If you do not specify the **/force**keyword, any simultaneous file operations on the same device are not terminated. Instead, an error message stating files are open for read or write access appears. If you specify the **/force** keyword, the fsck utility terminates files that are open for read or write access and continues to check for problems.

The table below lists the checks and actions that are performed by the fsck utility.

Table 1: fsck Utility Checks and Actions

Checks	Actions
Checks the boot sector and the partition table and reports the errors.	No action.
Validates the media with the signature in the last 2 bytes of the first sector (0x55 and 0xaa, respectively).	No action.
Checks the os_id to find whether this is a FAT-12 or FAT-16 file system (valid values include 0, 1, 4, and 6).	No action.
Checks the number of FAT's field (correct values are 1 and 2).	No action.

Checks	Actions
Checks these values: • n_fat_sectors cannot be less than 1. • n_root_entries cannot be less than 16. • n_root_sectors cannot be less than 2. • base_fat_sector, n_sectors_per_cluster, n_heads, n_sectors_per_track is not 0.	No action.
Checks the files and FAT for these errors:	
Checks the FAT for invalid cluster numbers.	If the cluster is a part of a file chain, the cluster is changed to end of file (EOF). If the cluster is not part of a file chain, it is added to the free list and unused cluster chain. The table below lists valid cluster numbers; numbers other than those listed in the table below are invalid numbers.
Checks the file's cluster chain for loops.	If the loop is broken, the file is truncated at the cluster where the looping occurred.
Checks the directories for nonzero size fields.	If directories are found with nonzero size fields, the size is reset to zero.
Checks for invalid start cluster file numbers.	If the start cluster number of a file is invalid, the file is deleted.
Checks files for bad or free clusters.	If the file contains bad or free clusters, the file is truncated at the last good cluster; an example is the cluster that points to this bad/free cluster.
Checks to see if the file's cluster chain is longer than indicated by the size fields.	If the file's cluster chain is longer than indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if two or more files share the same cluster (crosslinked).	If two or more files are crosslinked, you are prompted to accept the repair, and one of the files is truncated.
Checks to see if the file's cluster chain is shorter than is indicated by the size fields.	If the file's cluster chain is shorter than is indicated by the size fields, the file size is recalculated and the directory entry is updated.
Checks to see if there are any unused cluster chains.	If unused cluster chains are found, new files are created and linked to that file with the name fsck-*start cluster*

The table below lists the valid cluster numbers. Numbers other than those listed in the table below are invalid numbers.

Table 2: Valid Cluster Numbers

Cluster	FAT-12	FAT-16
Next entry in the chain	2-FEF	2-FFEF
Last entry in chain	FF8-FFF	FFF8-FFFF

Cluster	FAT-12	FAT-16
Available cluster	0	0
Bad Cluster	FF7	FFF7

Examples

Supported Platforms Other than the Cisco 7600 Series Router

The following example shows sample output from the **fsck** command in automatic mode:

```
Router# fsck /automatic disk1:
Proceed with the automatic mode? [yes] y
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
Start cluster of file disk1:/file1 is invalid, removing file
File disk1:/file2 has a free/bad cluster, truncating...
File disk1:/file2 truncated.
File disk1:/file3 has a free/bad cluster, truncating...
File disk1:/file3 truncated.
File disk1:/file4 has a invalid cluster, truncating...
File disk1:/file4 truncated.
File disk1:/file5 has a invalid cluster, truncating...
File disk1:/file5 truncated.
File disk1:/file6 has a invalid cluster, truncating...
File disk1:/file6 truncated.
File size of disk1:/file7 is not correct, correcting it
File disk1:/file8 cluster chain has a loop, truncating it
File disk1:/file8 truncated.
File disk1:/file9 cluster chain has a loop, truncating it
File disk1:/file9 truncated.
File disk1:/file16 has a free/bad cluster, truncating...
File disk1:/file16 truncated.
File disk1:/file20 has a free/bad cluster, truncating...
File disk1:/file20 truncated.
Reclaiming unused space...
Created file disk1:/fsck-4 for an unused cluster chain
Created file disk1:/fsck-41 for an unused cluster chain
Created file disk1:/fsck-73 for an unused cluster chain
Created file disk1:/fsck-106 for an unused cluster chain
Created file disk1:/fsck-121 for an unused cluster chain
Created file disk1:/fsck-132 for an unused cluster chain
Created file disk1:/fsck-140 for an unused cluster chain
Created file disk1:/fsck-156 for an unused cluster chain
Created file disk1:/fsck-171 for an unused cluster chain
Created file disk1:/fsck-186 for an unused cluster chain
Created file disk1:/fsck-196 for an unused cluster chain
Created file disk1:/fsck-235 for an unused cluster chain
Created file disk1:/fsck-239 for an unused cluster chain
Updating FAT...
fsck of disk1: complete
```

