Configuration Fundamentals Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)

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

CONTENTS

archive tar

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

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

Syntax Description

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

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

Command Default

The TAR archive file is not created.

Command Modes

Privileged EXEC (#)

Command History

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

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

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

boot system

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

Loading System Image from a URL or a TFTP File

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

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

Booting from a System Image in Internal Flash

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

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

Booting from a MOP Server

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

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

Booting from ROM

boot system rom

no boot system rom

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

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

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

Syntax Description

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

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

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

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

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

This section contains the following topics:

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

Changing the List of Boot System Commands

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

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

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

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

Booting Compressed Images

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

Understanding rcp

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

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

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

Understanding TFTP

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

Understanding FTP

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

Stopping Booting and Entering ROM Monitor Mode

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

copy

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

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

Syntax Description

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

destination-url	The destination URL (or alias) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded.

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

The table below shows two keyword shortcuts to URLs.

Table 1 Common Keyword Aliases to URLs

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

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

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

Table 2 URL Prefix Keywords for Special File Systems

Keyword	Source or Destination
cns:	Source URL for Cisco Networking Services files.
flh:	Source URL for flash load helper log files.
logging	Source URL which copies messages from the logging buffer to a file.
modem:	Destination URL for loading modem firmware on to supported networking devices.

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

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

Table 3 URL Prefix Keywords for Remote File Systems

Keyword	Source or Destination
ftp:	Source or destination URL for FTP network server. The syntax for this alias is as follows:**ftp:** [[[//username [:password]@]location]/directory]/ filename.
http://	Source or destination URL for an HTTP server (also called a web server). The syntax for this alias is as follows: http:// [[*username*:*password*]@]{*hostname* | *host-ip*}[/ *filepath*]/ *filename*

Keyword	Source or Destination
https://	Source or destination URL for a Secure HTTP (HTTPS) server. HTTPS uses Secure Socket Layer (SSL) encryption. The syntax for this alias is as follows:**https://**[[*username*:*password*]@] {*hostname* | *host-ip*}[/ *filepath*]/ *filename*
rcp:	Source or destination URL for a remote copy protocol (rcp) network server. The syntax for this alias is as follows:**rcp:**[[[//username@] location]/ directory]/filename
scp:	Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows:**scp://** *username@location*[/*directory*][/*filename*]
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is as follows:**tftp:** [[//location]/directory]/filename.

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

Table 4 URL Prefix Keywords for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of disk-based media.
flash:	Source or destination URL for flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that flash: is aliased to slot0:, allowing you to refer to the main flash memory storage area on all platforms.
harddisk:	Source or destination URL of the active harddisk file system.
slavebootflash:	Source or destination URL for internal flash memory on the slave RSP card of a router configured for HSA.
slaveram:	NVRAM on a slave RSP card of a router configured for HSA.

Alias	Source or Destination
slaveslot0:	Source or destination URL of the first Personal Computer Memory Card International Association (PCMCIA) card on a slave RSP card of a router configured for HSA.
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.
slot0:	Source or destination URL of the first PCMCIA flash memory card.
slot1:	Source or destination URL of the second PCMCIA flash memory card.
stby-bootflash:	Source or destination URL for boot flash memory in standby RP.
stby-harddisk:	Source or destination URL for the standby harddisk.
stby-usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the standby RP.
usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the active RP.
usbflash 0 9 :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router.
usbtoken [**0 9**] :	Source or destination URL for the USB eToken that has been plugged into the router.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
11.3T	This command was introduced.

Release	Modification
12.3(2)T	• The **http://** and **https://** keywords were added as supported remote source locations (file system URL prefixes) for files. • This command was enhanced to support copying files to servers that support SSH and the scp.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)S	The /**verify**and /**noverify** keywords were added.
12.0(26)S	The /**verify**and /**noverify** keywords were integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	The /**verify**and /**noverify** keywords were integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	The **http://** and **https://** keywords were enhanced to support file uploads.
12.3(14)T	The **usbflash 0 9 :**and **usbtoken 0 9 :**keywords were added to support USB storage.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	The Cisco ASR1000 series routers became available, and introduced the **copy** command in diagnostic mode.

Usage Guidelines

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

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

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

Timesaver

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

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

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

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

The following sections contain usage guidelines for the following topics:

Understanding Invalid Combinations of Source and Destination

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

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

Understanding Character Descriptions

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

Table 5 copy Character Descriptions

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

Character	Description
E	An uppercase E indicates an error. The copy process may fail.
V	A series of uppercase Vs indicates the progress during the verification of the image checksum.

Understanding Partitions

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

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

Using rcp

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

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

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

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

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

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

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

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

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

Using FTP

The FTP protocol requires a client to send a username and password with each FTP request to a remote FTP server. Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a

default username and password for all copy operations to or from an FTP server. Include the username in the **copy** command syntax if you want to specify a username for that copy operation only.

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

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

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

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

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

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

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

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

Using HTTP or HTTPS

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

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

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

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

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

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

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

Storing Images on Servers

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

Copying from a Server to Flash Memory

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

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

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

Verifying Images

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

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

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

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

Copying a Configuration File from a Server to the Running Configuration

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

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

Copying a Configuration File from a Server to the Startup Configuration

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

Storing the Running or Startup Configuration on a Server

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

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

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

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

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

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

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

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

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

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

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.

- The BOOTLDR environment variable specifies the flash device and filename containing the rxboot image that ROM uses for booting.
- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the flash memory device and filename that are used as the boot helper; the default is the first system image in flash memory.

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

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

Using the Copy Command with the Dual RSP Feature

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

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

Using the copy command with the ASR1000 Series Routers

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

Examples

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

Verifying the Integrity of the Image Before It Is Copied Example

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

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

```
CCO Hash                          MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

Copying an Image from a Server to Flash Memory Examples

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

Copying an Image from a Server to Flash Memory Example

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

```
Router#
copy rcp://netadmin@172.16.101.101/file1 flash:file1
Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]
Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

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

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

```
Router# copy tftp: flash:

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

Source file name? master/igs-bfpx-100.4.3
```

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

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

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

```
Router# copy rcp: slot0:
PCMCIA Slot0 flash
Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3068K     1027K     4096K      Read/Write     Direct
  2         4096K   1671K     2424K     4096K      Read/Write     Direct
  3         4096K      0K     4095K     4096K      Read/Write     Direct
  4         4096K   3825K      270K     4096K      Read/Write     Direct
[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   3142288  c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz

Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy '/tftpboot/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no]
yes

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

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

Saving a Copy of an Image on a Server Examples

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

Copy an Image from Flash Memory to an rcp Server Example

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

```
Router#
copy flash: rcp:
IP address of remote host [255.255.255.255]? 172.16.13.110
```

```
Name of file to copy? gsxx
writing gsxx - copy complete
```

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

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

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

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

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

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

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

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

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

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

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

```
Router# show slot0: partition 1
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]
```

```
Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)...  OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
  as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

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

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

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

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

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

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

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

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

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

Copying the Running Configuration to a Server Example

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

```
Router# configure terminal

Router(config)# ip rcmd remote-username netadmin1

Router(config)#
```

```
end

Router#
copy system:running-config rcp:

Remote host[]? 172.16.101.101

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

Copying the Startup Configuration to a Server Example

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

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

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

Saving the Current Running Configuration Example

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

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

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

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

Enter no to escape writing the configuration information to memory.

Moving Configuration Files to Other Locations Examples

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

Copying the Startup Configuration to a Flash Memory Device Example

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

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

Copying the Running Configuration to a Flash Memory Device Example

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

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

```
Building configuration...

5267 bytes copied in 0.720 secs
```

Copying to the Running Configuration from a Flash Memory Device Example

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

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

Copying to the Startup Configuration from a Flash Memory Device Example

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

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

Copying a Configuration File from one Flash Device to Another Example

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

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

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

Copying a File from a Remote Web Server Examples

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

```
Router# copy
```

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

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

```
Router# configure terminal

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

Router(config)# end

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

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

```
Router# configure terminal

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

Router(config)# end

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

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

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

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

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
cd	Changes the default directory or file system.
copy xmodem: flash:	Copies any file from a source to a destination.
copy ymodem: flash:	Copies any file from a source to a destination.
delete	Deletes a file on a flash memory device.
dir	Displays a list of files on a file system.
erase	Erases a file system.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.

Command	Description
ip scp server enable	Enables scp server-side functionality.
reload	Reloads the operating system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show (flash file system)	Displays the layout and contents of a flash memory file system.
slave auto-sync config	Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.
verify bootflash:	File system or directory containing the files to list, followed by a colon.

define interface-range

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

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

Syntax Description

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

Command Default

Interface-range macro is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

Examples

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

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

The following example shows how to create multiple loopback interfaces:

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

Related Commands

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

enable

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

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

Syntax Description

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

Command Default

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

Command History

Release	Modification
10.0	This command was introduced.

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

Usage Guidelines

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

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

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

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

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

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

Accessing a CLI View

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

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

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

Examples

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

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

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

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

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

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

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view
```

```
Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all
Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view “first.”
Router# enable view first

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

Related Commands

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

erase

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

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

Cisco 7600 Series Routers and Cisco ASR 1000 Series Routers

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

Syntax Description

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

Command Modes

Privileged EXEC (#) Diagnostic (#)

Command History

Release	Modification
11.0	This command was introduced.

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

Usage Guidelines

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

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

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

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

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

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

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

The **/no-squeeze-reserve-space** keyword is available on systems with small amounts of flash memory in order to conserve memory. When a squeeze operation is performed, the last two erase sectors are permanently reserved for the squeeze logs and squeeze buffer. The **/no-squeeze-reserve-space**keyword prevents the reservation of space that guarantees the ability to run the squeeze command. Disabling the squeeze operation keeps these memory sectors free. If any sectors using squeeze data are detected, they will be erased when the **/no-squeeze-reserve-space** keyword is used. The **/no-squeeze-reserve-space** keyword increases the available amount of usable flash space, but you may not be able to run the **squeeze** command. This is typically fine if the file system (such as flash) is used to store a single, large file. For example, an IOS image.

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

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

Examples

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

```
Router# erase nvram:
```

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

```
Router# erase flash:2

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

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

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

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

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

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
delete	Deletes a file on a flash memory device.

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

errdisable detect cause

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

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

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

Syntax Description

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

Command Default Error-disable detection is enabled for all causes.

Command Modes Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

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

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

Related Commands

Command	Description
show errdisable detect	Displays the error-disable detection status.

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

errdisable recovery

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

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

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

Syntax Description

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

gbic-invalid	Enables the recovery timer for the Gigabit Interface Converter (GBIC)-invalid error-disable cause.
l2ptguard	Enables the recovery timer for the Layer 2 Protocol Tunneling (L2PT) error-disable cause.
link-flap	Enables the recovery timer for the link-flap error-disable cause.
pagp-flap	Enables the recovery timer for the Port Aggregation Protocol (PAgP)-flap error-disable cause.
psecure-violation	Enables the recovery timer for the psecure-violation error-disable cause.
security-violation	Enables the automatic recovery of ports that were disabled because of 802.1X security violations.
rootguard	Enables the recovery timer for the root-guard error-disable cause.
udld	Enables the recovery timer for the Unidirectional Link Detection (UDLD) error-disable cause.
unicast-flood	Enables the recovery timer for the unicast-flood error-disable cause.
interval *seconds*	Specifies the time, in seconds, to recover from a specified error-disable cause. The range is from 30 to 86400. The default interval is 300.

Command Default

The recovery mechanisms are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command was implemented on the Supervisor Engine 2.

Release	Modification
12.2(18)SXD	This command was modified. The **arp-inspection** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

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

file verify auto

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

file verify auto

no file verify auto

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Global configuration

Command History

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

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

Usage Guidelines

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

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

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

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

Examples

The following example shows how to enable automatic image verification:

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

Related Commands

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

hostname

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

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

Command Modes

Global configuration

Command History

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

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

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

The following example changes the hostname to “host1”:

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

Related Commands

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

reload

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

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

Syntax Description

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

at *hh* **:** *mm*	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.
day	(Optional) Number of the day in the range from 1 to 31.
month	Month of the year.
reason *reason-string*	(Optional) Specifies a reason for reloading.
cancel	(Optional) Cancels a scheduled reload.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

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

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

Usage Guidelines

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

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

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

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

The **at** keyword can be used only if the system clock has been set on the router (either through Network Time Protocol [NTP], the hardware calendar, or manually). The time is relative to the configured time zone on the router. To schedule reloads across several routers to occur simultaneously, synchronize the time on each router with NTP.

When you specify the reload time using the **at** keyword, if you specify the month and day, the reload takes place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

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

The /verify and /noverify Keywords

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

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

The warm Keyword

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

Examples

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

```
Router# reload
```

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

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

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

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

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

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

The following example shows how to cancel a pending reload:

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

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

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

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

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

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

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

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

Related Commands

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

remote-span

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

remote-span

no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

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

Usage Guidelines

This command is not supported in the VLAN database mode.

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

Examples

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

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

This example shows how to remove the RSPAN designation:

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

Related Commands

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

setup

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

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

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


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


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

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

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

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

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


Router#
```

Related Commands

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

debug installer

To enable debugs in the installer, use the **debug installer** command in Privileged EXEC mode. To disable debugging use the **no** form of the command.

debug installer [**all** | **process** | **issu** | **common**]

Syntax Description

all	Enables all installer debugs
process	Enables all the debugs inside Installer process
issu	Enables all the debugs inside the installer's provisioning scripts
common	Enables all the debugs inside the installer common modules

Command Default

No debugs enabled

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Privileged EXEC

Usage Guidelines

The debug output for the above commands is displayed to the console and/or the IOS logging buffer.

Note **debug installer all** should typically be enabled when troubleshooting installation related problems

Examples

To enable all installer debugs, perform the following:

```
infra-p2-3#debug installer all
All installer debugging is on
```

Related Commands

Command	Description
debug iosd issu	Use this command to enable all the debugs inside the IOS issu_iosd and iosvrp_issu_upgrade subsystems

debug iosd issu

To enable all the debugs inside the IOS issu_iosd and iosvrp_issu_upgrade subsystems, use the **debug iosd issu** command in Privileged EXEC mode. To disable debugging use the **no** form of the command.

debug iosd issu

Command Default

Debugs not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Privileged EXEC

Usage Guidelines

No command variables

Note **debug iosd issu** should typically be enabled when troubleshooting installation related problems

Related Commands

Command	Description
debug installer all	Use this command to enable debugs in the installer.

show debugging

To display information about the types of debugging that are enabled for your router, use the show debugging command in privileged EXEC mode.

show debugging

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.3(7)T	The output of this command was enhanced to show TCP Explicit Congestion Notification (ECN) configuration.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The output of this command was enhanced to show the user-group debugging configuration.

Examples

The following is sample output from the show debugging command. In this example, the remote host is not configured or connected.

```
Router# show debugging
!
TCP:
  TCP Packet debugging is on
  TCP ECN debugging is on
!
Router# telnet 10.1.25.234
!
Trying 10.1.25.234 ...
!
00:02:48: 10.1.25.31:11001 <---> 10.1.25.234:23 out ECN-setup SYN
00:02:48: tcp0: O CLOSED 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:50: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:50: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
00:02:50: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:54: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:54: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:02: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:02: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:02: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 SYN with ECN disabled
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:18: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:18: tcp0: O SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:20: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:20: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:20: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:24: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:24: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:24: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:32: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:32: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:32: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
!Connection timed out; remote host not responding
```

The following is sample output from the show debugging command when user-group debugging is configured:

```
Router# show debugging
!
usergroup:
 Usergroup Deletions debugging is on
 Usergroup Additions debugging is on
 Usergroup Database debugging is on
 Usergroup API debugging is on

!
```

The following is sample output from the show debugging command when SNAP debugging is configured:

```
Router# show debugging
```

Persistent variable debugging is currently All

SNAP Server Debugging ON

SNAP Client Debugging ON

Router#

The table below describes the significant fields in the output.

Table 6 show debugging Field Descriptions

Field	Description
OPTS 4	Bytes of TCP expressed as a number. In this case, the bytes are 4.
ECE	Echo congestion experience.
CWR	Congestion window reduced.
SYN	Synchronize connections--Request to synchronize sequence numbers, used when a TCP connection is being opened.
WIN 4128	Advertised window size, in bytes. In this case, the bytes are 4128.
cwnd	Congestion window (cwnd)--Indicates that the window size has changed.
ssthresh	Slow-start threshold (ssthresh)--Variable used by TCP to determine whether or not to use slow-start or congestion avoidance.
usergroup	Statically defined usergroup to which source IP addresses are associated.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

show hosts [**vrf** *vrf-name*] [**view** [*view-name* | **default**]] [**all**] [*hostname* | **summary**]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Displays the default view.
all	(Optional) Display all the host tables.

hostname	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	Support was added for Cisco modem user interface feature.
12.4(4)T	The **vrf**, **all**, and **summary** keywords and *vrf-name* and *hostname* arguments were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q key to terminate command output.

Examples

The following is sample output from the **show hosts** command with no parameters specified:

```
Router# show hosts
```

```
Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host                    Port  Flags      Age Type   Address(es)
user                    None  (perm, OK)  0   IP    192.0.2.001
www.example.com         None  (perm, OK)  0   IP    192.0.2.111
                                                    192.0.2.112
```

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

Table 7 show hosts Field Descriptions

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the **ip hosts** command.
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.

Field	Description
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: • EX--Entries marked EX are expired. • OK--Entries marked OK are believed to be valid. • perm--A permanent entry is entered by a configuration command and is not timed out. • temp--A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. • ??--Entries marked ?? are considered suspect and subject to revalidation.
Age	Number of hours since the software last referred to the cache entry.
Type	Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the **ip hp-host global** configuration command, the **show hosts** command will display these hostnames as type HP-IP.
Address(es)	IP address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the **show inventory**command in user EXEC or privileged EXEC mode.

show inventory [**raw**] [**entity**]

Syntax Description

raw	(Optional) Retrieves information about all of the Cisco products--referred to as entities--installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification.
entity	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example “sfslot 1” will display the UDI information for slot 1 of an entity named sfslot.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Release	Modification
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXE5	This command was integrated into Cisco IOS Release 12.2(18)SXE5.

Usage Guidelines

The **show inventory**command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

The following is sample output from the **show inventory**command without any keywords or arguments. This sample output displays a list of Cisco entities installed in a router that are assigned a PID.

```
Router# show inventory
NAME: “Chassis”, DESCR: “12008/GRP chassis”
PID: GSR8/40           ,  VID: V01,  SN: 63915640
NAME: “slot 0”, DESCR: “GRP”
PID: GRP-B             ,  VID: V01,  SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC    ,  VID: V01,  SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port 0C3 POS multimode”
PID: LC-4OC3/POS-MM    ,  VID: V01,  SN: CAB014900GU
NAME: “slot 5”, DESCR: “1 port Gigabit Ethernet”
PID: GE-GBIC-SC-B      ,  VID: V01,  SN: CAB034251NX
NAME: “slot 7”, DESCR: “GRP”
PID: GRP-B             ,  VID: V01,  SN: CAB0428AN4O
NAME: “slot 16”, DESCR: “GSR 12008 Clock Scheduler Card”
PID: GSR8-CSC/ALRM     ,  VID: V01,  SN: CAB0429AUYH
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0428ALOS
NAME: “sfslot 2”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429AU0M
NAME: “sfslot 3”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0429ARD7
NAME: “PSslot 1”, DESCR: “GSR 12008 AC Power Supply”
PID: FWR-GSR8-AC-B     ,  VID: V01,  SN: CAB041999CW
```

The table below describes the fields shown in the display.

Table 8 show inventory Field Descriptions

Field	Description
NAME	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device.
DESCR	Physical description of the Cisco entity that characterizes the object. The physical description includes the hardware serial number and the hardware revision.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

For diagnostic purposes, the **show inventory**command can be used with the **raw** keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

Note The **raw** keyword option is primarily intended for troubleshooting problems with the **show inventory** command itself.

```
Router# show inventory raw
NAME: “Chassis”, DESCR: “12008/GRP chassis”
PID:                 ,  VID: V01,  SN: 63915640
NAME: “slot 0”, DESCR: “GRP”
PID:                 ,  VID: V01,  SN: CAB021300R5
NAME: “slot 1”, DESCR: “4 port ATM OC3 multimode”
PID: 4OC3/ATM-MM-SC  ,  VID: V01,  SN: CAB04036GT1
NAME: “slot 3”, DESCR: “4 port 0C3 POS multimode”
PID: LC-4OC3/POS-MM  ,  VID: V01,  SN: CAB014900GU
```

Enter the **show inventory**command with an *entity* argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the sfslot argument string is displayed.

```
Router# show inventory sfslot
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC        ,  VID: V01,  SN: CAB0428ALOS
NAME: “sfslot 2”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC        ,  VID: V01,  SN: CAB0429AU0M
NAME: “sfslot 3”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC        ,  VID: V01,  SN: CAB0429ARD7
```

You can request even more specific UDI information using the **show inventory**command with an *entity* argument value that is enclosed in quotation marks. In this example, only the details for the entity that exactly matches the sfslot 1 argument string are displayed.

```
Router# show inventory “sfslot 1”
NAME: “sfslot 1”, DESCR: “GSR 12008 Switch Fabric Card”
PID: GSR8-SFC          ,  VID: V01,  SN: CAB0428ALOS
```

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.

show pagp

To display port-channel information, use the **show pagp** command in user EXEC or privileged EXEC mode.

show pagp [*group-number*] {**counters** | **internal** | **neighbor** | **pgroup**}

Syntax Description

group-number	(Optional) Channel-group number; valid values are a maximum of 64 values from 1 to 282.
counters	Displays the traffic information.
internal	Displays the internal information.
neighbor	Displays the neighbor information.
pgroup	Displays the active port channels.

Command Default

This command has no default settings.

Command Modes

User EXEC 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.

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

Usage Guidelines

You can enter any **show pagp** command to display the active port-channel information. To display the nonactive information, enter the **show pagp** command with a group.

The **port-channel** *number*values from 257 to 282 are supported on the CSM and the FWSM only.

Examples

This example shows how to display information about the PAgP counters:

```
Router#
show pagp
 counters
          Information        Flush
Port      Sent   Recv     Sent   Recv
--------------------------------------
Channel group: 1
  Fa5/4    2660   2452     0      0
  Fa5/5    2676   2453     0      0
Channel group: 2
  Fa5/6    289    261      0      0
  Fa5/7    290    261      0      0
Channel group: 1023
  Fa5/9    0      0        0      0
Channel group: 1024
  Fa5/8    0      0        0      0
Router#
```

This example shows how to display internal PAgP information:

```
Router# show pagp
 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.
Channel group 1
                             Hello    Partner  PAgP     Learning
Port      Flags State   Timers  Interval Count   Priority  Method
Fa5/4     SC    U6/S7           30s      1        128       Any
Fa5/5     SC    U6/S7           30s      1        128       Any
Router#
```

This example shows how to display PAgP-neighbor information for all neighbors:

```
Router# show pagp
 neighbor
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
Channel group 1 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/4     JAB031301            0050.0f10.230c   2/45         2s SAC     2D
Fa5/5     JAB031301            0050.0f10.230c   2/46        27s SAC     2D
Channel group 2 neighbors
          Partner              Partner          Partner         Partner Group
Port      Name                 Device ID        Port       Age  Flags   Cap.
Fa5/6     JAB031301            0050.0f10.230c   2/47        10s SAC     2F
Fa5/7     JAB031301            0050.0f10.230c   2/48        11s SAC     2F
```

```
Channel group 1023 neighbors
          Partner              Partner          Partner          Partner Group
Port      Name                 Device ID        Port       Age   Flags   Cap.
Channel group 1024 neighbors
          Partner              Partner          Partner          Partner Group
Port      Name                 Device ID        Port       Age   Flags   Cap.
Router#
```

Related Commands

Command	Description
pagp learn-method	Learns the input interface of the incoming packets.
pagp port-priority	Selects a port in hot standby mode.

show processes cpu

To display detailed CPU utilization statistics (CPU use per process) when Cisco IOS, Cisco IOS XE, or Cisco IOS Software Modularity images are running, use the **show processes cpu**command in user EXEC or privileged EXEC mode.

Cisco IOS Software

show processes cpu [**history** [**table**] | **sorted** [**1min** | **5min** | **5sec**]]

Cisco IOS Software Modularity

show processes cpu [**detailed** [*process-id* | *process-name*] | **history**]

Cisco Catalyst 4500e Series Switches running IOS XE software

show processes cpu [**detailed process** [*process-id* | *process-name*] | **history** [**detailed** | **summary** | **table**] | **sorted**]

Syntax Description

history	(Optional) Displays CPU history in a graph format.
table	(Optional) Displays CPU history in a table format.
summary	(Optional) Displays a summary of the CPU history.
sorted	(Optional) Displays CPU utilization sorted by percentage.
1min	(Optional) Sorts CPU utilization based on 1 minute utilization.
5min	(Optional) Sorts CPU utilization based on 5 minutes utilization.
5sec	(Optional) Sorts CPU utilization based on 5 seconds utilization.

detailed	(Optional) Displays more detailed information about Cisco IOS processes (not for POSIX processes).
process-id	(Optional) Process identifier.
process-name	(Optional) Process name.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.2(2)T	This command was modified. The **history** keyword was added.
12.3(8)	This command was enhanced to display Address Resolution Protocol (ARP) output.
12.3(14)T	This command was enhanced to display ARP output.
12.2(18)SXF4	This command was enhanced to support Cisco IOS Software Modularity images.
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)SCB3	This command was integrated into Cisco IOS Release 12.2(33)SCB3. Support was added for Cisco uBR10012 and uBR7200 routers.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The output was modified to display the CPU time in microseconds that the process has used.
Cisco IOS XE Release 3.1.0.SG	This command was introduced on the Cisco Catalyst 4500e Serfies Switches.

Usage Guidelines

Cisco IOS Software

If you use the optional **history** keyword, three graphs are displayed for Cisco IOS images:

- CPU utilization for the last 60 seconds
- CPU utilization for the last 60 minutes
- CPU utilization for the last 72 hours

Maximum usage is measured and recorded every second; average usage is calculated on periods of more than one second. Consistently high CPU utilization over an extended period indicates a problem. Use the **show processes cpu** command to troubleshoot. Also, you can use the output of this command in the Cisco Output Interpreter tool to display potential issues and fixes. Output Interpreter is available to registered users of Cisco.com who are logged in and have Java Script enabled.

For a list of system processes, go to http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_tech_note09186a00800a65d0.shtml.

Cisco IOS Software Modularity

Cisco IOS Software Modularity images display only one graph that shows the CPU utilization for the last 60 minutes. The horizontal axis shows times (for example, 0, 5, 10, 15 minutes), and the vertical axis shows total percentage of CPU utilization (0 to 100 percent).

Examples

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. The following sections show output examples for each image:

- show processes cpu, page 93
- show processes cpu, page 93
- show processes cpu, page 93

Cisco IOS Software

The following is sample output from the **show processes cpu** command without keywords:

```
Router# show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(uS)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1        4000          67         59  0.00%  0.00%  0.00%   0 Chunk Manager
   2        4000      962255          0  0.00%  0.00%  0.00%   0 Load Meter
   3           0           1          0  0.00%  0.00%  0.00%   0 cpf_process_tp
   4           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
   5   586520704      732013       6668  0.00%  0.11%  0.08%   0 Check heaps
   6        4000         991          4  0.00%  0.00%  0.00%   0 Pool Manager
   7           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backg
   8           0           2          0  0.00%  0.00%  0.00%   0 Timers
   9           0           2          0  0.00%  0.00%  0.00%   0 ATM AutoVC Per
  10           0           2          0  0.00%  0.00%  0.00%   0 ATM VC Auto Cr
  11  2154956000     4809201        448  0.00%  0.03%  0.03%   0 EnvMon
 PID Runtime(uS)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  12           0           1          0  0.00%  0.00%  0.00%   0 OIR Handler
  13           0           1          0  0.00%  0.00%  0.00%   0 Crash writer
  14           0           1          0  0.00%  0.00%  0.00%   0 IPC Process le
  15           0       80189          0  0.00%  0.00%  0.00%   0 IPC Dynamic Ca
  16           0           1          0  0.00%  0.00%  0.00%   0 IPC Zone Manag
  17           0      962246          0  0.00%  0.00%  0.00%   0 IPC Service No
  18           0     4698177          0  0.00%  0.00%  0.00%   0 IPC Periodic T
  19           0     4698177          0  0.00%  0.00%  0.00%   0 IPC Deferred P
  20           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat Manag
  21           0           1          0  0.00%  0.00%  0.00%   0 IPC Seat Contr
  22           0      962246          0  0.00%  0.00%  0.00%   0 IPC Loadometer
<snip>
```

The following is sample output of the one-hour portion of the output. The Y-axis of the graph is the CPU utilization. The X-axis of the graph is the increment within the time period displayed in the graph. This

example shows the individual minutes during the previous hour. The most recent measurement is on the left of the X-axis.

```
Router# show processes cpu history!--- One minute output omitted
6665776865756676676666667667677676766666766767767666566667
6378016198993513709771991443732358689932740858269643922613
100
90
80         *  *                     * *     *  * *  *
70  * * ***** *  ** ***** ***  **** ******  *  *******     * *
60  #***##*##*#***#####*#*###*****#*###*#*#*##*#*##*#*##*****#
50  ############################################################
40  ############################################################
30  ############################################################
20  ############################################################
10  ############################################################
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
              CPU% per minute (last 60 minutes)
              * = maximum CPU% # = average CPU%!--- 72-hour output omitted
```

The top two rows, read vertically, display the highest percentage of CPU utilization recorded during the time increment. In this example, the CPU utilization for the last minute recorded is 66 percent. The device may have reached 66 percent only once during that minute, or it may have reached 66 percent multiple times. The device records only the peak reached during the time increment and the average over the course of that increment.

The following is sample output from the **show processes cpu** command on a Cisco uBR10012 router:

```
Router# show processes cpu
CPU utilization for five seconds: 2%/0%; one minute: 2%; five minutes: 2%
 PID Runtime(us)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           8       471         16  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       472          8  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 IPC 0x50000 Vers
   4           0        10          0  0.00%  0.00%  0.00%   0 C10K Card Event
   5           0        65          0  0.00%  0.00%  0.00%   0 Retransmission o
   6           0         5          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   7        5112       472      10830  0.63%  0.18%  0.18%   0 Check heaps
   8           0         1          0  0.00%  0.00%  0.00%   0 Pool Manager
   9           0         2          0  0.00%  0.00%  0.00%   0 Timers
  10           0         2          0  0.00%  0.00%  0.00%   0 Serial Backgroun
  11           0       786          0  0.00%  0.00%  0.00%   0 WBCMTS process
  12           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  13           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  14           0         1          0  0.00%  0.00%  0.00%   0 Crash writer
  15           0         1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
  16           0         1          0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
  17           0      2364          0  0.00%  0.00%  0.00%   0 Facility Alarm
  18           0        41          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
```

The following is sample output from the **show processes cpu** command that shows an ARP probe process:

```
Router# show processes cpu | include ARP
17       38140    389690         97  0.00%  0.00%  0.00%   0 ARP Input
36           0         1          0  0.00%  0.00%  0.00%   0 IP ARP Probe
40           0         1          0  0.00%  0.00%  0.00%   0 ATM ARP INPUT
80           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
114          0         1          0  0.00%  0.00%  0.00%   0 FR ARP
```

The table below describes the fields shown in the output.

Table 9 show processes cpu Field Descriptions

Field	Description
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minutes	CPU utilization for the last minute.
five minutess	CPU utilization for the last 5 minutes.
PID	Process ID.
Runtime (us)	CPU time that the process has used (in microseconds).
Invoked	Number of times that the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Process	Name of the process.

Note Because platforms have a 4- to 8-microsecond clock resolution, run times are considered reliable only after several invocations or a reasonable, measured run time.

Cisco IOS Software Modularity

The following is sample output from the **show processes cpu** command when a Software Modularity image is running:

```
Router# show processes cpu
Total CPU utilization for 5 seconds: 99.6%; 1 minute: 98.5%; 5 minutes: 85.3%
PID       5Sec    1Min     5Min Process
1         0.0%    0.1%     0.8% kernel
3         0.0%    0.0%     0.0% qdelogger
4         0.0%    0.0%     0.0% devc-pty
6         0.7%    0.2%     0.1% devc-ser2681
7         0.0%    0.0%     0.0% dumper.proc
4104      0.0%    0.0%     0.0% pipe
8201      0.0%    0.0%     0.0% mqueue
8202      0.0%    0.0%     0.0% fsdev.proc
8203      0.0%    0.0%     0.0% flashfs_hes_slot1.proc
8204      0.0%    0.0%     0.0% flashfs_hes_slot0.proc
8205      0.0%    0.0%     0.0% flashfs_hes_bootflash.proc
8206      0.0%    0.0%     0.0% dfs_disk2.proc
8207      0.0%    0.0%     0.0% dfs_disk1.proc
```

```
8208      0.0%    0.0%     0.0% dfs_disk0.proc
8209      0.0%    0.0%     0.0% ldcache.proc
8210      0.0%    0.0%     0.0% watchdog.proc
8211      0.0%    0.0%     0.0% syslogd.proc
8212      0.0%    0.0%     0.0% name_svr.proc
8213      0.0%    0.1%     0.0% wdsysmon.proc
--More--
```

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

Table 10 show processes cpu (Software Modularity) Field Descriptions

Field	Description
Total CPU utilization for five seconds	Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
1 minute	CPU utilization for the last minute.
5 minutes	CPU utilization for the last 5 minutes.
PID	Process ID.
5Sec	Percentage of CPU time spent at the interrupt level for this process during the last five seconds.
1Min	Percentage of CPU time spent at the interrupt level for this process during the last minute.
5Min	Percentage of CPU time spent at the interrupt level for this process during the last five minutes.
Process	Process name.

The following is partial sample output from the **show processes cpu**command with the **detailed**keyword when a Software Modularity image is running:

```
Router# show processes cpu detailed
Total CPU utilization for 5 seconds: 99.6%; 1 minute: 99.3%; 5 minutes: 88.6%
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
1         0.0%    0.7%     0.7% kernel                                 8.900
      1   0.4%    0.7%    11.4% [idle thread]          0  Ready        2m28s
      2   0.0%    0.0%     0.0%                       63  Receive      0.000
      3   0.0%    0.0%     0.0%                       10  Receive      0.000
      4   0.0%    0.0%     0.1%                       11  Receive      1.848
      5   0.0%    0.0%     0.0%                       63  Receive      0.000
.
.
.
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
8214      0.0%    0.0%     0.0% sysmgr.proc                            0.216
      1   0.0%    0.0%     0.0%                       10  Receive      0.132
      2   0.0%    0.0%     0.0%                       10  Sigwaitin    0.000
      3   0.0%    0.0%     0.0%                       10  Receive      0.004
      4   0.0%    0.0%     0.0%                       10  Receive      0.000
      5   0.0%    0.0%     0.0%                       10  Receive      0.000
      6   0.0%    0.0%     0.0%                       10  Receive      0.004
      7   0.0%    0.0%     0.0%                       10  Receive      0.000
      8   0.0%    0.0%     0.0%                       10  Receive      0.000
      9   0.0%    0.0%     0.0%                       10  Receive      0.000
     10   0.0%    0.0%     0.0%                       10  Receive      0.000
     11   0.0%    0.0%     0.0%                       10  Receive      0.000
     12   0.0%    0.0%     0.0%                       10  Receive      0.000
```

```
     13   0.0%    0.0%     0.0%                       10  Receive      0.028
     14   0.0%    0.0%     0.0%                       10  Receive      0.040
     15   0.0%    0.0%     0.0%                       10  Receive      0.000
     16   0.0%    0.0%     0.0%                       10  Receive      0.000
     17   0.0%    0.0%     0.0%                       10  Receive      0.004
     18   0.0%    0.0%     0.0%                       10  Receive      0.000
     19   0.0%    0.0%     0.0%                       10  Receive      0.000
     20   0.0%    0.0%     0.0%                       10  Receive      0.000
     21   0.0%    0.0%     0.0%                       10  Receive      0.004
     22   0.0%    0.0%     0.0%                       10  Receive      0.000
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
8215      0.0%    0.0%     0.0% kosh.proc                               0.044
      1   0.0%    0.0%     0.0%                       10  Reply        0.044
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
12290     0.0%    0.0%     0.0% chkptd.proc                             0.080
      1   0.0%    0.0%     0.0%                       10  Receive      0.080
      2   0.0%    0.0%     0.0%                       10  Receive      0.000
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
12312     0.0%    0.0%     0.0% sysmgr.proc                             0.112
      1   0.0%    0.0%     0.0%                       10  Receive      0.112
      2   0.0%    0.0%     0.0%                       10  Sigwaitin    0.000
PID/TID   5Sec    1Min     5Min Process             Prio  STATE        CPU
12316     0.0%    0.0%     0.0% installer.proc                          0.072
      1   0.0%    0.0%     0.0%                       10  Receive      0.000
      3   0.0%    0.0%     0.0%                       10  Nanosleep    0.000
      4   0.0%    0.0%     0.0%                       10  Sigwaitin    0.000
      6   0.0%    0.0%     0.0%                       10  Receive      0.000
Process sbin/ios-base, type IOS, PID = 12317
CPU utilization for five seconds: 12%/9%; one minute: 13%; five minutes: 10%
Task  Runtime(us)  Invoked  uSecs    5Sec   1Min   5Min TTY Task Name
   1         219     1503    145   0.00%  0.00%  0.00%   0 Hot Service Task
   2       23680    42384    558   2.39%  6.72%  4.81%   0 Service Task
   3        6104    11902    512   3.51%  1.99%  1.23%   0 Service Task
   4        1720     5761    298   1.91%  0.90%  0.39%   0 Service Task
   5           0        5      0   0.00%  0.00%  0.00%   0 Chunk Manager
   6           0        1      0   0.00%  0.00%  0.00%   0 Connection Mgr
   7           4      106     37   0.00%  0.00%  0.00%   0 Load Meter
   8        6240     7376    845   0.23%  0.15%  0.55%   0 Exec
   9         379       62   6112   0.00%  0.07%  0.04%   0 Check heaps
  10           0        1      0   0.00%  0.00%  0.00%   0 Pool Manager
  11           3        2   1500   0.00%  0.00%  0.00%   0 Timers
  12           0        1      0   0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  13           0        2      0   0.00%  0.00%  0.00%   0 AAA high-capacit
  14         307      517    593   0.00%  0.05%  0.03%   0 EnvMon
  15           0        1      0   0.00%  0.00%  0.00%   0 OIR Handler
  16         283       58   4879   0.00%  0.04%  0.02%   0 ARP Input
  17           0        2      0   0.00%  0.00%  0.00%   0 Serial Backgroun
  18           0       81      0   0.00%  0.00%  0.00%   0 ALARM_TRIGGER_SC
  19           0        2      0   0.00%  0.00%  0.00%   0 DDR Timers
  20           0        2      0   0.00%  0.00%  0.00%   0 Dialer event
  21           4        2   2000   0.00%  0.00%  0.00%   0 Entity MIB API
  22           0       54      0   0.00%  0.00%  0.00%   0 Compute SRP rate
  23           0        9      0   0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  24           0        1      0   0.00%  0.00%  0.00%   0 IPC Zone Manager
  25           0        1      0   0.00%  0.00%  0.00%   0 IPC Punt Process
  26           4      513      7   0.00%  0.00%  0.00%   0 IPC Periodic Tim
  27          11      513     21   0.00%  0.00%  0.00%   0 IPC Deferred Por
  28           0        1      0   0.00%  0.00%  0.00%   0 IPC Seat Manager
  29          83     1464     56   0.00%  0.00%  0.00%   0 EEM ED Syslog
.
.
.
```

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

Table 11 show processes cpu detailed (Software Modularity) Field Descriptions

Field	Description
Total CPU utilization for five seconds	Total CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
1 minute	CPU utilization for the last minute.
5 minutes	CPU utilization for the last 5 minutes.
PID/TID	Process ID or task ID.
5Sec	Percentage of CPU time spent at the interrupt level for this process during the last five seconds.
1Min	Percentage of CPU time spent at the interrupt level for this process during the last minute.
5Min	Percentage of CPU time spent at the interrupt level for this process during the last five minutes.
Process	Process name.
Prio	Priority level of the process.
STATE	Current state of the process.
CPU	CPU utilization of the process in minutes and seconds.
type	Type of process; can be either IOS or POSIX.
Task	Task sequence number.
Runtime(us)	CPU time that the process has used (in microseconds).
Invoked	Number of times that the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Task Name	Task name.

Cisco Catalyst 4500e Series Switches running IOS XE software

The following is sample output from the **show processes cpu** command:

```
Switch#show proc cpu
Core 0: CPU utilization for five seconds: 1%; one minute: 7%; five minutes: 5%
Core 1: CPU utilization for five seconds: 1%; one minute: 20%; five minutes: 12%
PID     Runtime(ms) Invoked   uSecs  5Sec 1Min 5Min TTY   Process
1       935         596       156971 0.00 0.00 0.00 0     init
2       0           79        10405  0.00 0.00 0.00 0     kthreadd
3       13          2450      5575   0.00 0.00 0.00 0     migration/0
4       12          808       15237  0.00 0.00 0.00 0     ksoftirqd/0
5       8           1413      6170   0.00 0.00 0.00 0     migration/1
6       14          894       16370  0.00 0.00 0.00 0     ksoftirqd/1
7       31          1422      21961  0.00 0.00 0.00 0     events/0
8       32          1269      25403  0.00 0.00 0.00 0     events/1
9       5           637       9070   0.00 0.00 0.00 0     khelper
61      80          79        102031 0.00 0.00 0.00 0     kblockd/0
62      90          183       497142 0.00 0.00 0.00 0     kblockd/1
75      0           21        1238   0.00 0.00 0.00 0     khubd
78      0           23        652    0.00 0.00 0.00 0     kseriod
83      7           26        271115 0.00 0.00 0.00 0     kmmcd
--More--
```

The following is partial sample output from the **show processes cpu**command with the **detailed**keyword:

```
switch#show proc cpu detailed
Core 0: CPU utilization for five seconds: 0%; one minute: 6%; five minutes: 5%
Core 1: CPU utilization for five seconds: 2%; one minute: 17%; five minutes: 12%
PID     T C  TID     Runtime(ms) Invoked   uSecs  5Sec   1Min 5Min TTY   Process
                                           (%)    (%)  (%)
1       L            935         596       156971 0.00 A 0.00 0.00 0     init
2       L            0           79        10405  0.00 A 0.00 0.00 0     kthreadd
3       L            13          2481      5573   0.00 A 0.00 0.00 0     migration/0
4       L            12          808       15237  0.00 A 0.00 0.00 0     ksoftirqd/0
5       L            8           1454      6157   0.00 A 0.00 0.00 0     migration/1
6       L            14          897       16341  0.00 A 0.00 0.00 0     ksoftirqd/1
7       L            31          1471      21661  0.00 A 0.00 0.00 0     events/0
8       L            33          1308      25496  0.00 A 0.00 0.00 0     events/1
9       L            5           637       9070   0.00 A 0.00 0.00 0     khelper
61      L            80          79        102031 0.00 A 0.00 0.00 0     kblockd/0
62      L            90          183       497142 0.00 A 0.00 0.00 0     kblockd/1
75      L            0           21        1238   0.00 A 0.00 0.00 0     khubd
78      L            0           23        652    0.00 A 0.00 0.00 0     kseriod
83      L            7           26        271115 0.00 A 0.00 0.00 0     kmmcd
120     L            0           25        320    0.00 A 0.00 0.00 0     pdflush
121     L            103         195       531687 0.00 A 0.00 0.00 0     pdflush
122     L            0           29        172    0.00 A 0.00 0.00 0     kswapd0
123     L            0           31        161    0.00 A 0.00 0.00 0     aio/0
124     L            0           33        121    0.00 A 0.00 0.00 0     aio/1
291     L            0           35        142    0.00 A 0.00 0.00 0     kpsmoused
--More--
```

The following is sample output from the **show processes cpu history summary**command:

```
Switch#show processes cpu history summary
History information for system:
   22233111111111111111111111111111111111111111111111111111111111111111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
              * = maximum CPU%   # = average CPU%
```

```
   3333333333343333253333343333343333343333343333343333343333333
100
 90
 80
 70
 60
 50          * *
 40
 30                     * ** * **     *    **      *          **
 20          # #       #*##*#*##*       *    *     *
 10                    *              #           ##         ##
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
   6556545556545545545555555555555555555655655555655554655655655555555565555
100
 90
 80
 70
 60
 50**
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                      CPU% per hour (last 72 hours)
                 * = maximum CPU%   # = average CPU%
```

The following is sample output from the **show processes cpu history detailed**command:

```
Switch#show processes cpu history detailed
History information for core 0:
   2223311111111111111111111111111111111111111111111111111111111111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
              * = maximum CPU%   # = average CPU%
   3333333333343333253333343333343333343333343333343333343333333
100
 90
 80
 70
 60          *
 50
 40
 30
 20                     ** * ** *                   *         *
 10                       * *  * *    *  * ** *    *      *    *
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
   6556545556545545545555555555555555555655655555655554655655655555555565555
100
 90
 80
 70
 60*
 50
 40
```

```
 30 *
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                       CPU% per hour (last 72 hours)
                     * = maximum CPU%   # = average CPU%
History information for core 1:
   22233111111111111111111111111111111111111111111111111111111111111111
100
 90
 80
 70
 60
 50
 40
 30
 20
 10             *****
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)
              * = maximum CPU%   # = average CPU%
   33333333333433332533333433333433333433333433333433333433333333
100            *
 90          *
 80
 70
 60
 50
 40                     **********    *    **      **         **
 30                                      *    *
 20
 10*                  *
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
   65565455565455455555555555555555565565555565555465565565555555565555
100*
 90 *
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
                       CPU% per hour (last 72 hours)
                     * = maximum CPU%   # = average CPU%
Switch#show proc cpu history table
CPU utilization for five seconds: 1%/0% at 01:14:44
PID                5Sec                Process
10319              6                   iosd
CPU utilization for five seconds: 1%/0% at 01:14:49
PID                5Sec                Process
10319              6                   iosd
CPU utilization for five seconds: 1%/0% at 01:14:54
PID                5Sec                Process
10319              6                   iosd
CPU utilization for five seconds: 1%/0% at 01:14:59
PID                5Sec                Process
10319              6                   iosd
Switch#
```

The table below describes the fields shown in the output.

Table 12 show processes cpu Field Descriptions

Field	Description
Core (#)	Core for which CPU utilization is being generated.
CPU utilization for five seconds	CPU utilization for the last 5 seconds. The second number indicates the percent of CPU time spent at the interrupt level.
one minutes	CPU utilization for the last minute.
five minutess	CPU utilization for the last 5 minutes.
PID	Process ID.
Runtime (us)	CPU time that the process has used (in microseconds).
Invoked	Number of times that the process has been invoked.
uSecs	Microseconds of CPU time for each process invocation.
5Sec	CPU utilization by task in the last 5 seconds.
1Min	CPU utilization by task in the last minute.
5Min	CPU utilization by task in the last 5 minutes.
TTY	Terminal that controls the process.
Process	Name of the process.

Related Commands

Command	Description
show processes	Displays information about active processes.
show processes memory	Displays the amount of system memory used per system process.

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) Keywords used to customize output. You can enter more than one keyword. • **all** --Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters. • **brief** --Displays the configuration without certification data and encrypted filter details. The **brief** keyword can be used with the **linenum** keyword. • **class-map** [*name*][**linenum**]--Displays class map information. The **linenum** keyword can be used with the **class-map** *name* option. • **control-plane** [**cef-exception**| **host**| **transit**]--Displays control-plane information. The **cef-exception**, **host**, and **transit** keywords can be used with the **control-plane** option. • **flow** {**exporter** | **monitor** | **record**}--Displays global flow configuration commands. The **exporter**, **monitor**, and **record**keywords can be used with the **flow** option. • **full** --Displays the full configuration. • **interface** *type number* -- Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface ethernet 0**). Keywords for common interfaces include **async**, **ethernet**, **fastEthernet**, **group-async**, **loopback**, **null**, **serial**, and **virtual-template**. Use the **show run interface ?** command to determine the interfaces available on your system. • **linenum** --Displays line numbers in the output. The **brief** or **full** keyword can be used with the **linenum** keyword. The **linenum**keyword can be used with the **class-map**, **interface**, **map-class**, **policy-map**, and **vc-class** keywords. • **map-class** [**atm** | **dialer** | **frame-relay**] [**name**] [**linenum**]--Displays map class information. This option is described separately; see the **show running-config map-class** command page.

	• **partition types** -- Displays the configuration corresponding to a partition. The **types** keyword can be used with the **partition**option. • **policy-map** [*name*][**linenum**]--Displays policy map information. The **linenum** keyword can be used with the **policy-map** *name* option. • **vc-class** [*name*] [**linenum**]--Displays VC-class information (the display is available only on certain routers such as the Cisco 7500 series routers). The **linenum** keyword can be used with the **vc-class** *name* option.
	• **view full** --Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view. • **vrf** *name* --Displays the Virtual routing and forwarding (VRF)-aware configuration module number . • **vlan** [*vlan-id*]--Displays the specific VLAN information ; valid values are from 1 to 4094.

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was replaced by the **more system:running-config** command.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the output modifier (|) was added.
12.2(4)T	This command was modified. The **linenum** keyword was added.

Release	Modification
12.3(8)T	This command was modified. The **view full**option was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **module** *number* and **vlan** *vlan-id* keywords and arguments were added for the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Release 12.2(17d)SXB and implemented on the Supervisor Engine 2.
12.2(33)SXH	This command was modified. The **all**keyword was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was enhanced to display the configuration information for traffic shaping overhead accounting for ATM and was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was modified. Support for the Cisco 7300 series router was added.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **partition** and **vrf** keywords were added. The **module** and **vlan** keywords were removed.
15.0(1)M	This command was modified. The output was modified to include encrypted filter information.
12.2(33)SXI	This command was modified. The output was modified to display Access Control List (ACL) information.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface serial 2/1 linenum | begin 3**. To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

Prior to Cisco IOS Release 12.2(33)SXH, the **show running-config**command output omitted configuration commands set with default values. Effective with Cisco IOS Release 12.2(33)SXH, the **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all**commands is the same; that is, the configured parameter is displayed.

Note In Cisco IOS Release 12.2(33)SXH, the **all**keyword expands the output to include some of the commands that are configured with default values. In subsequent Cisco IOS releases, additional configuration commands that are configured with default values will be added to the output of the **show running-config all**command.

Effective with Cisco IOS Release 12.2(33)SXI, the **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list**command.

Cisco 7600 Series Router

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command displays the operating mode of an interface, and the **show running-config** command displays the configured mode of the interface.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode that is displayed becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is displayed with the **show running-config** command.

Examples

The following example shows the configuration for serial interface 1. The fields are self-explanatory.