Cisco 7600 Series Router

This example shows how to run a check of the current file system:

```
Router# fsck
```

```
 Checking the boot sector and partition table...
 Checking FAT, Files and Directories...
 Files
 1) disk0:/FILE3 and
 2) disk0:/FILE2
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] q
 Ignoring this error and continuing with the rest of the check...
 Files
 1) disk0:/FILE5 and
 2) disk0:/FILE4
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] 1
 File disk0:/FILE5 truncated.
 Files
 1) disk0:/FILE7 and
 2) disk0:/FILE6
 have a common cluster.
.
.
.
1) disk0:/FILE15 and
 2) disk0:/FILE13
 have a common cluster.
 Press 1/2 to truncate or any other character to ignore[confirm] i
 Ignoring this error and continuing with the rest of the check...
 Reclaiming unused space...
 Created file disk0:/fsck-11 for an unused cluster chain
 Created file disk0:/fsck-20 for an unused cluster chain
 Created file disk0:/fsck-30 for an unused cluster chain
 Created file disk0:/fsck-35 for an unused cluster chain
 Created file disk0:/fsck-40 for an unused cluster chain
 Created file disk0:/fsck-46 for an unused cluster chain
 Created file disk0:/fsck-55 for an unused cluster chain
 Created file disk0:/fsck-62 for an unused cluster chain
 Created file disk0:/fsck-90 for an unused cluster chain
 Updating FAT...
 fsck of disk0: complete
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
pwd	Shows the current setting of the **cd** command.

full-help

To get help f or the full set of user-level commands, use the f**ull-help** command in line configuration mode.

full-help

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Line configuration

Command History

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

Usage Guidelines

The **full-help** command enables (or disables) an unprivileged user to see all of the help messages available. It is used with the **show ?** command.

Examples

In the following example, the **show ?** command is used first with full-help disabled. Then **full-help** is enabled for the line, and the **show ?** command is used again to demonstrate the additional help output that is displayed.

```
Router> show ?
  bootflash  Boot Flash information
  calendar   Display the hardware calendar
  clock      Display the system clock
  context    Show context information
  dialer     Dialer parameters and statistics
  history    Display the session command history
  hosts      IP domain-name, lookup style, nameservers, and host table
  isdn       ISDN information
  kerberos   Show Kerberos Values
  modemcap   Show Modem Capabilities database
  ppp        PPP parameters and statistics
  rmon       rmon statistics
  sessions   Information about Telnet connections
  snmp       snmp statistics
  terminal   Display terminal configuration parameters
  users      Display information about terminal lines
  version    System hardware and software status
Router> enable
Password:<letmein>


Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# line console 0
Router(config-line)# full-help
Router(config-line)# exit

Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# disable
Router> show ?
  access-expression  List access expression
  access-lists       List access lists
  aliases            Display alias commands
  apollo             Apollo network information
  appletalk          AppleTalk information
  arp                ARP table
  async              Information on terminal lines used as router interfaces
  bootflash          Boot Flash information
  bridge             Bridge Forwarding/Filtering Database [verbose]
  bsc                BSC interface information
  bstun              BSTUN interface information
  buffers            Buffer pool statistics
  calendar           Display the hardware calendar
 .
```

```
.
.
translate          Protocol translation information
ttycap             Terminal capability tables
users              Display information about terminal lines
version            System hardware and software status
vines              VINES information
vlans              Virtual LANs Information
whoami             Info on current tty line
x25                X.25 information
xns                XNS information
xremote            XRemote statistics
```

Related Commands

Command	Description
help	Displays a brief description of the help system.

help

To display a brief description of the help system, use the **help** command in any command mode.

help

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

All configuration modes

Command History

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

Usage Guidelines

The **help** command provides a brief description of the context-sensitive help system, which functions as follows:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called *word help* , because it lists only the keywords or arguments that begin with the abbreviation you entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called *command syntax help* , because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

Examples

In the following example, the **help** command is used to display a brief description of the help system:

```
Router#
 help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

The following example shows how to use word help to display all the privileged EXEC commands that begin with the letters "co." The letters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command.

```
Router# co?
configure  connect  copy
Router# co
```

The following example shows how to use command syntax help to display the next argument of a partially complete **access-list** command. One option is to add a wildcard mask. The <cr> symbol indicates that the other option is to press Enter to execute the command without adding any more keywords or arguments. The characters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command or to execute that command as it is.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
  A.B.C.D  Mask of bits to ignore
  <cr>
Router(config)# access-list 99 deny 131.108.134.234
```

Related Commands

Command	Description
full-help	Enables help for the full set of user-level commands for a line.

hidekeys

To suppress the display of password information in configuration log files, use the **hidekeys** command in configuration change logger configuration mode. To allow the display of password information in configuration log files, use the **no** form of this command.

hidekeys
no hidekeys

Syntax Description

This command has no arguments or keywords.

Command Default

Password information is displayed.

Command Modes

Configuration change logger configuration (config-archive-log-config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Enabling the **hidekeys** command increases security by preventing password information from being displayed in configuration log files.

Examples

The following example shows how to prevent password information from being displayed in configuration log files:

```
Device# configure terminal
!
Device(config)# archive
Device(config-archive)# log config
Device(config-archive-log-config)# hidekeys
Device(config-archive-log-config)# end
```

Related Commands

Command	Description
archive	Enters archive configuration mode.
log config	Enters configuration change logger configuration mode.
logging enable	Enables the logging of configuration changes.
logging size	Specifies the maximum number of entries retained in the configuration log.
notify syslog	Enables the sending of notifications of configuration changes to a remote syslog.
show archive log config	Displays entries from the configuration log.

history

To enable the command history function, use the **history** command in line configuration mode. To disable the command history function, use the **no** form of this command.

history

no history

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled with ten command lines in the buffer.

Command Modes

Line configuration

Command History

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

Usage Guidelines

The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists.

To change the number of command lines that the system will record in its history buffer, use the **history size** line configuration command.

The **history** command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The **no history** command disables the history function.

The **show history** EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. The table below lists the keys you can use to recall commands from the command history buffer.

Table 3: History Keys

Key(s)	Functions
Ctrl-P or Up Arrow[1]	Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or Down Arrow1	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands.

[1] The arrow keys function only with ANSI-compatible terminals.

Examples

In the following example, the command history function is disabled on line 4:

```
Router(config)# line 4

Router(config-line)# no history
```

Related Commands

Command	Description
history size	Sets the command history buffer size for a particular line.
show history	Lists the commands you have entered in the current EXEC session.

Command	Description
terminal history	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

history size

To change the command history buffer size for a particular line, use the **history size** command in line configuration mode. To reset the command history buffer size to ten lines, use the **no** form of this command.

history size *number-of-lines*
no history size

Syntax Description

number-of-lines	Specifies the number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10.

Command Default

10 command lines

Command Modes

Line configuration

Command History

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

Usage Guidelines

The **history size** command should be used in conjunction with the **history** and **show history** commands. The **history** command enables or disables the command history function. The **show history** command lists the commands you have entered in the current EXEC session. The number of commands that the history buffer will show is set by the **history size** command.

Note The **history size** command only sets the size of the buffer; it does not reenable the history function. If the **no history** command is used, the **history** command must be used to reenable this function.

Examples

The following example displays line 4 configured with a history buffer size of 35 lines:

```
Router(config)# line 4
Router(config-line)# history size 35
```

Related Commands

Command	Description
history	Enables or disables the command history function.
show history	Lists the commands you have entered in the current EXEC session.

Command	Description
terminal history size	Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session.

hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** command in line configuration mode. To restore the default, use the **no** form of this command.

hold-character *ascii-number*
no hold-character

Syntax Description

ascii-number	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

Command Default

No hold character is defined.

Command Modes

Line configuration

Command History

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

Usage Guidelines

The Break character is represented by zero; NULL cannot be represented. To continue the output, enter any character after the hold character. To use the hold character in normal communications, precede it with the escape character. See the "ASCII Character Set" appendix for a list of ASCII characters.

Examples

The following example sets the hold character to Ctrl-S, which is ASCII decimal character 19:

```
Router(config)# line 8
Router(config-line)# hold-character 19
```

Related Commands

Command	Description
terminal hold-character	Sets or changes the hold character for the current session.

hostname

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

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M4	This command was integrated into Cisco IOS Release 15.0(1)M4 and support for numeric hostnames added.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example changes the hostname to “host1”:

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

Related Commands

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

hw-module reset

To reset a module by turning the power off and then on, use the **hw-module reset** command in privileged EXEC mode.

hw-module module *num* **reset**

Syntax Description

module *num*	Applies the command to a specific module; see the “Usage Guidelines” section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The *num* argument designates the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to reload a specific module:

```
Router#
hw-module module 3 reset
```

hw-module shutdown

To shut down the module, use the **hw-module shutdown** command in privileged EXEC mode.

hw-module module *num* **shutdown**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command is supported on the SSL Services Module and the NAM.

If you enter the hw-module **shutdown**command to shut down the module, you will have to enter the no power enable module command and the **power enable module** command to restart (power down and then power up) the module.

Examples

This example shows how to shut down and restart the module:

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

insecure

To configure a line as insecure, use the **insecure** command in line configuration mode. To disable this function, use the **no** form of this command.

insecure
no insecure

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes Line configuration

Command History

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

Usage Guidelines Use this command to identify a modem line as insecure for DEC local area transport (LAT) classification.

Examples In the following example, line 10 is configured as an insecure dialup line:

```
Router(config)# line 10
Router(config-line)# insecure
```

install

To install Software Maintenance Upgrade (SMU) packages, use the **install** command in privileged EXEC mode.

install {**abort** | **activate** | **file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} [{**auto-abort-timer timer** *timer* **prompt-level** {**all** | **none**}}] | **add file** {**bootflash:** | **flash:** | **ftp:** | **harddisk:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **tftp:** | **webui:**} [{**activate** [{**auto-abort-timer** *timer* **prompt-level** {**all** | **none**}**commit**}]}] | **commit** | **auto-abort-timer stop** | **deactivate file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **label** *id*{**description** *description* | **label-name** *name*} | **remove** {**file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **inactive** } | **rollback to** {**base** | **committed** | **id** {*install-ID* } | **label**{*label-name*}}}

Syntax Description

abort	Aborts the current install operation.
activate	Validates whether the SMU is added through the install add command. This keyword runs a compatibility check, updates package status, and if the package can be restarted, it triggers post-install scripts to restart the necessary processes, or triggers a reload for non-restartable packages.
file	Specifies the package to be activated.
{**bootflash:** | **flash:** | **harddisk:** | **webui:**}	Specifies the location of the installed package.
auto-abort-timer *timer*	(Optional) Installs an auto-abort timer. The timer is set by the **activate** keyword and removed by the **commit** keyword. After the expiry of the **install auto-abort timer** command, a device can be rolled back to a stage before the **install commit** command is used.

prompt-level {**all** | **none**}	(Optional) Prompts the user about installation activities. For example, the **activate** keyword, automatically triggers a reload for packages that require a reload. Before activating the package, a message will prompt users as to whether they want to continue. The **all** keyword allows you to enable prompts. The **none** keyword disable prompts.
add	Copies files from a remote location (via FTP, TFTP) to a device and performs Software Maintenance Upgrade (SMU) compatibility check for the platform and image versions. This keyword runs base compatibility checks to ensure that a specified package is supported on a platform. It also adds an entry in the package file, so that the status can be monitored and maintained.
{ **bootflash:** | **flash:** |**ftp:** |**harddisk:** |**http:** |**https:** | **pram:** |**rcp:** | **scp:** | **tftp:** |**webui:**}	Specifies the package to be added.
commit	Makes SMU changes persistent over reloads. You can do a commit after activating a package, while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.
auto-abort-timer stop	Stops the auto-abort timer. If the roll back timer is not stopped through the command, the device rolls back to an older software version when rollback timer expires. Default:120 minutes.
deactivate	Deactivates an installed package. Deactivating a package also updates the package status and triggers a process restart or a reload.
label *id*	Specifies the id of the install point to label.
description	Adds a description to specified install point.
label-name *name*	Adds a description to specified install point.
remove	Remove installed packages. The package file is removed from the file system. The **remove** keyword can only be used on packages that are currently inactive.
inactive	Removes all inactive packages from the device.

rollback	Rollbacks the SMU package to the base version, the last committed version, or a known commit ID.
to base	Returns to the base image.
committed	Returns to the installation state when the last commit operation was performed.
id *install-ID*	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

Command Default

Packages are not installed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.6.1	This command was introduced.

Usage Guidelines

An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package contain a minimal set of files for patching the release along with some metadata that describes the contents of the package.

Packages must be added prior to activating the SMU.

A package must be deactivated, before it is removed from the device.

Example

The following example shows how to add an install package on a device:

```
Device# install add file tftp://172.16.0.1//tftpboot/folder1/isr4300-
universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin

install_add: START Sun Feb 26 05:57:04 UTC 2017
Downloading file tftp://172.16.0.1//tftpboot/folder1/isr4300-universalk9.2017-01-10_13.15.1.
CSCvb12345.SSA.dmp.bin
Finished downloading file
tftp://172.16.0.1//tftpboot/folder1/isr4300-universalk9.2017-01-10_13.15.1.
CSCvb12345.SSA.dmp.bin to
bootflash:isr4300-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
SUCCESS: install_add /bootflash/isr4300-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin

Sun Feb 26 05:57:22 UTC 2017
```

The following example shows how to activate an install package:

```
Device# install activate file bootflash:isr4300-universalk9.2017-01-10_13.15.1.
CSCxxx.SSA.dmp.bin

install_activate: START Sun Feb 26 05:58:41 UTC 2017
DMP package.
Netconf processes stopped
SUCCESS: install_activate
/bootflash/isr4300-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:58:58 UTC 2017
```

```
*Feb 26 05:58:47.655: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:58:47.661: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.
*Feb 26 05:58:47.667: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:59:43.269: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 05:59:44.624: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
```

The following example shows how to commit an installed package:

```
Device# install commit

install_commit: START Sun Feb 26 06:46:48 UTC 2017
SUCCESS: install_commit  Sun Feb 26 06:46:52 UTC 2017
```

The following example shows how to rollback to the base SMU package:

```
Device# install rollback to base

install_rollback: START Sun Feb 26 06:50:29 UTC 2017
7 install_rollback: Restarting impacted processes to take effect
7 install_rollback: restarting confd

*Feb 26 06:50:34.957: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.962: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.963: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.Netconf processes stopped
7 install_rollback: DMP activate complete
SUCCESS: install_rollback  Sun Feb 26 06:50:41 UTC 2017
*Feb 26 06:51:28.901: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 06:51:30.339: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
```

Related Commands

Command	Description
show install	Displays information about install packages.

international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[), use the **international** command in line configuration mode. To display characters in 7-bit format, use the **no** form of this command.

international
no international

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes Line configuration

Command History

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

Usage Guidelines If you are configuring a Cisco IOS platform using the Cisco web browser user interface (UI), this function is enabled automatically when you enable the Cisco web browser UI using the **ip http server** global configuration command.

Examples The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[) when you are using Telnet to access the platform:

```
line vty 4
 international
```

Related Commands

Command	Description
terminal international	Prints the Escape character as a single character instead of as the caret and bracket symbols (^[) for a current Telnet session in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji).

ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

ip bootp server
no ip bootp server

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
12.0(1)T	The DHCP relay agent and DHCP server features were introduced. BOOTP forwarding is now handled by the DHCP relay agent implementation.
12.2(8)T	The **ip dhcp bootp ignore** command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, the BOOTP service is enabled. When disabled, the **no ip bootp server** command will appear in the configuration file.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is based on BOOTP, both of these services share the "well-known" UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131; the client port is 68). To disable DHCP services (DHCP relay and DHCP server), use the **no service dhcp** command. To disable BOOTP services (in releases 12.2(8)T and later), but leave DHCP services enabled, use the **ip dhcp bootp ignore** command.

If both the BOOTP server and DHCP server are disabled, "ICMP port unreachable" messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded. If DHCP is enabled, using the **no ip bootp server** command by itself will not stop the router from listening on UDP port 67.

Note As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network. Any network device that has User Data Protocol (UDP), TCP, BOOTP, DHCP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Examples

In the following example, BOOTP and DHCP services are disabled on the router:

```
Router(config)# no ip bootp server

Router(config)# no service dhcp
```

Related Commands

Command	Description
ip dhcp bootp ignore	Configures the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, allowing you continue using DHCP while disabling BOOTP.
service dhcp	Enables the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent features.

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no**form of this command.

ip finger [**rfc-compliant**]
no ip finger

Syntax Description

rfc-compliant	(Optional) Configures the system to wait for "Return" or "/W" input when processing Finger requests. This keyword should not be used for those systems.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(5), 12.1(5)T	This command was changed from being enabled by default to being disabled by default.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The Finger service allows remote users to view the output equivalent to the **show users** [**wide**] command.

When **ip finger** is configured, the router will respond to a **telnet** *a.b.c.d* **finger** command from a remote host by immediately displaying the output of the **show users**command and then closing the connection.

When the **ip finger rfc-compliant**commandis configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the **show users** EXEC command, or enter **/W** to display the output of the **show users wide** EXEC command. After this information is displayed, the connection is closed.

Note As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network. Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the **rfc-compliant**form of this command should not be configured for devices with more than 20 simultaneous users.

Examples

The following example disables the Finger protocol:

```
Router(config)# no ip finger
```

ip ftp passive

To configure the router to use only passive FTP connections, use the **ip ftp passive**command in global configuration mode . To allow all types of FTP connections, use the **no**form of this command.

ip ftp passive
no ip ftp passive

Syntax Description This command has no arguments or keywords.

Command Default All types of FTP connections are allowed.

Command Modes Global configuration

Command History

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

Examples In the following example, the router is configured to use only passive FTP connections:

```
Router(config)# ip ftp passive
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp password

To specify the password to be used for File Transfer Protocol (FTP) connections, use the **ip ftp password**command in global configuration mode. To return the password to its default, use the **no** form of this command.

ip ftp password [*type*] *password*
no ip ftp password

Syntax Description

type	(Optional) Type of encryption to use on the password. A value of 0 disables encryption. A value of 7 indicates proprietary encryption.
password	Password to use for FTP connections.

Command Default The router forms a password *username@routername.domain*. The variable *username* is the username associated with the current session, *routername* is the configured host name, and *domain* is the domain of the router.

Command Modes Global configuration

Command History

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

Note Any software that supports RFC1738 does not allow user name, path, or filename with pattern %xy, where (where x and y are any two hexa values 0-f, 0-F)

Examples

The following example configures the router to use the username “red” and the password “blue” for FTP connections:

```
Router(config)# ip ftp username red

Router(config)# ip ftp password blue
```

Related Commands

Command	Description
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ip ftp source-interface**command in global configuration mode. To use the address of the interface where the connection is made, use the **no** form of this command.

ip ftp source-interface *interface-type interface-number*
no ip ftp source-interface

Syntax Description

interface-type interface-number	The interface type and number to use to obtain the source address for FTP connections.

Command Default

The FTP source address is the IP address of the interface that the FTP packets use to leave the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.3(6)	Destination address lookup in a Virtual Private Network (VPN) routing and forwarding (VRF) table was added for the transfer of FTP packets.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to set the same source address for all FTP connections.

In Cisco IOS 12.3(6) and later releases, FTP is VRF-aware, which means that FTP transfer is supported across an interface within a VRF instance. To specify a VRF as a source for FTP connections, the VRF must be associated with the same interface that you configure with the **ip ftp source-interface** command. In this configuration, FTP looks for the destination IP address for file transfer in the specified VRF table. If the specified source interface is not up, Cisco IOS software selects the address of the interface closest to the destination as the source address.

Examples

The following example shows how to configure the router to use the IP address associated with Ethernet interface 0 as the source address on all FTP packets, regardless of which interface is actually used to send the packet:

```
Router> enable
Router# configure terminal
Router(config)# ip ftp source-interface ethernet 0
```