```
Router# show running-config interface serial 1
Building configuration...
Current configuration:
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output. The fields are self-explanatory.

```
Router# show running-config interface ethernet 0/0 linenum
Building configuration...
Current configuration : 104 bytes
 1 : !
 2 : interface Ethernet0/0
 3 :  ip address 10.4.2.63 255.255.255.0
 4 :  no ip route-cache
 5 :  no ip mroute-cache
 6 : end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Router# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.172.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
   29 : isdn switch-type primary-5ess
   30 : !
   .
   .
   .
   126 : end
```

The following example shows how to display the module and status configuration for all modules on a Cisco 7600 series router. The fields are self-explanatory.

```
Router#
show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname Router
!
boot buffersize 126968
boot system flash slot0:7600r
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
 main-cpu
  auto-sync standard
!
```

```
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
!
!
!
 shutdown
!
!
.
.
.
```

In the following sample output from the **show running-config** command, the **shape average**command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory

```
Router# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Router# show running-config class-map
Building configuration...
Current configuration : 2910 bytes
!
class-map type stack match-all ip_tcp_stack
 match field IP protocol eq 0x6 next TCP
class-map type access-control match-all my
 match field UDP dest-port eq 1111
 match encrypted
  filter-version 0.1, Dummy Filter 2
  filter-id      123
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
oeahb4L6JK+XuC0q8k9AqXvBeQWzVfdg8WV67WEXbiWdXGQs6BEXqQeb4Pfow570zM4eDw0gxlp/Er8w
/lXsmolSgYpYuxFMYb1KX/H2iCXvA76VX7w5TElb/+6ekgbfP/d5ms6DEzKa8DlOpl+Q95lP194PsIlU
wCyfVCwLS+T8p3RDLi8dKBgQMcDW4Dha1ObBJTpV4zpwhEdMvJDu5PATtEQhFjhN/UYeyQiPRthjbkJn
```

```
LzT8hQFxwYwVW8PCjkyqEwYrr+R+mFG/C7tFRiooaW9MU9PCpFd95FARvlU=#
  exit
class-map type stack match-all ip_udp_stack
 match field IP protocol eq 0x11 next UDP
class-map type access-control match-all psirt1
 match encrypted
  filter-version 0.0_DummyVersion_20090101_1830
  filter-id      cisco-sa-20090101-dummy_ddts_001
  filter-hash    FC50BED10521002B8A170F29AF059C53
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
DkGbVq0FPAsVJKguU15lQPDfZyTcHUXWsj8+tD+dCSYW9cjkRU9jyST4vO4u69/L62QlbyQuKdyQmb10
6sAeY5vDsDfDV05k4o5eD+j8cMt78iZT0Qg7uGiBSYBbak3kKn/5w2gDd1vnivyQ7g4Ltd9+XM+GP6XL
27RrXeP5A5iGbzC7KI9t6riZXk0gmR/vFw1a5wck0D/iQHIlFa/yRPoKMSFlqfIlLTe5NM7JArSTKET2
pu7wZammTz4FF6rY#
  exit
 match start TCP payload-start offset 0 size 10 regex "abc.*def"
 match field TCP source-port eq 1234
class-map type access-control match-all psirt2
 match encrypted
  filter-version 0.0_DummyVersion_20090711_1830
  filter-id      cisco-sa-20090711-dummy_ddts_002
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
configure terminal	Enters global configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps, and displays ATM overhead accounting information, if configured.

Command	Description
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show software authenticity file

To display information related to software authentication for a specific image file, use the **show software authenticity file** command in privileged EXEC mode.

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

Syntax Description

flash0:	Displays information related to software authentication for flash 0 resources.
filename	Name of the filename in memory.
flash1:	Displays information related to software authentication for flash 1 resources.
flash:	Displays information related to software authentication for flash resources.
nvram:	Displays information related to software authentication for NVRAM resources.
usbflash0:	Displays information related to software authentication for Universal Serial Bus (USB) flash 0 resources.
usbflash1:	Displays information related to software authentication for USB flash 1 resources.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for the Cisco 1941, 2900, and 3900 routers.

Usage Guidelines

The show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information.

Examples

The following example displays software authentication related information for an image file named c3900-universalk9-mz.SSA:

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

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

Table 13 show software authenticity file Field Descriptions

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

Field	Description
Hash Algorithm	Displays the type of hash algorithm used in digital signature verification.
Signature Algorithm	Displays the type of signature algorithm used in digital signature verification.
Key Version	Displays the key version used for verification.

Related Commands

Command	Description
show software authenticity keys	Displays the software public keys that are in the storage with the key types.
show software authenticity running	Displays information related to software authentication for the current ROMMON, monitor library (monlib), and Cisco IOS image used for booting.

show software authenticity keys

To display the software public keys that are in the storage with the key types, use the **show software authenticity keys**command in privileged EXEC mode.

show software authenticity keys

Syntax Description

This command has no argument or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for the Cisco 1941, 2900, and 3900 routers.

Usage Guidelines

The display from this command includes the public keys that are in the storage with the key types.

Examples

The following is sample output from the show software authenticity keys command:

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

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

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

Table 14 show software authenticity running Field Descriptions

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

Related Commands

Command	Description
show software authenticity file	Displays information related to software authentication for the loaded image file.
show software authenticity running	Displays information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting.

show software authenticity running

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show software authenticity running** command in privileged EXEC mode.

show software authenticity running

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced for the Cisco 1941, 2900, and 3900 routers.

Usage Guidelines

The information displayed by the show software authenticity running command about the current ROMMON, monlib and Cisco IOS image used for booting includes:

- Image credential information
- Key type used for verification
- Signing information
- Any other attributes in the signature envelope

Examples

The following example displays software authentication related information for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting:

```
Router(mode-prompt
)# show software authenticity running
```

```
SYSTEM IMAGE
------------------
Image type : Development
Signer Information
Common Name : xxx
Organization Unit : xxx
Organization Name : xxx
Certificate Serial Number : xxx
Hash Algorithm : xxx
Signature Algorithm : 2048-bit RSA
Key Version : xxx
Verifier Information
Verifier Name : ROMMON 2
Verifier Version : System Bootstrap, Version 12.4(20090409:084310)
ROMMON 2
---------------
Image type : Development
Signer Information
Common Name : xxx
Organization Unit : xxx
Organization Name : xxx
Certificate Serial Number : xxx
Hash Algorithm : xxx
Signature Algorithm : 2048-bit RSA
Key Version : xxx
Verifier Information
Verifier Name : ROMMON 2
Verifier Version : System Bootstrap, Version 12.4(20090409:084310)
```

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

Table 15 show software authenticity running Field Descriptions

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

Field	Description
Verifier Version	Version of the program responsible for performing the digital signature verification.
ROMMON 2	Section of the output displaying the current ROM monitor (ROMMON) information.

Related Commands

Command	Description
show software authenticity file	Displays the software authenticity related information for the loaded image file.
show software authenticity keys	Displays the software public keys that are in the storage with the key types.

show software installer rollback-timer

The **show software installer rollback-timer** command displays the current auto-rollback timer status for a standalone platform or all switches in a stacked system.

show software installer rollback-timer

Command Default

There are no command options.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

There are no command options.

Examples

To show the auto-rollback timer status for the current switch, perform the following.

```
infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           active      00:31:28
2           active      00:31:43

infra-p2-3#

infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           inactive       -
2           inactive       -

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.
show version	To display information about the currently loaded software along with hardware and device information, use the **show version** command.

show software package

To display information about a specific bundle or package file, use the **show software package** command in privileged EXEC mode.

show software package *bundle or package url* [**detail**][**verbose**]

Syntax Description

bundle or package url	Specify the name of the bundle or package file whose information should be displayed.
detail	(optional) This command option is intended to provide additional details about the specified package or bundle file. Currently, no additional information is displayed.
verbose	(optional) provides some additional info in the log files

Command Default

No default behavior or values.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The 'show software package' command displays information about the specified bundle or package file.

If a package file is specified, this command displays information from its package metadata.

If a bundle file is specified, this command displays information from its bundle metadata, and also information from the package metadata of each package included in the bundle.

Examples

The following example shows the **show software package** output for a bundle file.

```
infra-p2-3#show software package flash:cat3k_caa-universalk9.SSA.03.09.19.
   EMP.150-9.19.EMP.bin
Package: cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
  Size: 220766688
  Timestamp: 2012-11-15 11:53:50 UTC
  Canonical path: /flash/cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
  Header size:     2928 bytes

  Internal package information:
    Name: rp_super
    BuildTime: Thu Nov 15 01:55:09 PST 2012
    ReleaseDate: Thu Nov 15 01:55:09 PST 2012
    RouteProcessor: mips
    Platform: ng3k
    User: udonthi
    PackageName: cat3k_caa-universalk9
    Build: 03.09.19.EMP
    Dependencies: PROVIDES:cat3k_caa-base,03.09.19.EMP,mips;cat3k_caa-infra,
03.09.19.EMP,
     mips;cat3k_caa-platform,03.09.19.EMP,mips;cat3k_caa-iosd-universalk9,150-9.19.EMP,
     mips;cat3k_caa-wcm,03.09.19.EMP,mips;cat3k_caa-drivers,03.09.19.EMP,mips;
    BuildType: Production

  Package is bootable from media and tftp.
  Package contents:

  Package: cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Size: 74390336
    Timestamp: 2012-11-15 11:55:30 UTC
    Header size:     412 bytes

    Internal package information:
      Name: rp_base
      BuildTime: Thu Nov 15 01:52:19 PST 2012
      ReleaseDate: Thu Nov 15 01:52:19 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-base
      Build: 03.09.19.EMP
      Dependencies: PROVIDES: nova-gold,03.09.19.EMP,mips; nova-goldlib,
03.09.19.EMP,mips;
       nova-base,03.09.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:#
      BuildType: Production

    Package is not bootable.

  Package: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Size: 2734772
    Timestamp: 2012-11-15 11:55:37 UTC
    Header size:     252 bytes

    Internal package information:
      Name: drivers
      BuildTime: Thu Nov 15 01:54:53 PST 2012
      ReleaseDate: Thu Nov 15 01:54:53 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-drivers
      Build: 03.09.19.EMP
      Dependencies: PROVIDES: ng3k-drivers,03.09.19.EMP,mips#REQUIRES:#WORKSWITH:
       #CONFLICTS:#
      BuildType: Production
```

```
    Package is not bootable.

  Package: cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Size: 32465772
    Timestamp: 2012-11-15 11:55:32 UTC
    Header size:     436 bytes

    Internal package information:
      Name: rp_infra
      BuildTime: Thu Nov 15 01:53:08 PST 2012
      ReleaseDate: Thu Nov 15 01:53:08 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-infra
      Build: 03.09.19.EMP
      Dependencies: PROVIDES: nova-infra,03.09.19.EMP,mips;
       nova-infralibs,03.09.19.EMP,mips; nova-web,03.09.19.EMP,mips;
       nova-shell,03.09.19.EMP,mips; nova-console-relay,03.09.19.EMP,mips;
       nova-mgmte,03.09.19.EMP,mips; nova-ng3k-flash,03.09.19.EMP,mips#
EQUIRES:#WORKSWITH:#CONFLICTS:#
      BuildType: Production

    Package is not bootable.

  Package: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Size: 30384940
    Timestamp: 2012-11-15 11:55:34 UTC
    Header size:     372 bytes

    Internal package information:
      Name: rp_iosd
      BuildTime: Thu Nov 15 01:54:09 PST 2012
      ReleaseDate: Thu Nov 15 01:54:09 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-iosd-universalk9
      Build: 150-9.19.EMP
      Dependencies: PROVIDES: iosd-stuff,03.09.19.EMP,mips; nova-ioslibs-required,
       03.09.19.EMP,mips; ioucon,150-9.19.EMP,mips;
       ng3k-iosd-universalk9,150-9.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:#
      BuildType: Production

    Package is not bootable.

  Package: cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Size: 18148064
    Timestamp: 2012-11-15 11:55:33 UTC
    Header size:     296 bytes

    Internal package information:
      Name: rp_platform
      BuildTime: Thu Nov 15 01:53:39 PST 2012
      ReleaseDate: Thu Nov 15 01:53:39 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-platform
      Build: 03.09.19.EMP
      Dependencies: PROVIDES: nova-platformlibs-required,03.09.19.EMP,mips;
       ng3k-platform,03.09.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:#
      BuildType: Production

    Package is not bootable.

  Package: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
    Size: 62638800
    Timestamp: 2012-11-15 11:55:37 UTC
    Header size:     280 bytes

    Internal package information:
```

```
      Name: rp_wcm
      BuildTime: Thu Nov 15 01:54:34 PST 2012
      ReleaseDate: Thu Nov 15 01:54:34 PST 2012
      RouteProcessor: mips
      Platform: ng3k
      User: udonthi
      PackageName: cat3k_caa-wcm
      Build: 03.09.19.EMP
      Dependencies: PROVIDES: wcm-ng3k,03.09.19.EMP,mips; nova-wcmlibs-required,
       03.09.19.EMP,mips#REQUIRES:#WORKSWITH:#CONFLICTS:#
      BuildType: Production

    Package is not bootable.


infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.
show version	To display information about the currently loaded software along with hardware and device information, use the **show version** command.

show version

To display information about the currently loaded software along with hardware and device information, use the **show version** command in user EXEC, privileged EXEC, or diagnostic mode.

show version

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers

show version [**switch***node*][**running** | **committed** | **provisioned**]

Cisco ASR 1000 Series Routers

show version [*rp-slot*] [**installed** [**user-interface**] | **provisioned** | **running**]

Cisco Catalyst 4500e Series Switches running IOS XE software

show version [*rp-slot*] [**running**]

Cisco Catalyst 6500 Series Routers

show version [**epld** *slot*]

Syntax Description

switch*node*	(optional) Only a single switch may be specified. Default is all switches in a stacked system.
running	(optional) Specifies information on the files currently running. cat3850 and ct5760: (optional) Displays information about the active package set currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the booted bundle.

committed	(optional) Displays information about the committed package set. If no installation operations have been performed since bootup, this output will be the same as **show version running**. If any installation operations have been performed since bootup, this output will display the set of packages that will be activated/running on the next reload. **Note** This command option is only applicable when running in installed mode.
provisioned	(optional)Specifies information on the software files that are provisioned. cat3850 and ct5760: (optional) Displays information about the provisioned package set. In most cases, the provisioned package set is the same as the committed package set. These package sets will differ if an installation was performed with the 'auto-rollback' option and the installed packages have not yet been committed using the 'software commit' command. This command option is only applicable when running in installed mode.
rp-slot	Specifies the software of the RP in a specific RP slot of a Cisco ASR 1000 Series Router. Options include: • **r0** --the RP in RP slot 0. • r1 --the RP in RP slot 1. • rp active --the active RP. • rp standby --the standby RP.
installed	Specifies information on the software installed on the RP
user-interface	Specifies information on the files related to the user-interface.
epld *slot*	(Optional) Specifies the software of the EPLD slot of a Cisco Catalyst 6500 Series Router.

Command Default No default behavior or values.

Command Modes User EXEC (>) Privileged EXEC (#) Diagnostic (diag)--Cisco ASR 1000 Series Routers only

Command History

Release	Modification
9.0	This command was introduced.
12.1EC	This command was integrated into Cisco IOS Release 12.1EC.
12.1(1a)T1	This command was modified to include information about the clock card on CMTS routers.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.3(4)T	The output format of this command was updated.
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 12.2(17d)SXB.
12.2(25)S	The output format of this command was updated.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.
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: • the command became available in diagnostic mode. • the *rp-slot*, **installed**, **user-interface**, **provisioned**, and **running** options all became available for the first time.
12.2(18)SX	Added ELPD keyword and output for the Cisco Catalyst 6500 Series Router.
Cisco IOS XE Release 2.4	The output format of this command was updated.
Cisco IOS XE Release 3.1.0.SG	This command was introduced on the Cisco Catalyst 4500e Serfies Switches with support for the rp-slot parameter and running command option.

Release	Modification
IOS XE 3.2.0 SE	Command introduced on the Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers with support for the switch keyword and running, provisioned and committed command options.

Usage Guidelines

This command displays information about the Cisco IOS software version currently running on a routing device, the ROM Monitor and Bootflash software versions, and information about the hardware configuration, including the amount of system memory. Because this command displays both software and hardware information, the output of this command is the same as the output of the **show hardware** command. (The **show hardware** command is a command alias for the **show version** command.)

Specifically, the **show version** command provides the following information:

- Software information
  - Main Cisco IOS image version
  - Main Cisco IOS image capabilities (feature set)
  - Location and name of bootfile in ROM
  - Bootflash image version (depending on platform)
- Device-specific information
  - Device name
  - System uptime
  - System reload reason
  - Config-register setting
  - Config-register settings for after the next reload (depending on platform)
- Hardware information
  - Platform type
  - Processor type
  - Processor hardware revision
  - Amount of main (processor) memory installed
  - Amount I/O memory installed
  - Amount of Flash memory installed on different types (depending on platform)
  - Processor board ID

The output of this command uses the following format:

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
  <software-type

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>,  <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>,  <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
```

```
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <
Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

See the Examples section for descriptions of the fields in this output.

Cisco ASR 1000 Series Routers

Entering **show version**without any of the options on the Cisco ASR 1000 Series Router will generate output similar to **show version** on other Cisco routers.

In order to understand the **show version**output on Cisco ASR 1000 Series Routers, it is important to understand that the individual sub-packages run the processes on the router. Among other things, the output of this command provides information on where various individual sub-packages are stored on the router, and which processes these individual sub-packages are and are not currently running.

More specifically, the command displays each individual sub-package file on the router, the hardware where the sub-package could be running, and whether the sub-package is currently being run on that hardware.

The **show version provisioned** command displays only the individual sub-packages that can be provisioned, which are the RP-specific sub-packages (RP Access, RP Base, RP Control, and RP IOS) and the provisioning file. The output includes the individual sub-package file, the hardware where the sub-package could be running, and whether the sub-package is currently being run on that hardware.

The command displays only the individual sub-packages that are currently active. The output includes the individual sub-package file and the hardware where the sub-package is running.

Cisco Catalyst 4500e Series Switches

Entering show version without any of the options on a Cisco Catalyst 4500e Series Switch running IOS XE software will generate output similar to **show version** on other Cisco platforms. One notable difference is that the output displays the IOS XE software version instead of the IOS image version.

The IOS XE software bundle includes a set of individual packages that comprise the complete set of software that runs on the switch. The **show version running** command displays the list individual packages that are currently active, that is, the set of packages included in the IOS XE software bundle currently running on the Cisco Catalyst 4500e Series Switch.

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers

Entering **show version** without any of the options on a Cisco Catalyst 3850 Series Switch or Cisco 5760 Series Wireless Controller will generate output similar to **show version** on other Cisco platforms. One notable difference is that the output displays the IOS XE software version instead of the IOS image version.

The IOS XE software bundle includes a set of individual packages that comprise the complete set of software that runs on the switch or wireless controller.

The **show version running** command displays the list of individual packages that are currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the bundle.

The **show version committed** command displays information about the switch's or wireless controller's committed package set. If no installation operations have been performed since bootup, this output will be the same as **show version running**. If any installation operations have been performed since bootup, this

output will display the set of packages that will be activated/running on the next reload. This command is not applicable when running in bundle mode.

The **show version provisioned** command displays information about the provisioned package set. In most cases, the provisioned package set is the same as the committed package set. These package sets will differ if an installation was performed with the **auto-rollback** option and the installed packages have not yet been committed by use of the **software commit** command. This command is not applicable when running in bundle mode.

Examples

Cisco 3660 Router

The following is sample output from the **show version** command issued on a Cisco 3660 running Cisco IOS Release 12.3(4)T:

```
Router# show version

Cisco IOS Software, 3600 Software (C3660-I-M), Version 12.3(4)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Thu 18-Sep-03 15:37 by ccai
ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)
ROM:
C3660-1 uptime is 1 week, 3 days, 6 hours, 41 minutes
System returned to ROM by power-on
System image file is "slot0:tftpboot/c3660-i-mz.123-4.T"
Cisco 3660 (R527x) processor (revision 1.0) with 57344K/8192K bytes of memory.
Processor board ID JAB055180FF
R527x CPU at 225Mhz, Implementation 40, Rev 10.0, 2048KB L2 Cache
3660 Chassis type: ENTERPRISE
2 FastEthernet interfaces
4 Serial interfaces
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of NVRAM.
16384K bytes of processor board System flash (Read/Write)
Flash card inserted. Reading filesystem...done.
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
Configuration register is 0x2102
```

Cisco 7200 Router

The following is sample output from the **show version** command issued on a Cisco 7200 router running Cisco IOS Release 12.4(4)T. This output shows the total bandwidth capacity and the bandwith capacity that is configured on the Cisco 7200. Displaying bandwidth capacity is available in Cisco IOS Release 12.2 and later releases.

```
Router# show version
Cisco IOS Software, 7200 Software (C7200-JS-M), Version 12.4(4)T, RELEASE SOFTW)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 27-Oct-05 05:58 by ccai
ROM: System Bootstrap, Version 12.1(20000710:044039) [nlaw-121E_npeb 117], DEVEE
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(16), RELEASE SOFTWARE (fc4)
router uptime is 5 days, 18 hours, 2 minutes
System returned to ROM by reload at 02:45:12 UTC Tue Feb 14 2006
System image file is "disk0:c7200-js-mz.124-4.T"
Last reload reason: Reload Command
Cisco 7206VXR (NPE400) processor (revision A) with 491520K/32768K bytes of memo.
Processor board ID 26793934
R7000 CPU at 350MHz, Implementation 39, Rev 3.2, 256KB L2 Cache
6 slot VXR midplane, Version 2.6
Last reset from power-on
```

```
PCI bus mb0_mb1 (Slots 0, 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb0_mb1 has a total of 440 bandwidth points.
This configuration is within the PCI bus capacity and is supported.
PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 390 bandwidth points
This configuration is within the PCI bus capacity and is supported.
Please refer to the following document "Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines" on Cisco.com <http://www.cisco.com>
for c7200 bandwidth points oversubscription and usage guidelines.
4 Ethernet interfaces
2 FastEthernet interfaces
2 ATM interfaces
125K bytes of NVRAM.
62976K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125952K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2002

Router#
```

For information about PCI buses and bandwidth calculation, go to the "Cisco 7200 Series Port Adapter Installation Requirements" chapter, of the *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines* guide.

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

Table 16 show version Field Descriptions

Field	Description
Cisco IOS Software, *platform* Software (*image-id*), Version *software-version*, *release-type* For example: Cisco IOS Software, 7200 Software (C7200-G4JS-M), Version 12.3(4)T	*platform* --Cisco hardware device name. *image-id* --The coded software image identifier, in the format *platform-features-format* (for example, “c7200-g4js-mz”. *software-version* --The Cisco IOS software release number, in the format *x.y*(*z*)*A*, where *x.y* is the main release identifier, *z* is the maintenance release number, and *A*, where applicable, is the special release train identifier. For example, 12.3(4)T indicates the fourth maintenance release of the 12.3T special technology release train. **Note** In the full software image filename, 12.3(4)T appears as 123-4.T. In the IOS Upgrade Planner, 12.3(4)T appears as 12.3.4T (ED). *release-type* --The description of the release type. Possible values include MAINTENANCE [for example, 12.3(3)] or INTERIM [for example, 12.3(3.2)]. **Tip** Refer to “The ABC’s of Cisco IOS Networking” (available on Cisco.com) for more information on Cisco IOS software release numbering and software versions. Cisco IOS is a registered trademark (R) of Cisco Systems, Inc.

Field	Description
Technical Support: http://www.cisco.com/techsupport Copyright (c) *date-range* by Cisco Systems, Inc.	The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. Cisco IOS software, including the source code, user-help, and documentation, is copyrighted by Cisco Systems, Inc. It is Cisco's policy to enforce its copyrights against any third party who infringes on its copyright.
ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)	The system "bootstrap" software, stored in ROM memory.
BOOTFLASH:	The system "bootflash" software, stored in Flash memory (if applicable).
device uptime is ... For example: C3660-1 uptime is 1 week, 3 days, 6 hours, 41 minutes	The amount of time the system has been up and running.
System returned to ROM by *reload-reason* at *timedaydate* For example: System returned to ROM by reload at 20:56:53 UTC Tue Nov 4 2003	Shows the last recorded reason for a system reload, and time of last reload.
Last reload reason: *reload-reason* For example: Last reload reason: Reload command	Shows the last recorded reason for a system reload.

Field	Description
Last reset from *reset-reason* For example: Last reset from power-on	Shows the last recorded reason for a system reset. Possible *reset-reason* values include: • power-on--System was reset with the initial power on or a power cycling of the device. • s/w peripheral--System was reset due to a software peripheral. • s/w nmi--System was reset by a nonmaskable interrupt (NMI) originating in the system software. For example, on some systems, you can configure the device to reset automatically if two or more fans fail. • push-button--System was reset by manual activation of a RESET push-button (also called a hardware NMI). • watchdog--System was reset due to a watchdog process. • unexpected value--May indicate a bus error, such as for an attempt to access a nonexistent address (for example, “System restarted by bus error at PC 0xC4CA, address 0x210C0C0”). (This field was formerly labeled as the “System restarted by” field.”)
System image file is “*file-location/ file-name* ” For example: System image file is "slot0:tftpboot/c3660-i-mz.123-3.9.T2"	Displays the file location (local or remote filesystem) and the system image name.

Field	Description
Cisco *platform* (*processor-type*) processor (revision *processor-revision-id*) with *free* - *DRAM-memory* K/ *packet-memory* K bytes of memory. Example--Separate DRAM and Packet Memory: Cisco RSP4 (R5000) processor with 65536K/ 2072K bytes of memory Example--Combined DRAM and Packet Memory: Cisco 3660 (R527x) processor (revision 1.0) with 57344K/8192K bytes of memory.	This line can be used to determine how much Dynamic RAM (DRAM) is installed on your system, in order to determine if you meet the "Min. Memory" requirement for a software image. DRAM (including SDRAM) is used for system processing memory and for packet memory. Two values, separated by a slash, are given for DRAM: The first value tells you how DRAM is available for system processing, and the second value tells you how much DRAM is being used for Packet memory. The first value, Main Processor memory, is either: • The amount of DRAM available for the processor, or • The total amount of DRAM installed on the system. The second value, Packet memory, is either: • The total physical input/output (I/O) memory (or "Fast memory") installed on the router (Cisco 4000, 4500, 4700, and 7500 series), or • The amount of "shared memory" used for packet buffering. In the shared memory scheme (Cisco 2500, 2600, 3600, and 7200 Series), a percentage of DRAM is used for packet buffering by the router's network interfaces. **Note** The terms "I/O memory" or "iomem"; "shared memory"; "Fast memory" and "PCI memory" all refer to "Packet Memory". Packet memory is either separate physical RAM or shared DRAM. Separate DRAM and Packet Memory The 4000, 4500, 4700, and 7500 series routers have separate DRAM and Packet memory, so you only need to look at the first number to determine total DRAM. In the example to the left for the Cisco RSP4, the first value shows that the router has 65536K (65,536 kilobytes, or 64 megabytes) of DRAM. The second value, 8192K, is the Packet memory. Combined DRAM and Packet Memory

Field	Description
	The 2500, 2600, 3600, and 7200 series routers require a minimum amount of I/O memory to support certain interface processors. The 1600, 2500, 2600, 3600, and 7200 series routers use a fraction of DRAM as Packet memory, so you need to add both numbers to find out the real amount of DRAM. In the example to the left for the Cisco 3660, the router has 57,344 kilobytes (KB) of free DRAM and 8,192 KB dedicated to Packet memory. Adding the two numbers together gives you 57,344K + 8,192K = 65,536K, or 64 megabytes (MB) of DRAM.
	For more details on memeory requirements, see the document "How to Choose a Cisco IOS® Software Release" on Cisco.com.
Configuration register is *value* For example: Configuration register is 0x2142 (will be 0x2102 at next reload)	Shows the current configured hex value of the software configuration register. If the value has been changed with the **config-register** command, the register value that will be used at the next reload is displayed in parenthesis. The boot field (final digit) of the software configuration register dictates what the system will do after a reset. For example, when the boot field of the software configuration register is set to 00 (for example, 0x0), and you press the NMI button on a Performance Route Processor (PRP), the user-interface remains at the ROM monitor prompt (rommon>) and waits for a user command to boot the system manually. But if the boot field is set to 01 (for example, 0x1), the system automatically boots the first Cisco IOS image found in the onboard Flash memory SIMM on the PRP. The factory-default setting for the configuration register is 0x2102. This value indicates that the router will attempt to load a Cisco IOS software image from Flash memory and load the startup configuration file.

Catalyst 6500 Series Switches and Cisco 7600 Series Routers

This example shows how to display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1 (nightly.E020626) NIG
HTLY BUILD
```

```
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 26-Jun-02 06:20 by
Image text-base: 0x40008BF0, data-base: 0x419BA000
ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)
Router uptime is 2 weeks, 8 hours, 48 minutes
Time since Router switched to active is 1 minute
System returned to ROM by power-on (SP by power-on)
System image file is "sup-bootflash:c6sup22-jsv-mz"
cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.
Processor board ID SAD06210067
R7000 CPU at 300Mhz, Implementation 39, Rev 3.3, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
3 Virtual Ethernet/IEEE 802.3  interface(s)
48 FastEthernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.
16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102
Router#
```

The following table describes the fields that are shown in the example.

Table 17 show version Field Descriptions

Field	Description
IOS (tm) c6sup2_rp Software (c6sup2_rp-JSV-M), Version 12.1(nightly.E020626) NIGHTLY BUILD	Version number. Always specify the complete version number when reporting a possible software problem. In the example output, the version number is 12.1.
ROM: System Bootstrap, Version 12.1(11r)E1, RELEASE SOFTWARE (fc1)	Bootstrap version string.
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE	Boot version string.
Router uptime is	Amount of time that the system has been up and running.
Time since Router switched to active	Amount of time since switchover occurred.
System restarted by	Log of how the system was last booted, both as a result of normal system startup and of system error. For example, information can be displayed to indicate a bus error that is typically the result of an attempt to access a nonexistent address, as follows: System restarted by bus error at PC 0xC4CA, address 0x210C0C0
System image file is	If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”

Field	Description
cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.	Remaining output in each display that shows the hardware configuration and any nonstandard software options.
Configuration register is	Configuration register contents that are displayed in hexadecimal notation.

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

This example shows how to display the ELPD version information of a slot:

```
Router# show version epld 4

Module 4 EPLD's:
Number of EPLD's: 6
EPLD A : 0x5
EPLD B : 0x2
EPLD C : 0x1
EPLD D : 0x1
EPLD E : 0x1
Router#
```

Cisco uBR7246VXR Router

The following is sample output from the **show version** command for a Cisco uBR7246 VXR with the cable clock card installed:

```
Router#
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-P-M), Version 12.1(10)EC, RELEASE SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 02-Feb-00 16:49 by ccai
Image text-base:0x60008900, data-base:0x61192000
ROM:System Bootstrap, Version 12.0(15)SC, RELEASE SOFTWARE
VXR1 uptime is 2 days, 1 hour, 24 minutes
System returned to ROM by power-on at 10:54:38 PST Sat Feb 5 2000
System restarted at 11:01:08 PST Sat Feb 5 2000
System image file is "slot1:ubr7200-p-mz.121-0.8.T"
cisco uBR7246VXR (NPE300) processor (revision B) with 122880K/40960K bytes of memory.
Processor board ID SAB0329005N
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0
Last reset from power-on
X.25 software, Version 3.0.0.
National clock card with T1 controller
1 FastEthernet/IEEE 802.3 interface(s)
2 Cable Modem network interface(s)
125K bytes of non-volatile configuration memory.
16384K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
20480K bytes of Flash PCMCIA card at slot 1 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
Router#
```

The following table describes significant fields shown in these displays.

Table 18 show version Field Descriptions

Field	Description
IOS (tm) 7200 Software (UBR7200-P-M), Version xx.x	Always specify the complete version number when reporting a possible software problem. In the example, the version number is Cisco IOS Release 12.1(10)EC.
ROM: System Bootstrap	Bootstrap version string.
Router uptime is	The amount of time the system has been up and running.
System restarted at	Also displayed is a log of how the system was last booted, as a result of normal system startup or system error.
System image file is	If the software was booted over the network, the Internet address of the boot host is shown. If the software was loaded from onboard ROM, this line reads “running default software.”
cisco uBR7246VXR (NPE300) processor	The remaining output in each display shows the hardware configuration and any nonstandard software options.
Configuration register is	The configuration register contents, displayed in hexadecimal notation.

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

Cisco uBR10012 Router

The following example shows sample output from the show version command on a Cisco uBR10012 universal broadband router running Cisco IOS Release 12.3(17b)BC4:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K2-K9P6U2-M), Version 12.3(17b)BC4, RELEASE SOFTWA
RE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Wed 22-Nov-06 11:41 by tinhuang
Image text-base: 0x60010F0C, data-base: 0x62480000
ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios-rommon 1
12], DEVELOPMENT SOFTWARE
ubr10k uptime is 2 days, 22 hours, 13 minutes
System returned to ROM by reload at 01:34:58 UTC Sun Jun 8 2008
System image file is "disk0:ubr10k2-k9p6u2-mz.123-17b.BC4"
Last reload reason: Reload command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
```

```
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco uBR10000 (PRE2-RP) processor with 946175K/98304K bytes of memory.
Processor board ID TBA05380380
R7000 CPU at 500MHz, Implementation 39, Rev 4.1, 256KB L2, 8192KB L3 Cache
Backplane version 1.1, 8 slot
Last reset from register reset
PXF processor tmc0 is running.
PXF processor tmc1 is running.
PXF processor tmc2 is running.
PXF processor tmc3 is running.
1 TCCplus card(s)
1 FastEthernet/IEEE 802.3 interface(s)
3 Gigabit Ethernet/IEEE 802.3 interface(s)
24 Cable Modem network interface(s)
2045K bytes of non-volatile configuration memory.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
125440K bytes of ATA PCMCIA card at slot 1 (Sector size 512 bytes).
65536K bytes of Flash internal SIMM (Sector size 512KB).
Secondary is up.
Secondary has 1044480K bytes of memory.
Configuration register is 0x2102
```

Cisco ASR 1000 Series Routers

In Cisco IOS XE Release 2.4

```
In the following example, the show version command is responsible for displaying the
packages installed, provisioned and running on the current RP.
```

In the following example, the command is entered on a Cisco ASR 1000 Series Router in diagnostic mode. Note that the output shows what every file that can be found in the consolidated package is or is not currently running (provisioning file, RP Access, RP Base, RP Control, RP IOS, ESP Base, SIP Base, SIP SPA).

```
PE23_ASR-1006#
Package: Provisioning File, version: n/a, status: active
  File: consolidated:packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: b6cb06b1ed02e041d48644340aa077833cff2076
Package: rpbase, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpbase.02.04.00.122-33.XND.pkg, on: RP0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 093f2c935b9dc4ed136623bc43488c6517b9a4ae
Package: rpcontrol, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP0/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP0/1
  Built: 2009-06-29_23.07, by: mcpre
```

```
  File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: rpbase, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpbase.02.04.00.122-33.XND.pkg, on: RP1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 093f2c935b9dc4ed136623bc43488c6517b9a4ae
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP1/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP1/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d
Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP1/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: rpcontrol, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpcontrol.02.04.00.122-33.XND.pkg, on: RP1/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: d71e05c824cb889048b3353257bd16129eb72c44
Package: rpios-advipservicesk9, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpios-advipservicesk9.02.04.00.122-33.XND.pkg, on: RP1/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 4167d300514153f67c3815c487c270c14449185d

Package: rpaccess, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-rpaccess.02.04.00.122-33.XND.pkg, on: RP1/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 0b0d108cd2683570778668697b7ffca2451b78b3
Package: espbase, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-espbase.02.04.00.122-33.XND.pkg, on: ESP0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 3ae9255c7272a30f5dae319dec109acd29d9ae87
Package: espbase, version: 02.04.00.122-33.XND, status: inactive
  File: consolidated:asr1000rp1-espbase.02.04.00.122-33.XND.pkg, on: ESP1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 3ae9255c7272a30f5dae319dec109acd29d9ae87
Package: sipbase, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP0/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP0/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP0/2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP0/3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipbase, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP1/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP1/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: active
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP1/2
  Built: 2009-06-29_23.07, by: mcpre
```

```
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP1/3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipbase, version: 02.04.00.122-33.XND, status: inactive
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP2/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP2/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP2/2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP2/3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipbase, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP3/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP3/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP3/2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP3/3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836

Package: sipbase, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP4
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP4/0
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP4/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP4/2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP4/3
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipbase, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipbase.02.04.00.122-33.XND.pkg, on: SIP5
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: fc6e41d7de2ded3a16b6dc7e5e3a1151b788d254
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP5/0
  Built: 2009-06-29_23.07, by: mcpre
```

```
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP5/1
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: sipspa, version: 02.04.00.122-33.XND, status: n/a
  File: consolidated:asr1000rp1-sipspa.02.04.00.122-33.XND.pkg, on: SIP5/2
  Built: 2009-06-29_23.07, by: mcpre
  File SHA1 checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
Package: Sipspa, Version: 02.04.00.122-33.xnd, Status: N/a
  File: Consolidated:asr1000rp1-sipspa.02.04.00.122-33.xnd.pkg, On: Sip5/3
  Built: 2009-06-29_23.07, By: Mcpre
  File Sha1 Checksum: 24fb5b788582e062c900e2713b5c56a2704ca836
```

Table 19 show version installed, provisioned, and running Field Descriptions

Field	Description
Package:	The individual sub-package name.
version:	The consolidated package version of the individual sub-package.
status:	Reveals if the sub-package is active or inactive for the specific hardware component only.
File:	The location and filename of the individual sub-package file.
on:	The hardware component.
Built:	The date the individual sub-package was built.
File SHA1 checksum:	The SHA1 sum for the file. This sum can be compared against a SHA1 sum generated by any SHA1 sum-generating tool.

Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers

The following is sample output from the show version command on a Cisco Catalyst 3850 Series Switch that is the active switch in a 2-member stack:

```
infra-p2-3#show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-
M), Version 03.09.19.EMP EARLY DEPLOYMENT ENGINEERING NOVA_WEEKLY BUILD, synced to
DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 15-Nov-12 01:45 by udonthi

ROM: IOS-XE ROMMON
BOOTLDR: C3850 Boot Loader (C3850-HBOOT-M) Version 1.2, engineering software (D)

infra-p2-3 uptime is 5 minutes
Uptime for this control processor is 7 minutes
System returned to ROM by reload
System image file is "flash:packages.conf"
Last reload reason: Reload command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
```

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

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: Ipservices
License Type: Permanent
Next reload license Level: Ipservices

cisco WS-C3850X-24P-PROTO2 (MIPS) processor with 2097152K bytes of physical memory.
Processor board ID FHH1515P03Y
1 Virtual Ethernet interface
56 Gigabit Ethernet interfaces
8 Ten Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
2097152K bytes of physical memory.
160618K bytes of Crash Files at crashinfo:.
160618K bytes of Crash Files at crashinfo-1:.
706860K bytes of Flash at flash:.
698827K bytes of Flash at flash-1:.
3915670K bytes of USB Flash at usbflash0:.
0K bytes of Dummy USB Flash at usbflash0-1:.
0K bytes of  at webui:.

Base Ethernet MAC Address          : 64:00:f1:25:11:00
Motherboard Assembly Number        : 73-12240-03
Motherboard Serial Number          : FHH15130010
Model Revision Number              : 01
Motherboard Revision Number        : 02
Model Number                       : WS-C3850X-24P-PROTO2
System Serial Number               : FHH1515P03Y


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
     1 32    WS-C3850X-24P-PROT 03.09.19.EMP      cat3k_caa-universalk9 INSTALL
     2 32    WS-C3850X-24P-PROT 03.09.19.EMP      cat3k_caa-universalk9 INSTALL


Switch 01
---------
Switch uptime                      : 7 minutes
Base Ethernet MAC Address          : 64:00:f1:25:1a:00
Motherboard Assembly Number        : 73-12240-03
Motherboard Serial Number          : FHH1513000T
Model Revision Number              : 01
Motherboard Revision Number        : 02
Model Number                       : WS-C3850X-24P-PROTO2
System Serial Number               : FHH1515P047

Configuration register is 0x2 (will be 0x102 at next reload)

infra-p2-3#
```

In the following example, the show version running command is entered on a Cisco Catalyst 3850 Series Switch to view information about the packages currently running on both switches in a 2-member stack:

```
infra-p2-3#show version running
Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi
```

```
Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi


Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi
```

In the following example, the show version provisioned and show version committed commands are entered on a Cisco Catalyst 3850 Series Switch that is the active switch in a 2-member stack. The show version committed commands displays information about the packages in the committed package set that will be running on the next reload. The show version provisioned command displays information about the packages in the provisioned package set.

In most cases, the show version provisioned and show version committed output will display the same information, since the provisioned and committed packages sets include the same packages. The provisioned package set may differ from the committed package set in cases where a **software install** operation was performed with the **auto-rollback** command option, and the **software commit** command has not yet been entered. This is the case in the sample output below, where the packages from the 03.09.19.EMP were installed with the **auto-rollback** command option, but the 'software commit' command has not yet been entered.

The show version provisioned and show version committed commands are not applicable when the switch is booted in bundle mode.

```
infra-p2-3#show version provisioned
Package: Provisioning File, version: n/a, status: active
  File: packages.conf, on: Switch1
  Built: n/a, by: n/a

Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
```

```
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi


Package: Provisioning File, version: n/a, status: active
  File: packages.conf, on: Switch2
  Built: n/a, by: n/a

Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch2
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi


infra-p2-3#show version committed

Package: Provisioning File, version: n/a, status: active
  File: packages.conf, on: Switch1
  Built: n/a, by: n/a

Package: Base, version: 03.09.17.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.17.EMP.pkg, on: Switch1
  Built: Mon Nov 12 20:27:51 PST 2012, by: udonthi

Package: Infra, version: 03.09.17.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.17.EMP.pkg, on: Switch1
  Built: Mon Nov 12 20:28:53 PST 2012, by: udonthi

Package: Platform, version: 03.09.17.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.17.EMP.pkg, on: Switch1
  Built: Mon Nov 12 20:29:33 PST 2012, by: udonthi

Package: IOS, version: 150-9.17.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg, on: Switch1
  Built: Mon Nov 12 20:29:58 PST 2012, by: udonthi

Package: WCM, version: 03.09.17.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.17.EMP.pkg, on: Switch1
  Built: Mon Nov 12 20:30:29 PST 2012, by: udonthi

Package: Drivers, version: 03.09.17.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.17.EMP.pkg, on: Switch1
```

```
  Built: Mon Nov 12 20:31:01 PST 2012, by: udonthi


Package: Provisioning File, version: n/a, status: active
  File: packages.conf, on: Switch2
  Built: n/a, by: n/a

Package: Base, version: 03.09.17.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:27:51 PST 2012, by: udonthi

Package: Infra, version: 03.09.17.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:28:53 PST 2012, by: udonthi

Package: Platform, version: 03.09.17.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:33 PST 2012, by: udonthi

Package: IOS, version: 150-9.17.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:58 PST 2012, by: udonthi

Package: WCM, version: 03.09.17.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:30:29 PST 2012, by: udonthi

Package: Drivers, version: 03.09.17.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:31:01 PST 2012, by: udonthi


infra-p2-3#
```

Table 20 ***Table 5,Cisco Catalyst 3850 Series Switches and Cisco 5760 Series Wireless Controllers show version running Field Descriptions***

Field	Description
Package:	The individual sub-package name.
version:	The individual sub-package version.
status:	Reveals if the package is active or inactive for the specific Supervisor module.
File:	The filename of the individual package file.
on:	The slot number of the Active or Standby Supervisor that this package is running on.
Built:	The date the individual package was built.

Cisco Catalyst 4500e Series Switches

The following is sample output from the show version command on a Cisco Catalyst 4500e Series Switch running IOS XE software:

```
Switch#show version
Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
(cat4500e-UNIVERSALK9-M), Experimental Version 3.1.0.SG
[/nobackup/xxxx/cwab/build/arch_ppc/buildtree-ios/vob/ios/sys 100] Copyright (c)
1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Apr-10 09:19 by xxxx

Cisco IOS-XE software, Copyright (c) 2005-2010 by cisco Systems, Inc.
```

```
All rights reserved. Certain components of Cisco IOS-XE software are licensed under the
GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL
Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can
redistribute
and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see
the documentation or "License Notice" file accompanying the IOS-XE software, or the
applicable URL provided on the flyer accompanying the IOS-XE software.


Image text-base: 0x100D9954, data-base: 0x14B379D8

ROM: 12.2(54r)XO(0.246)
Jawa Revision 7, Snowtrooper Revision 0x0.0x14

gsgsw-g9-35 uptime is 4 minutes
Uptime for this control processor is 5 minutes System returned to ROM by reload System
image file is "tftp://1.2.3.4/tftpboot/xxxx/x.bin"

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S.
and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Information for 'iosd'
 License Level: entservices Type: Evaluation
 Next reboot license Level: entservices

cisco WS-C4510R-E (MPC8572) processor (revision 2) with 786516K/16384K bytes of memory.
Processor board ID SPE1046002Q
MPC8572 CPU at 1.5GHz, Supervisor 7
Last reset from Reload
1 Virtual Ethernet interface
84 Gigabit Ethernet interfaces
14 Ten Gigabit Ethernet interfaces

Configuration register is 0x920

Switch#
```

In the following example, the show version running command is entered on a Cisco Catalyst 4500e Series Switch to view the list of packages contained in the IOS XE software bundle currently loaded on the system.

```
Switch# show version running

Package: Base, version: 3.0.0, status: active
30
 File: cat4500e-base.SSA.3.0.0.pkg, on: Slot5
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:08:38 PDT 2010, by: xxxx

Package: Infra, version: 3.0.0, status: active
 File: cat4500e-infra.SSA.3.0.0.pkg, on: Slot5
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:09:30 PDT 2010, by: xxxx

Package: IOS, version: 150-1.XO, status: active
 File: cat4500e-universalk9.SSA.150-1.XO.pkg, on: Slot5
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:10:02 PDT 2010, by: xxxx
```

```
Package: Base, version: 3.0.0, status: active
 File: cat4500e-base.SSA.3.0.0.pkg, on: Slot6
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:08:38 PDT 2010, by: xxxx

Package: Infra, version: 3.0.0, status: active
 File: cat4500e-infra.SSA.3.0.0.pkg, on: Slot6
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:09:30 PDT 2010, by: xxxx

Package: IOS, version: 150-1.XO, status: active
 File: cat4500e-universalk9.SSA.150-1.XO.pkg, on: Slot6
 From Bundle: cat4500e-universalk9.SSA.3.1.0.SG
 Built: Mon Apr 19 10:10:02 PDT 2010, by: xxxx
 Switch#
```

Table 21 Table 6,Cisco Catalyst 4500e Series Switches show version running Field Descriptions

Field	Description
Package:	The individual sub-package name.
version:	The individual sub-package version.
status:	Reveals if the package is active or inactive for the specific Supervisor module.
File:	The filename of the individual package file.
on:	The slot number of the Active or Standby Supervisor that this package is running on.
From Bundle:	The name of the IOS XE software bundle that includes this package.
Built:	The date the individual package was built.

Related Commands

Command	Description
show diag	Displays hardware and diagnostic information for a networking device, a line card, a processor, a jacket card, a chassis, or a network module.
show inventory	Displays the Cisco Unique Device Identifier information, including the Product ID, the Version ID, and the Serial Number, for the hardware device and hardware components.

software clean

To remove any and all packages and provisioning files that are no longer in use, use the **software clean** command in Privileged EXEC mode.

software clean[**file***file url*][**switch***nodes*] [**verbose**]

Syntax Description

file*file url*	Full path to wildcarded filename(s). Optional when running in installed mode. When no command options are specified, all unused package, bundle and provisioning files in the current boot directory will be cleaned.
switch*nodes*	(optional) Specifies which switch(es) should perform the clean operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
verbose	(optional) provides some additional info in the log files .

Command Default

No software package(s) will be cleaned by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

If no specific file to be deleted is indicated, the installer will search for unused packages and provisioning files on a given media device (eg., bootflash:, usb0: etc) to delete. One or more nodes may be given.

With no options specified for **software clean**, all unused packages and provisioning files on the currently booted device will be cleaned. The currently booted device is where the committed `packages.conf` file resides.

Examples

This example uses the 'software clean' command with no command options to clean the current boot directory, flash:, on a standalone switch that is running in installed mode.

```
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 09:45:11 +00:00  nvram_config
 7379  drwx        4096  Nov 15 2012 09:19:24 +00:00  mnt
 7396  -rwx        1244  Nov 14 2012 18:32:55 +00:00  packages.conf.00-
 7390  -rwx    74390300  Nov 15 2012 09:18:17 +00:00  cat3k_caa-base.SSA.
03.09.17.EMP.pkg
 7383  -rwx    74601776  Nov 14 2012 18:31:59 +00:00  cat3k_caa-base.SSA.
03.09.16.EMD.pkg
 7384  -rwx     2732724  Nov 14 2012 18:32:08 +00:00  cat3k_caa-drivers.SSA.
03.09.16.EMD.pkg
 7385  -rwx    49886128  Nov 14 2012 18:32:02 +00:00  cat3k_caa-infra.SSA.
03.09.16.EMD.pkg
 7387  -rwx    30579500  Nov 14 2012 18:32:05 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.16.EMD.pkg
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7389  -rwx    62814928  Nov 14 2012 18:32:08 +00:00  cat3k_caa-wcm.SSA.03.09.16.EMD.pkg
 7388  -rwx    18193120  Nov 14 2012 18:32:03 +00:00  cat3k_caa-platform.SSA.
03.09.16.EMD.pkg
 7397  -rwx        1243  Nov 15 2012 09:18:55 +00:00  packages.conf
 7391  -rwx     2734772  Nov 15 2012 09:18:17 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7392  -rwx    32465772  Nov 15 2012 09:18:24 +00:00  cat3k_caa-infra.SSA.
03.09.17.EMP.pkg
 7393  -rwx    30384940  Nov 15 2012 09:18:35 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7394  -rwx    18143968  Nov 15 2012 09:18:39 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7395  -rwx    62638800  Nov 15 2012 09:18:51 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (208535552 bytes free)
infra-p2-3#
infra-p2-3#software clean
Preparing clean operation ...
[2]: Cleaning up unnecessary package files
[2]: No path specified, will use booted path flash:packages.conf
[2]: Cleaning flash:
[2]: Preparing packages list to delete ...
    cat3k_caa-base.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-infra.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-platform.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    packages.conf
        File is in use, will not delete.
[2]: Files that will be deleted:
    cat3k_caa-base.SSA.03.09.16.EMD.pkg
    cat3k_caa-drivers.SSA.03.09.16.EMD.pkg
    cat3k_caa-infra.SSA.03.09.16.EMD.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.16.EMD.pkg
    cat3k_caa-platform.SSA.03.09.16.EMD.pkg
```

```
    cat3k_caa-wcm.SSA.03.09.16.EMD.pkg
    packages.conf.00-

[2]: Do you want to proceed with the deletion? [yes/no]: y
[2]: Clean up completed


infra-p2-3#
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 09:45:11 +00:00  nvram_config
 7379  drwx        4096  Nov 15 2012 09:19:24 +00:00  mnt
 7390  -rwx    74390300  Nov 15 2012 09:18:17 +00:00  cat3k_caa-base.SSA.
03.09.17.EMP.pkg
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7397  -rwx        1243  Nov 15 2012 09:18:55 +00:00  packages.conf
 7391  -rwx     2734772  Nov 15 2012 09:18:17 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7392  -rwx    32465772  Nov 15 2012 09:18:24 +00:00  cat3k_caa-infra.SSA.
03.09.17.EMP.pkg
 7393  -rwx    30384940  Nov 15 2012 09:18:35 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7394  -rwx    18143968  Nov 15 2012 09:18:39 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7395  -rwx    62638800  Nov 15 2012 09:18:51 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (447623168 bytes free)
infra-p2-3#
```

Related Commands

Command	Description
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software commit

To commit a package set that was installed using the **auto-rollback** command option of the **software install** command, use the **software commit** command in Privileged EXEC mode.

software commit[**switch***node*] [**verbose**]

Syntax Description

switch*nodes*	(optional) specifies which switch(es) should perform the commit operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack
verbose	(optional) provides some additional info in the log files

Command Default

No software package(s) will be committed by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software commit** command cancels the rollback timer, if it is running, and commits a software upgrade. A commit makes an upgrade, ie. a package set, persistent. A committed package set will run after a node is reloaded.