The following example shows how to configure the router to use the VRF table named vpn1 to look for the destination IP address for the transfer of FTP packets:

```
Router# configure terminal
Router(config)# ip ftp source-interface ethernet 0
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 200:1
Router(config-vrf)# route-target both 200:1
Router(config-vrf)# interface ethernet 0
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# end
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

ip ftp username

To configure the username for File Transfer Protocol (FTP) connections, use the **ip ftp username**command in global configuration mode . To configure the router to attempt anonymous FTP, use the **no**form of this command.

ip ftp username *username*
no ip ftp username

Syntax Description

username	Username for FTP connections.

Command Default

The Cisco IOS software attempts an anonymous FTP.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

In the following example, the router is configured to use the username “red” and the password “blue”for FTP connections:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

Related Commands

Command	Description
ip ftp passive	Configures the router to use only passive FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp source-interface	Specifies the source IP address for FTP connections.

ip rarp-server

To enable the router to act as a Reverse Address Resolution Protocol (RARP) server, use the **ip rarp-server** command in interface configuration mode. To restore the interface to the default of no RARP server support, use the **no**form of this command.

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.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

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 router does not interfere with RARP traffic on subnets that need no RARP assistance.

The Cisco IOS software answers incoming RARP requests only if both of the following two conditions are met:

- The **ip rarp-server** command has been configured for the interface on which the request was received.
- A static entry is 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 it's workstations. By bridging RARP packets and using both the **ip helper-address** interface configuration command and the **ip forward-protocol** global configuration command, the Cisco IOS software shouldbe 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 router, is the host that the client can contact to TFTP load the bootstrap image. This causes the workstations to fail to boot.

By using the **ip rarp-server** command, the Cisco IOS software 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 router 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 Cisco IOS software must 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 following form:

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

RFC 903 documents the RARP.

Examples

The following partial example configures a router to act as a RARP server. The router 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, a router is configured to act as a RARP server, with TFTP and portmapper requests forwarded to the Sun server:

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
```

```
interface ethernet 0
! Configure the router 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

Command	Description
ip forward-protocol	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip rcmd domain-lookup

To reena ble the basic Domain Name Service (DNS) security check for rcp and rsh, use the **ip rcmd domain-lookup**command in global configuration mode. T o disable the basic DNS security check for remote copy protocol (rcp) and remote shell protoco (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.

Command Default

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The abbreviation RCMD (remote command) is used to indicate both rsh and rcp.

DNS lookup for RCMD is enabled by default (provided general DNS services are enabled on the system using the **ip domain-lookup**command).

The **no ip rcmd domain-lookup** command is used to disable the DNS lookup for RCMD. The **ip rcmd domain-lookup** command is used to reenable the DNS lookup for RCMD.

DNS lookup for RCMD is performed as a basic security check. This check is performed using a host authentication process. When enabled, the system records the address of the requesting client. That address is mapped to a host name using DNS. Then a DNS request is made for the IP address for that host name. The IP address received is then checked against the original requesting address. If the address does not match with any of the addresses received from DNS, the RCMD request will not be serviced.

This reverse lookup is intended to help protect against spoofing. However, please note that the process only confirms that the IP address is a valid “routable” address; it is still possible for a hacker to spoof the valid IP address of a known host.

The DNS lookup is done after the TCP handshake but before the router (which is acting as a rsh/rcp server) sends any data to the remote client.

The **no ip rcmd domain-lookup** 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. This means that if the **no ip domain-lookup** command is in the current configuration, DNS will be bypassed for rcp and rsh even if the **ip rcmd domain-lookup** command is enabled.

Examples

In the following example, the DNS security check is disabled for RCMD (rsh/rcp):

```
Router(config)# no ip rcmd domain-lookup
```

Related Commands

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.

ip rcmd rcp-enable

To configure the Cisco IOS software to allow remote users to copy files to and from the router using remote copy protocol (rcp), use the **ip rcmd rcp-enable** command in global configuration mode. To disable rcp on the device, use the **no** form of this command.

ip rcmd rcp-enable
no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

To allow a remote user to execute rcp commands on the router, you must also create an entry for the remote user in the local authentication database using the **ip rcmd remote-host** command.

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 router.

To protect against unauthorized users copying the system image or configuration files, the router is not enabled for rcp by default.

Examples

In the following example, the rcp service is enabled on the system, the IP address assigned to the Loopback0 interface is used as the source address for outbound rcp and rsh packets, and access is granted to the user “netadmin3”on the remote host 172.16.101.101:

```
Router(config)# ip rcmd rcp-enable

Router(config)# ip rcmd source-interface Loopback0

Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd remote-host

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using remote shell protocol (rsh) or remote copy protocol (rcp), use the **ip rcmd remote-host** command in global configuration mode. To remove an entry for a remote user from the local authentication database, use the **no** form of this command.

ip rcmd remote-host *local-username* {*ip-addresshost-name*} *remote-username* [**enable** [*level*]]
no ip rcmd remote-host *local-username* {*ip-addresshost-name*} *remote-username* [**enable** [*level*]]

Syntax Description

local-username	Name of the user on the local router. You can specify the router name as the username. This name needs to be communicated to the network administrator or to the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
ip-address	IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
host-name	Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
remote-username	Name of the user on the remote host from which the router will accept remotely executed commands.
enable [*level*]	(Optional) Enables the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the **privilege level** global configuration command in the *Release 12.2 Cisco IOS Security Command Reference.*

Command Default

No entries are in the local authentication database.

Command Modes

Global configuration

Command History

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

Usage Guidelines

A TCP connection to a router 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 router. 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 router, you must create an entry for the remote user in the local authentication database. You must also enable the router to act as an rsh or rcp server.