Examples

This example uses the 'software install file' command with the 'auto-rollback' command option to install the bundle onto both switches in a stack via tftp . After the switches reload with the new software, the 'software commit' command is used to stop the rollback timer and commit the candidate package set.

```
infra-p2-3#software install file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.
03.09.19.EMP.150-9.19.EMP.bin auto-rollback 45
Preparing install operation ...
[2]: Downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.19.EMP.
150-9.19.EMP.bin to active switch 2
[2]: Finished downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.
03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Copying software from active switch 2 to switch 1
[2]: Finished copying software to switch 1
[1 2]: Starting install operation
[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Copying package files
[1 2]: Package files copied
[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Verifying and copying expanded package files to flash:
[1 2]: Verified and copied expanded package files to flash:
[1 2]: Starting compatibility checks
[1 2]: Finished compatibility checks
[1 2]: Starting application pre-installation processing
[1 2]: Finished application pre-installation processing
[1]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[1 2]: Creating pending provisioning file
[1 2]: Finished installing software.  New software will load on reboot.
[1 2]: Setting rollback timer to 45 minutes

[1 2]: Do you want to proceed with reload? [yes/no]: y
[1]: Reloading
[2]: Pausing before reload
*Nov 15 10:24:24.891: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for switch 1, reason User requested reload
*Nov 15 10:24:25.051: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr:  Stack port 2 on
switch 2 is down
*Nov 15 10:24:25.051: %STACKMGR-1-SWITCH_REMOVED: 2 stack-mgr:  Switch 1 has been
removed from the stack
*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby
removal (raw-event=PEER_NOT_PRESENT(3))

*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected standby down or
crashed (raw-event=PEER_DOWN(2))
```

```
*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby
removal (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Nov 15 10:24:27.054: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to
down
*Nov 15 10:24:28.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/1, changed state to down
[2]: Reloading

infra-p2-3#
*Nov 15 10:24:39.911: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for switch 2, reason User requested reload
*Nov 15 10:24:39.912: %STACKMGR-1-RELOAD: 2 stack-mgr:  reloading due to reason User
requested reload
*Nov 15 10:24:40.423: %IOSXE-3-PLATFORM: 2 process sysmgr: Reset/Reload requested by
[stack-manager].

< Switches were reloaded and booted with the newly installed software>

*Nov 15 10:34:21.345: %AUTHMGR_SPI-6-START: Auth Manager SPI server started (infra-
p2-3-1)
*Nov 15 10:34:24.612: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Nov 15 10:34:24.624: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Nov 15 10:34:24.510: %SSH-5-DISABLED: SSH 1.99 has been disabled (infra-p2-3-1)
*Nov 15 10:34:24.511: %SSH-5-ENABLED: SSH 1.99 has been enabled (infra-p2-3-1)
infra-p2-3#
infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           active      00:31:28
2           active      00:31:43

infra-p2-3#
infra-p2-3#software commit
Preparing commit operation ...
[1 2]: Starting commit operation
[1 2]: Finished committing software changes.


infra-p2-3#
infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           inactive       -
2           inactive       -

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.

Command	Description
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software expand

To expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory, use the **software expand** command in Privileged EXEC mode.
To expand the individual IOS XE Software packages and the provisioning file from the running bundle, use the **software expand running** command in Privileged EXEC mode.

software expand {**file** *source url* | **running**}[**to***destination url*] [**switch***nodes*][**verbose**]

Syntax Description

file*source url*	URL of the bundle to be expanded. If a network URL is specified, the **to** keyword must also be used to specify the destination location. The **file** and **running** keywords are mutually exclusive
running	Specifies that the packages from the running bundle should be expanded . The **to** keyword must also be used to specify the destination location . The **file** and **running** keywords are mutually exclusive . The running command option is not allowed when running in installed mode.

to*destination url*	Specifies the local or UFS directory where the expanded bundle contents are copied to. **Note** If this option is not entered, the contents are extracted into the same directory as the source bundle. This keyword is mandatory when the source URL is a network URL, and also when the **running** keyword is used .
switch*nodes*	(optional) Specifies which switch(es) should perform the expand operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
verbose	(optional) provides some additional info in the log files

Command Default

Command is used to expand an IOS XE software bundle. The contents are extracted into the same directory as the source bundle by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

If the **to** option is not entered, the contents will be extracted into the default installation location for the platform.

The bundle file is unchanged after the operation is complete.

Examples

This example uses the following steps to prepare a switch for booting in installed mode, i.e., booting a package provisioning file (packages.conf)

1. Boot in bundle mode using 'boot flash:<bundle name>' Can also boot from usbflash0 : or via tftp

```
switch: b tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin
Reading full image into
memory................................................................................
......................................................................................
............................................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042fef4
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60747bc0
Initramfs Size    : 0xdbf2f9/14414585
Compression Format: .mzip

Bootable image at @ ram:0x6042fef4
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range
[0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin"
uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services

:
:

*Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/1, changed state to down
*Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/2, changed state to down
*Nov 15 10:49:36.822: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to
up
infra-p2-3>
infra-p2-3>enable
infra-p2-3#
```

2. Use the 'software clean file flash:' command to remove any unused package, bundle and provisioning files from flash:

```
infra-p2-3#software clean file flash:
Preparing clean operation ...
[2]: Cleaning up unnecessary package files
[2]: Preparing packages list to delete ...
[2]: Files that will be deleted:
    cat3k_caa-base.SSA.03.09.19.EMP.pkg
    cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
    packages.conf

[2]: Do you want to proceed with the deletion? [yes/no]: yes
[2]: Clean up completed


infra-p2-3#
```

3. Use the 'software expand running to flash:' command to expand the running bundle to flash:

```
infra-p2-3#software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle
```

```
infra-p2-3#
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 10:49:37 +00:00  nvram_config
14753  drwx        4096  Nov 15 2012 10:20:27 +00:00  mnt
 7381  -rw-    74390300  Nov 15 2012 10:54:24 +00:00  cat3k_caa-base.SSA.
03.09.17.EMP.pkg
 7382  -rw-     2734772  Nov 15 2012 10:54:24 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7383  -rw-    32465772  Nov 15 2012 10:54:24 +00:00  cat3k_caa-infra.SSA.
03.09.17.EMP.pkg
 7384  -rw-    30384940  Nov 15 2012 10:54:24 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7385  -rw-    18143968  Nov 15 2012 10:54:24 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7380  -rw-        1243  Nov 15 2012 10:55:03 +00:00  packages.conf
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7387  -rw-    62638800  Nov 15 2012 10:54:24 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (447627264 bytes free)
infra-p2-3#
```

4. Reload the switch

```
infra-p2-3#reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

*Nov 15 10:56:35.800: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
command.
*Nov 15 10:56:36.569: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for
all switches, reason Reload command
*Nov 15 10:56:36.570: %STACKMGR-1-RELOAD: 2 stack-mgr:  reloading due to reason Reload
command
*Nov 15 10:56:37.071: %IOSXE-3-PLATFORM: 2 process sysmgr: Reset/Reload requested by
[stack-manager].
<Thu Nov 15 10:56:37 2012> Message from sysmgr: Reset Reason:Reset/Reload requested by
[stack-manager]. [Reload command]
```

5. Boot the installed packages using 'boot flash:packages.conf '

```
switch: boot flash:packages.conf
Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74390300
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042f354
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60747020
Initramfs Size    : 0xdbf2f9/14414585
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
boot_system: 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

All packages are Digitally Signed
Starting System Services

:
:

*Nov 15 11:05:23.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/1, changed state to down
```

```
*Nov 15 11:05:23.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/2, changed state to down
*Nov 15 11:05:24.286: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to
up
infra-p2-3>
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software install file

To install IOS XE Software files, use the **software install file** command in Privileged EXEC mode.

software install file *bundle url* [**switch***nodes*] [**auto-rollback***minutes*][**force**][**on-reboot**] [**provisioning-file***provisioning-file url*][**force**][**new**][**verbose**]

Syntax Description

file *bundle url*	Specify the url of the bundle file to be installed.
switch*nodes*	(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
auto-rollback*minutes*	(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit '). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).

on-reboot	(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.
provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:
force	(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
new	(optional) Indicates that the post-install package set should contain only the packages being installed. Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.
verbose	(optional) provides some additional info in the log files

Command Default Command is used to install IOS XE software. No software will be installed by default.

Command Modes Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software install file** command is used to install package files from a software bundle when the system is running in installed mode. By default, the command will install software on all nodes in the system.

The following tasks are performed during the **software install file** operation.

- For a network installation, download the specified software bundle into memory on the active node (or standalone node is a standalone system).

- In a multi-node system, copy the software bundle to each node if the file does not already exist on the node. If installing a bundle that resides in local media on the active node (flash: or usbflash0:), the bundle file (.bin) is copied to the corresponding local device on each node. If installing a bundle via the network, the bundle is copied to memory on each node in the system.

- Expand the package files from the specified bundle into flash: on each node after verifying each package's digital signature

- Perform compatibility checks on all nodes in the system to ensure that the software running on all nodes after installation will be compatible. This task is skipped if the **force** command option is used.

- Start the auto-rollback timer if the **auto-rollback** command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the 'software commit' command is issued.

- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (**software rollback** command).

- Commit the newly installed software packages if the **auto-rollback** command option was not used.

- Prompt the user to reload (if the **on-reboot** command option was not used).

Note The **software install file** command cannot be used if the system is running in bundle mode. In this case, the **software expand** command can be used to prepare the system to boot in installed mode.

Examples

The following example installs the cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin bundle from a tftp server. The bundle is first downloaded to RAM, then the package files included in the bundle are extracted and copied to flash:. The .bin file itself is not copied to flash:.

Note You need IOSd IP connectivity to install via tftp .

```
infra-p2-3#software install file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
Preparing install operation ...
[2]: Downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Finished downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Starting install operation
```

```
[2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[2]: Verifying and copying expanded package files to flash:
[2]: Verified and copied expanded package files to flash:
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software.  New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]: n

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.

Command	Description
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software install source switch

To install the running IOS XE software packages from one stack member to one or more other stack members, use the **software install source switch** command in Privileged EXEC mode.

software install source switch*node* [**switch***node*] [**auto-rollback***minutes*][**force**][**on-reboot**] [**verbose**][**new**][**provisioning-file***provisioning-file url*]

Syntax Description

switch*node*	Specifies which switch in the stack to use as the package source. Only a single switch may be specified and there is no default value
switch*nodes*	(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.

auto-rollback*minutes*	(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit '). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).
force	(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
on-reboot	(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.
verbose	(optional) provides some additional info in the log files
new	(optional) Indicates that the post-install package set should contain only the packages being installed. Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.

provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:

Command Default

Command is used to install IOS XE software. No software will be installed by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software install source switch** command is used to install the running package files from one stack member to one or more other stack members while the system is running in installed mode.

The following tasks are performed during the **software install source switch** operation.

- Copy the running software packages from flash: on the specified source switch to flash: on all other switches specified in the command.

- Perform compatibility checks on all switches in the stack to ensure that the software running on all stack members after installation will be compatible. This task is skipped if the **force** command option is used.

- Start the auto-rollback timer if the **auto-rollback** command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the **software commit** command is issued.

- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (**software rollback** command).

- Commit the newly installed software packages if the **auto-rollback** command option was not used.

- Prompt the user to reload (if the **on-reboot** command option was not used).

Note The **software install source switch** command cannot be used if the system is running in bundle mode. In this case, the **software expand** command can be used to prepare the system to boot in installed mode.

Examples

In the following example, the switches in a 2-member stack are running different (but compatible) software packages. The **software install source switch** command is used to install the currently running packages on the standby switch (switch 1) to the active switch (switch 2).

```
infra-p2-3#show version running
Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi


Package: Base, version: 03.09.17.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:27:51 PST 2012, by: udonthi

Package: Drivers, version: 03.09.17.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:31:01 PST 2012, by: udonthi

Package: Infra, version: 03.09.17.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:28:53 PST 2012, by: udonthi

Package: IOS, version: 150-9.17.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:58 PST 2012, by: udonthi

Package: Platform, version: 03.09.17.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:33 PST 2012, by: udonthi

Package: WCM, version: 03.09.17.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:30:29 PST 2012, by: udonthi



infra-p2-3#
infra-p2-3#software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
```

```
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software.  New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]: no

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software rollback

To roll back the committed Cisco IOS XE Software to a previous installation point, use the **software rollback** command in Privileged EXEC mode.

software rollback [**switch***node*] [**as-booted**][**provisioning-file***provisioning-file url*][**on-reboot**] [**force**][**verbose**]

Syntax Description

switch*nodes*	(optional) specifies which switch(es) should perform the rollback operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack
as-booted	(optional) Used to rollback any installations that have occurred since bootup and commit the booted packages.conf file.
provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the rollback. Default is the running provisioning file. Valid locations are flash: or usbflash0:
on-reboot	(optional) Indicates that the user should not prompted to reload when the rollback operation completes. The user must then use the reload command to boot the system with the newly installed packages.

force	(optional) Specifies that the operation will be forced. Forced means that the rollback will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
verbose	(optional) provides some additional info in the log files

Command Default

No software will be rolled-back by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software rollback** command rolls back the committed software, ie. set of packages, to a previous installation point.

The software rollback functionality relies on the existence of one or more **rollback provisioning files** in flash:, along with all of the .pkg files listed in the rollback provisioning file(s).

The rollback provisioning files are visible in flash: as packages.conf.00-, packages.conf.01-, etc.

- packages.conf.00- is a snapshot of the packages.conf file as it looked prior to the last installation operation.

- packages.conf.01- is a snapshot of the packages.conf file as it looked two installations ago. (This pattern continues for all provisioning files.)

When the **software rollback** command is used, packages.conf.00- becomes packages.conf, packages.conf.01- becomes packages.conf.00-, etc.

Note If the **software clean** command is used, future attempts to do a software rollback will fail if the rollback provisioning file and/or the packages listed in it have been cleaned.

Examples

This example uses the 'software rollback' command to revert to the previously installed package set (packages.conf.00 -).

```
infra-p2-3#software rollback
Preparing rollback operation ...
[2]: Starting rollback operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished rolling back software changes. New software will load on reboot.

[2]: Do you want to proceed with reload? [yes/no]: n

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.

test cable-diagnostics

To test the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics**command in privileged EXEC mode.

test cable-diagnostics tdr interface *type number*

Syntax Description

tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
interface *type*	Specifies the interface type; see the “Usage Guidelines” section for valid values.
number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Cisco 7600 series routers.
12.2(17b)SXA	This command was changed to provide support for the 4-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6704-10GE).
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

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

Usage Guidelines

Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- The TDR test is supported on Cisco 7600 series routers running Release 12.2(17a)SX and later releases on specific mdoules. See the Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.
- The valid values for **interface** *type*are **fastethernet** and **gigabitethernet**.
- Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.
- Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.
- The interface must be up before running the TDR test. If the port is down, the **test cable-diagnostics tdr** command is rejected and the following message is displayed:

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

- If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.
- For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.
- For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the **no mdix auto**command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.
- If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.
- If you change the port speed from 1000 to 10/100, enter the **no mdix auto**command before running the TDR test. Note that entering the **speed 1000** command enables auto-MDIX regardless of whether the **no mdix auto**command has been run.

Examples

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clears all interfaces that support TDR.
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source to the specified destination, use the **traceroute mac**command in privileged EXEC mode.

traceroute mac *source-mac-address* {*destination-mac-address* | **interface** *type interface-number destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

traceroute mac interface *type interface-number source-mac-address* {*destination-mac-address* | **interface** *type interface-number destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

source-mac-address	Media Access Control (MAC) address of the source switch in hexadecimal format.
destination-mac-address	MAC address of the destination switch in hexadecimal format.
interface *type*	Specifies the interface where the MAC address resides; valid values are **FastEthernet**, **GigabitEthernet**, and **Port-channel**.
interface-number	Module and port number or the port-channel number; valid values for the port channel are from 1 to 282.
vlan *vlan-id*	(Optional) Specifies the virtual local area network (VLAN) on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid values are from 1 to 4094.
detail	(Optional) Displays detailed information about the Layer 2 trace.

ip	Specifies the IP address where the MAC address resides.
source-ip-address	IP address of the source switch as a 32-bit quantity in dotted-decimal format.
source-hostname	IP hostname of the source switch.
destination-ip-address	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
destination-hostname	IP hostname of the destination switch.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on the Cisco 7600 series router that is configured with a Supervisor Engine 2.

Do not use leading zeros when entering a VLAN ID.

For Layer 2 traceroute to functional properly, you must enable CDP on all of the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten .

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and a message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and a message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and a message appears.

When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute utility terminates at that hop and displays an error message.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display detailed information about the Layer 2 path:

```
Router# traceroute mac 0001.0000.0204 0001.0000.0304 detail
Source 1001.0000.0204 found on VAYU[WS-C6509] (10.1.1.10)
1 VAYU / WS-C6509 / 10.1.1.10 :
Gi6/1 [full, 1000M] => Po100 [auto, auto]
2 PANI / WS-C6509 / 10.1.1.12 :
Po100 [auto, auto] => Po110 [auto, auto]
3 BUMI / WS-C6509 / 10.1.1.13 :
Po110 [auto, auto] => Po120 [auto, auto]
4 AGNI / WS-C6509 / 10.1.1.11 :
Po120 [auto, auto] => Gi8/12 [full, 1000M]
Destination 1001.0000.0304 found on AGNI[WS-C6509] (10.1.1.11)
Layer 2 trace completed.
Router#
```

This example shows the output when the switch is not connected to the source switch:

```
Router# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 1000.0201.0501 found on con5[WS-C6509] (10.2.5.5)
con5 / WS-C6509 / 10.2.5.5 :
        Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 10.2.1.1 :
        Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C6509 / 10.2.2.2 :
        Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed.
Router#
```

This example shows the output when the switch cannot find the destination port for the source MAC address:

```
Router# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
Router#
```

This example shows the output when the source and destination devices are in different VLANs:

```
Router# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
Router#
```

This example shows the output when the destination MAC address is a multicast address:

```
Router# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
Router#
```

This example shows the output when the source and destination switches belong to multiple VLANs:

```
Router# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
Router#
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Router# traceroute mac interface fastethernet0/1 0000.0201.0601 interface
fastethernet0/3 0000.0201.0201
Source 1000.0201.0601 found on con6[WS-C6509] (10.2.6.6)
con6 (10.2.6.6) :Fa0/1 =>Fa0/3
con5                (10.2.5.5       )  :    Fa0/3 =>Gi0/1
con1                (10.2.1.1       )  :    Gi0/1 =>Gi0/2
con2                (10.2.2.2       )  :    Gi0/2 =>Fa0/1
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed
Router#
```

This example shows how to display detailed traceroute information:

```
Router# traceroute mac ip 10.2.66.66 10.2.22.22 detail
Translating IP to mac.....
10.2.66.66 =>0000.0201.0601
10.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C6509] (10.2.6.6)
con6 / WS-C6509 / 10.2.6.6 :
        Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C6509 / 10.2.5.5 :
        Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 10.2.1.1 :
        Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C6509 / 10.2.2.2 :
        Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed.
Router#
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Router# traceroute mac ip con6 con2
Translating IP to mac .....
10.2.66.66 =>0000.0201.0601
10.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6
con6 (10.2.6.6) :Fa0/1 =>Fa0/3
con5                (10.2.5.5       )  :    Fa0/3 =>Gi0/1
con1                (10.2.1.1       )  :    Gi0/1 =>Gi0/2
con2                (10.2.2.2       )  :    Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
Router#
```

This example shows the output when ARP cannot associate the source IP address with the corresponding MAC address:

```
Router# traceroute mac ip 10.2.66.66 10.2.77.77
Arp failed for destination 10.2.77.77.
Layer2 trace aborted.
Router#
```

upgrade rom-monitor

To set the execution preference on a read-only memory monitor (ROMMON), use the **upgrade rom-monitor** command in privileged EXEC or diagnostic mode.

upgrade rom-monitor slot *num* {**sp** | **rp**} **file** *filename*

upgrade rom-monitor slot *num* {**sp** | **rp**} {**invalidate** | **preference**} {**region1** | **region2**}

Cisco ASR 1000 Series Aggregation Services Routers

upgrade rom-monitor filename *URL slot*

Syntax Description

slot *num*	Specifies the slot number of the ROMMON to be upgraded.
sp	Upgrades the ROMMON of the Switch Processor.
rp	Upgrades the ROMMON of the Route Processor.
file *filename*	Specifies the name of the S-record (SREC) file; see the “Usage Guidelines” section for valid values.
invalidate	Invalidates the ROMMON of the selected region.
preference	Sets the execution preference on a ROMMON of the selected region.
region1	Selects the ROMMON in region 1.
region2	Selects the ROMMON in region 2.
filename	Specifies the ROMMON package filename.
URL	The URL to a ROMMON file. The URL always begins with a file system, such as **bootflash:**, **harddisk:**, **obfl:**, **stby-harddisk:**, or **usb**[**0**-**1**], then specifies the path to the file.

slot	The slot that contains the hardware that will receive the ROMMON upgrade. Options are: • *number* --the number of the Session Initiation Protocol (SIP) slot that requires the ROMMON upgrade • **all** --All hardware on the router • **F0** --Embedded-Service-Processor slot 0 • **F1** --Embedded-Service-Processor slot 1 • **FP** --All installed Embedded-Service-Processors • **R0** --Route-Processor slot 0 • **R1** --Route-Processor slot 1 • **RP** --Route-Processor

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(14)SX	This command was introduced on 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.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.

Usage Guidelines

Caution If you enter the **upgrade rom-monitor** command from a Telnet session instead of a console connection, service may be interrupted.

The **slot** *num*keyword and argument combination is required for this command to function properly.

The **sp** or **rp**keyword is required if you installed a supervisor engine in the specified slot.

Valid values for **file** *filename* are the following:

- **bootflash:**
- **disk0:**
- **disk1:**
- **flash:**
- **ftp:**
- **rcp:**
- **sup-bootflash:**
- **sup-slot0:**
- **tftp:**

On Cisco ASR 1000 Series Routers, this command can be used to upgrade ROMMON in privileged EXEC and diagnostic mode. The hardware receiving the ROMMON upgrade must be reloaded to complete the upgrade.

From Cisco IOS Release 12.4(24)T, you can use the **upgrade rom-monitor** command on Cisco 3200 series routers to upgrade ROMMON and the system bootstrap, if a newer version of ROMMON is available on the system.

Examples

This example shows how to upgrade the new ROMMON image to the flash device on a Supervisor Engine 2:

```
Router# upgrade rom-monitor
 slot 1 sp file tftp://dirt/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
   Erasing flash
   Programming flash
   Verifying new image
   ROMMON image upgrade complete
   The card must be reset for this to take effect
Router#
```

In the following example, a ROMMON upgrade is performed to upgrade to Cisco IOS Release 12.2(33r)XN1 on a Cisco ASR 1000 Series Router using an ROMMON image stored on the bootflash: file system. All hardware is upgraded on the Cisco ASR 1000 Series Router in this example, and the router is then reloaded to complete the procedure.

```
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# copy tftp bootflash:
Address or name of remote host []? 127.23.16.81

Source filename []? auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg
Destination filename [asr1000-rommon.122-33r.XN1.pkg]?
Accessing tftp://127.23.16.81/auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg...
```

```
Loading auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg from 127.23.16.81 (via
GigabitEthernet0): !!!
[OK - 553164 bytes]
553164 bytes copied in 1.048 secs (527828 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Dec 2 2004 12:02:09 +00:00  lost+found
14401  drwx        4096   Dec 2 2004 12:05:05 +00:00  .ssh
86401  drwx        4096   Dec 2 2004 12:05:07 +00:00  .rollback_timer
   12  -rw-    33554432  Nov 20 2007 19:53:47 +00:00  nvram_00100
   13  -rw-     6401536  Dec 23 2004 19:45:11 +00:00  mcp-fpd-pkg.122-test.pkg
28801  drwx        4096   Nov 1 2007 17:00:36 +00:00  .installer   15  -rw-
553164  Nov 28 2007 15:33:49 +00:00  asr1000-rommon.122-33r.XN1.pkg
   16  -rw-    51716300  Nov 14 2007 16:39:59 +00:00  asr1000rp1-
espbase.v122_33_xn_asr_rls0_throttle.pkg
   17  -rw-    21850316  Nov 14 2007 16:41:23 +00:00  asr1000rp1-rpaccess-
k9.v122_33_xn_asr_rls0_throttle.pkg
   18  -rw-    21221580  Nov 14 2007 16:42:21 +00:00  asr1000rp1-
rpbase.v122_33_xn_asr_rls0_throttle.pkg
   19  -rw-    27576524  Nov 14 2007 16:43:50 +00:00  asr1000rp1-
rpcontrol.v122_33_xn_asr_rls0_throttle.pkg
   20  -rw-    48478412  Nov 14 2007 16:45:50 +00:00  asr1000rp1-rpios-
advipservicesk9.v122_33_xn_asr_rls0_throttle.pkg
   21  -rw-    36942028  Nov 14 2007 16:47:17 +00:00  asr1000rp1-
sipbase.v122_33_xn_asr_rls0_throttle.pkg
   22  -rw-    14749900  Nov 14 2007 16:48:17 +00:00  asr1000rp1-
sipspa.v122_33_xn_asr_rls0_throttle.pkg
   23  -rw-        6049  Nov 14 2007 16:49:29 +00:00  packages.conf
   14  -rw-   213225676  Nov 20 2007 19:53:13 +00:00  asr1000rp1-
advipservicesk9.v122_33_xn_asr_rls0_throttle.bin
928833536 bytes total (451940352 bytes free)
Router# upgrade rom-monitor filename bootflash:/asr1000-rommon.122-33r.XN1.pkg all
Upgrade rom-monitor on Route-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Upgrade rom-monitor on Embedded-Service-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 1
Target copying rom-monitor image file
```

```
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Router# reload
<reload bootup output removed for brevity>
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
```

Related Commands

Command	Description
show rom-monitor	Displays the ROMMON status.

verify

To verify the checksum of a file on a flash memory file system or compute a Message Digest 5 (MD5) signature for a file, use the **verify** command in privileged EXEC mode.

verify [**/md5** [*md5-value*]] *filesystem* **:** [*file-url*]

Cisco 7600 Series Router

verify {**/md5** *flash-filesystem* [*expected-md5-signature*] | **/ios** *flash-filesystem* | *flash-filesystem*}

Syntax Description

/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
md5-value	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system calculates the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
filesystem **:**	File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are **flash:** and **bootflash:**.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.
Cisco 7600 Series Router	

/md5 *flash-filesystem*	Computes an MD5 signature for a file; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
expected-md5-signature	(Optional) MD5 signature.
/ios *flash-filesystem*	Verifies the compressed Cisco IOS image checksum; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
flash-filesystem	Device where the Flash memory resides; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.

Command Default

The current working device is the default device (file system).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(4)T	The **/md5** keyword was added.
12.2(18)S	The **verify** command was enhanced to verify the hash that is contained in the image, and the output was enhanced to show the hash value in addition to the entire hash image (CCO hash).
12.0(26)S	The **verify** command enhancements were integrated into Cisco IOS Release 12.0(26)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.3(4)T	The **verify** command enhancements were integrated into Cisco IOS Release 12.3(4)T.
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 replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into flash memory; it is not displayed when the image file is copied from one disk to another.

Supported Platforms Other than the Cisco 7600 Series Router

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To display the contents of flash memory, use the **show flash** command. The flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, issue the **verify** command using the **/md5** keyword. For example, issuing the **verify flash:c7200-is-mz.122-2.T.bin /md5**command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify flash:c7200-is-mz.122-2.T.bin /md5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Cisco 7600 Series Router

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or onto a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature that is posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures manually by entering the **verify /md5** *filename* command.

Check the displayed signature against the MD5 signature that is posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the **verify /md5** *flash-filesystem:filenam expected-md5-signature* command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f
.
.
.
Done
!
 %Error verifying disk0:c6msfc2-jsv-mz
 Computed signature  = 0f369ed9e98756f179d4f29d6e7755d3
 Submitted signature = 0f
```

To display the contents of the flash memory, enter the **show flash** command. The listing of the flash contents does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

Supported Platforms Other than Cisco 7600 Series Router

The following example shows how to use the **verify** command to check the integrity of the file c7200-js-mz on the flash memory card inserted in slot 0:

```
Router# dir slot0:

Directory of slot0:/
  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time
20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz

Verified slot0:c7200-js-mz
```

In the following example, the **/md5** keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:

Verify filename []? c7200-js-mz

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

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?
  WORD  Expected md5 signature
  <cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
.
Done
!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

The following example shows how the output of the **verify** command was enhanced to show the hash value in addition to the entire hash image (CCO hash):

```
Router# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz
.
.
.
Done
!
Embedded Hash           MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash               MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash                MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

Cisco 7600 Series Router

This example shows how to use the **verify** command:

```
Router# verify cat6k_r47_1.cbi
.
.
.
File cat6k_r47_1.cbi verified OK.
```

This example shows how to check the MD5 signature manually:

```
Router# verify /md5 c6msfc2-jsv-mz
.
.
.
Done
!
 verify /md5 (disk0:c6msfc2-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

This example shows how to allow the system to compare the MD5 signatures:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
.
Done
!
 verified /md5 (disk0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#
```

This example shows how to verify the compressed checksum of the Cisco IOS image:

```
Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k222-jsv-mz
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
copy /noverify	Disables the automatic image verification for the current copy operation.

Command	Description
dir	Displays a list of files on a file system.
file verify auto	Verifies the compressed Cisco IOS image checksum.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.
show flash	Displays the layout and contents of flash memory.

vtp

To configure the global VLAN Trunking Protocol (VTP) state, use the **vtp** command in global configuration mode. To return to the default value, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} {**vlan** | **mst** | **unknown**} | **password** *password-value* [**hidden** | **secret**] | **pruning** | **version** {**1** | **2** | **3**}}

no vtp

Syntax Description

domain *domain-name*	Sets the VTP administrative domain name.
file *filename*	Sets the ASCII name of the IFS file system file where the VTP configuration is stored.
interface *interface-name*	Sets the name of the preferred source for the VTP-updater ID for this device.
only	(Optional) Specifies to use only this interface's IP address as the VTP-IP updater address.
mode client	Sets the type of VTP-device mode to client mode.
mode off	Sets the type of VTP-device mode to off mode.
mode server	Sets the type of VTP-device mode to server mode.
mode transparent	Sets the type of VTP-device mode to transparent mode.
vlan	Specifies VTP version 3 VLAN instances.
mst	Specifies VTP version 3 MST instances.
unknown	Specifies VTP version 3 for all other instances.
password *password-value*	Specifies the administrative-domain password.

hidden	(Optional) Specifies that the VTP version 3 secret key generated from the password be saved in the const_nvram:vlan.dat file.
secret	(Optional) Allows you to directly configure the VTP version 3 password secret key.
pruning	Enables the administrative domain to permit pruning.
version {**1** | **2** | **3**}	Specifies the administrative-domain VTP version number.

Command Default

The defaults are as follows:

- **vtp domain** and **vtp interface** co mmands have no default settings.
- *filename* is const-nvram:vlan.dat .
- VTP mode is **mode server** for VLANs and **transparent** for all other features.
- No password is configured.
- Pruning is disabled.
- Administrative-domain VTP version number 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	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 Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The **mode off**keyword combination was added.
12.2(33)SXI	Support for VTP version 3 was added.

Usage Guidelines

Note The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP.

When you define the domain-name value , the dom ain name is case sensitive and can be from 1 to 32 characters.

The *filename* and *interface-name*values are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

Caution If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.

A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on a Cisco 7600 series router affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The **vtp password**, **vtp pruning**, and **vtp version** commands are not placed in startup memory but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure the **pruning** keyword in VTP-server mode; the **version** keyword is configurable in VTP-server mode or VTP transparent mode.

The password-value argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All Cisco 7600 series routers in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on Cisco 7600 series routers in the same VTP domain.

If all Cisco 7600 series routers in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one Cisco 7600 series router; the version number is then propagated to the other version 2-capable Cisco 7600 series routers in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified.

If you enter the **vtp mode off** command, it sets the device to off. If you enter the **no vtp mode off** command, it resets the device to the VTP server mode.

In VTP version 3, the VTP mode has to be specified on a per-feature basis. Use the **vlan** and **mst** keywords to configure the VTP mode on VLAN and MST instances. To configure the VTP mode for any other feature, use the **unknown** keyword. When you convert from either VTP version 1 or 2 to version 3, the current mode configuration will be preserved.

With VTP version 3, a new method is available for hiding the VTP password from the configuration file. When you use the **hidden** keyword, the secret key that is generated from the password string is saved in the const_nvram:vlan.dat file. If you use the **secret** keyword, you can directly configure the password secret key. By using the **secret** keyword, you can distribute the password in the secret key format rather than in the cleartext format.

Examples

This example shows how to set the device's management domain:

```
Router(config)#
vtp domain DomainName1
```

This example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)#
vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
```

This example shows how to set the VTP mode to client:

```
Router(config)#
vtp mode client
Setting device to VTP CLIENT mode.
```

This example shows how to disable VTP mode globally:

```
Router(config)# vtp mode off
Setting device to VTP OFF mode.
```

This example shows how to reset the device to the VTP server mode:

```
Router(config)# no vtp mode off
Setting device to VTP OFF mode.
```

Related Commands

Command	Description
show vtp	Displays the VTP statistics and domain information.
vtp (interface configuration)	Enables VTP on a per-port basis.