To enable the router to act as an rsh server, issue the **ip rcmd rsh-enable** command. To enable the router to act as an rcp server, issue the **ip rcmd rcp-enable** command.The router 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 router 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 or to permit a remote user of rcp to copy files to the router, specify the **enable** keyword and level. For information on the enable level, refer to the **privilege level** global configuration command in the *Release 12.2 Cisco IOS Security Command Reference.*

An entry that you configure in the authentication database differs from an entry in a UNIX *.rhosts*file in the following aspect. 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 need not include the local username; the local username is determined from the user account. To provide equivalent support on a router, 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 router 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, that is, it does not match any address listed with DNS for the host name, then the software will reject the remote-command execution request.

Note that if no DNS servers are configured for the router, then that device cannot authenticate the host in this manner. In this case, the Cisco IOS software sends 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 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 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.

Examples

The following example allows the remote user *named netadmin3* on a remote host with the IP address 172.16.101.101 to execute commands on *router1* using the rsh or rcp protocol. User netadmin3 is allowed to execute commands in privileged EXEC mode.

```
Router(config)# ip rcmd remote-host router1 172.16.101.101 netadmin3 enable
```

Related Commands

Command	Description
ip rcmd rcp-enable	Configures the Cisco IOS software to allow remote users to copy files to and from the router.

Command	Description
ip domain-lookup	Enables the IP DNS-based host name-to-address translation.
ip rcmd rsh-enable	Configures the router to allow remote users to execute commands on it using the rsh protocol.

ip rcmd remote-username

To configure the remote username to be used when requesting a remote copy using remote copy protocol (rcp), use the **ip rcmd remote-username**command in global configuration mode . To remove from the configuration the remote username, use the **no**form of this 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. 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.

Command Default

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

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

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, tty lines are commonly used for access services. The concept of tty originated with UNIX. For UNIX systems, each physical device is represented in the file system. Terminals are called tty devices (tty stands for teletype, the original UNIX terminal).

Command Modes

Global configuration

Command History

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

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. If the server has a

directory structure, as do UNIX systems, all files and images to be copied are searched for or written relative to the directory of the remote user's account.

Note Cisco IOS Release 10.3 added the **ip** keyword to **rcmd** commands. If you are upgrading from Release 10.2 to Release 10.3 or a later release, this keyword is automatically added to any **rcmd** commands you have in your Release 10.2 configuration files.

Examples

The following example configures the remote username to netadmin1:

```
Router(config)# ip rcmd remote-username netadmin1
```

Related Commands

Command	Description
boot network rcp	Changes the default name of the network configuration file from which to load configuration commands.
boot system rcp	Specifies the system image that the router loads at startup.
bridge acquire	Forwards any frames for stations that the system has learned about dynamically.
copy	Copies any file from a source to a destination.

ip rcmd rsh-enable

To configure the router to allow remote users to execute commands on it using remote shell protocol (rsh), use the **ip rcmd rsh-enable** command in global configuration mode. To disable a router that is enabled for rsh, use the **no** form of this command.

ip rcmd rsh-enable
no ip rcmd rsh-enable

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

rsh, used as a client process, gives users the ability to remotely get router information (such as status) without the need to connect into the router and then disconnect. This is valuable when looking at many statistics on many different routers.

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

The **no ip rcmd rsh-enable** command does not prohibit a local user of the router from executing a command on other routers and UNIX hosts on the network using rsh. The no form of this command only disables remote access to rsh on the router.

Examples

The following example enables a router as an rsh server:

```
Router(config)# ip rcmd rsh-enable
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip rcmd source-interface

To force remote copy protocol (rcp) or remote shell protocol (rsh) to use the IP address of a specified interface for all outgoing rcp/rsh communication packets, use the **ip rcmd source-interface** command in global configuration mode. To disable a previously configured **ip rcmd source-interface** command, use the **no** form of this command.

ip rcmd source-interface *interface-id*
no ip rcmd source-interface *interface-id*

Syntax Description

interface-id	The name and number used to identify the interface. For example, Loopback2.

Command Default

The address of the interface closest to the destination is used as the source interface for rcp/rsh communications.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If this command is not used, or if the interface specified in this command is not available (not up), the Cisco IOS software uses the address of the interface closest to the destination as the source address.

Use this command to force the system to tag all outgoing rcp/rsh packets with the IP address associated with the specified interface. This address is used as the source address as long as the interface is in the up state.

This command is especially useful in cases where the router has many interfaces, and you want to ensure that all rcp and/or rsh packets from this router have the same source IP address. A consistent address is preferred

so that the other end of the connection (the rcp/rsh server or client) can maintain a single session. The other benefit of a consistent address is that an access list can be configured on the remote device.

The specified interface must have an IP address associated with it. If the specified interface does not have an IP address or is in a down state, then rcp/rsh reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the up state.

Examples

In the following example, Loopback interface 0 is assigned an IP address of 220.144.159.200, and the **ip rcmd source-interface** command is used to specify that the source IP address for all rcp/rsh packets will be the IP address assigned to the Loopback0 interface:

```
interface Loopback0
description Loopback interface
ip address 220.144.159.200 255.255.255.255
no ip directed-broadcast
!
.
.
.
clock timezone GMT 0
ip subnet-zero
no ip source-route
no ip finger
ip rcmd source-interface Loopback0
ip telnet source-interface Loopback0
ip tftp source-interface Loopback0
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password shhhhsecret
no ip bootp server
ip domain-name net.galaxy
ip name-server 220.144.159.1
ip name-server 220.144.159.2
ip name-server 219.10.2.1
!
.
.
.
```

Related Commands

Command	Description
ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp.

ip telnet source-interface

To specify the IP address of an interface as the source address for Telnet connections, use the **ip telnet source-interface** command in global configuration mode. To reset the source address to the default for each connection, use the **no** form of this command.

ip telnet source-interface *interface*
no ip telnet source-interface

Syntax Description

interface	The interface whose address is to be used as the source for Telnet connections.

Command Default

The address of the closest interface to the destination is the source address.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to set the IP address of an interface as the source for all Telnet connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

Examples

The following example forces the IP address for Ethernet interface 1 as the source address for Telnet connections :

```
Router(config)# ip telnet source-interface Ethernet1
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

ip tftp blocksize

To negotiate a transfer TFTP blocksize, use the **ip tftp blocksize** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip tftp blocksize *bytes*

no ip tftp blocksize

Syntax Description

bytes	Size of the TFTP block, in bytes. The range is from 512 to 8192.

Command Default

The default TFTP blocksize is 512 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2S	This command was introduced for the 12.2S releases.
15.1(1)SG	This command was integrated into the 15.1(1)SG releases.
Cisco IOS XE Release 3.3SE	This command was integrated into the Cisco IOS XE Release 3.3SE releases.

Examples

The following example shows how to set a 1024 byte TFTP blocksize:

```
Router> enable
Router# configure terminal
Router(config)# ip tftp bblocksize 1024
```

Related Commands

Command	Description
ip tftp min-timeout	Specifies the minimum timeout period for retransmission of data.

ip tftp boot-interface

To use an interface for TFTP booting, use the **ip tftp boot-interface**command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip tftp boot-interface *type number*
no ip tftp boot-interface

Syntax Description

type	The type of the interface to be used. You can choose from a list of interfaces.
number	The related interface number. Each interface has a related range of numbers. For example, the Virtual Multipoint Interface has a range of interface numbers from 1 to 2147483647.

Command Default

No interface is used for TFTP booting.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS 15.0(1)M.

Examples

The following example shows how to ensure that an interface is used for TFTP booting:

```
Router> enable
Router# configure terminal
Router(config)# ip tftp boot-interface
```

Related Commands

Command	Description
ip tftp min-timeout	Specifies the minimum timeout period for retransmission of data.

ip tftp min-timeout

To specify the minimum timeout period for retransmission of data using TFTP, use the **ip tftp min-timeout**command in global configuration mode. To disable, use the **no** form of this command.

ip tftp min-timeout *seconds*
no ip tftp min-timeout

Syntax Description

seconds	Specifies the timeout value, in seconds. The range is from 4 to 20.

Command Default

The default minimum timeout period for retransmission of data is 4 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS 15.0(1)M.

Examples

The following example shows how to specify the minimum timeout period for retransmission of data as 5 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip tftp min-timeout 5
```

Related Commands

Command	Description
ip tftp boot-interface	Ensures that an interface is used for TFTP booting.

ip tftp source-interface

To specify the IP address of an interface as the source address for TFTP connections, use the **ip tftp source-interface** command in global configuration mode. To return to the default, use the **no** form of this command.

ip tftp source-interface *interface-type interface-number*

no ip tftp source-interface

Syntax Description

interface-type interface-number	The interface type and number whose address is to be used as the source for TFTP connections.

Command Default

The address of the closest interface to the destination is selected as the source address.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.3(6)	Destination address lookup in a Virtual Private Network (VPN) routing and forwarding (VRF) table was added for the transfer of TFTP packets.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to set the IP address of an interface as the source for all TFTP connections.

If the specified interface is not up, the Cisco IOS software selects the address of the interface closest to the destination as the source address.

In Cisco IOS 12.3(6) and later releases, TFTP is VRF-aware, which means that TFTP transfer is supported across an interface within a Virtual Private Network (VPN) routing and forwarding (VRF) instance. To specify a VRF as a source for TFTP connections, the VRF must be associated with the same interface that you configure with the **ip tftp source-interface** command. In this configuration, TFTP looks for the destination IP address for file transfer in the specified VRF table.

Examples

The following example shows how to configure the router to use the IP address associated with loopback interface 0 as the source address for TFTP connections :

```
Router# configure terminal
Router(config)# ip tftp source-interface loopback0
```

The following example shows how to configure the router to use the VRF table named vpn1 to look for the destination IP address for TFTP connections. In this example, file transfer using TFTP is accomplished across an interface within a VRF (VRF vpn1) link.

```
Router# configure terminal
Router(config)# ip tftp source-interface ethernet 1/0
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target both 100:1
Router(config-vrf)# interface ethernet 1/0
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# end
```

Related Commands

Command	Description
ip ftp source-interface	Forces outgoing FTP packets to use the IP address of a specified interface as the source address.
ip radius source-interface	Forces outgoing RADIUS packets to use the IP address of a specified interface as the source address.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated**command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated [{[**group-address** *groupaddress*] | [**redirect-list** *access-list*] | [**group-list** *access-list*] | [**password** *password*]}]
no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Command Default

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the "I See You" responses for the "Here I Am" messages that it has received

on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.