

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	Parameter	Description
	tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
	interface <i>type</i>	Specifies the interface type; see the “Usage Guidelines” section for valid values.
	<i>number</i>	Module and port number.

Defaults 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.
	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 modules. 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.

test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash** command in EXEC mode.

test flash

Syntax Description This command has no arguments or keywords.

Defaults This command has no default values.

Command Modes EXEC

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.

Examples In the following example, the Flash memory is tested:

```
test flash
```

Related Commands	Command	Description
	test interfaces	Tests the system interfaces on the modular router.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** command in EXEC mode.

test interfaces

Syntax Description This command has no arguments or keywords.

Defaults This command has no default values.

Command Modes EXEC

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

Usage Guidelines The **test interfaces** EXEC command is intended for the factory checkout of network interfaces. It is not intended for diagnosing problems with an operational router. The **test interfaces** output does not report correct results if the router is attached to a “live” network. For each network interface that has an IP address that can be tested in loopback (MCI and ciscoBus Ethernet and all serial interfaces), the **test interfaces** command sends a series of ICMP echoes. Error counters are examined to determine the operational status of the interface.

Examples In the following example, the system interfaces are tested:

```
test interfaces
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test memory	Performs a test of Multibus memory (including nonvolatile memory) on the modular router.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory** command in privileged EXEC mode. The memory test overwrites memory.

test memory

Syntax Description This command has no arguments or keywords.

Command Default This command overwrites memory.

Command Modes Privileged EXEC

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

Usage Guidelines The memory test overwrites memory. If you use the **test memory** command, you will need to rewrite nonvolatile memory. For example, if you test Multibus memory, which is the memory used by the CSC-R 4-Mbps Token Ring interfaces, you will need to reload the system before the network interfaces will operate properly. The **test memory** command is intended primarily for use by Cisco personnel.

Examples In the following example, the memory is tested:

```
test memory
```

Related Commands	Command	Description
	test flash	Tests Flash memory on MCI and envm Flash EPROM interfaces.
	test interfaces	Tests the system interfaces on the modular router.

test memory destroy

To destroy a memory chunk or dangling reference, use the **test memory destroy** command in privileged EXEC mode.

```
test memory destroy [chunk | mgd-chunk | force-chunk | dangling-reference] chunk-id
```

Syntax Description

chunk	(Optional) Ordinary chunk of memory.
mgd-chunk	(Optional) Managed chunk of memory.
force-chunk	(Optional) Chunk of memory that is destroyed forcefully.
dangling-reference	(Optional) Dangling reference of memory.
<i>chunk-id</i>	Address of the chunk to be destroyed.

Command Default

This command destroys memory chunks or dangling references on a router.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

The **force-chunk** keyword destroys a chunk of ordinary (not managed) memory, even if the memory has elements or siblings that are not free.



Caution

Use the **force-chunk** keyword carefully. A crash or corruption will occur if someone refers to the destroyed chunk or its elements.

Examples

In the following example, a chunk of ordinary memory is destroyed:

```
test memory destroy force-chunk
```

Related Commands

Command	Description
test memory chunk	Allocates or frees chunk elements from a chunk.
test memory create chunk	Creates a memory chunk.

test platform police get

To get the IPv6 internal police rate, use the **test platform police get** command in privileged EXEC mode.

test platform police get

Syntax Description This command has no arguments or keywords.

Defaults 0 (No rate has been applied.)

Command Modes Privileged EXEC (Router#)

Command History	Release	Modification
	12.2(33)SRD1	The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines Use this command under the **exec** command of the line card console. It is not visible from the route processor (RP) console.

Examples The following example shows show to get the IPv6 internal police rate:

```
Router-dfc3# enable
Router-dfc3# test platform police ipv6 get
IPv6 with HBH header is policed at 100000 kbps
```

Related Commands	Command	Description
	test platform police set	Sets the IPv6 internal police rate.

test platform police set

To set the IPv6 internal police rate, use the **test platform police set** command in privileged EXEC mode.

test platform police set *rate*



Note There is not a **no** version of this command. If you have set a rate limit and wish to cancel it, you will need to use this command to set the rate to 0.

Syntax Description

<i>rate</i>	The range is 0 to 100000 kbps. <ul style="list-style-type: none"> For the SIP-400, you can configure a rate up to, and including 25600 packets per second (PPS). For the ES+ line cards, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG line cards, you can configure a rates of: <ul style="list-style-type: none"> 16 Kbps—2 Mbps; granularity of 16 kbps 2 Mbps—100 Mbps; granularity of 64 kbps
-------------	---

Defaults

For ES40 line cards, the default police rate is 12.8Mbps.

For the SIP-400, the default police rate is 21.36kpps.

Command Modes

Privileged EXEC (Router#)

Command History

Release	Modification
12.2(33)SRD1	The command was introduced on the Cisco 7600 series routers for the ES+ line cards, the SIP-400, and the 7600-ES+ITU-2TG and 7600-ES+ITU-4TG.

Usage Guidelines

Use this command under EXEC command of the line card console. It is not visible from the route processor (RP) console.

For both the ES+ line cards and the SIP-400, setting the police rate to 0 turns off the policing.

For both the ES+ line cards and the SIP-400, when the policer is set from the the line card console, the setting remains effective even if the line card is moved to another chassis running the Cisco IOS Release 12.2(33)SRD1 (or later) image.

For the SIP-400, IPv6 HBH packets will continue to go through the QoS policing configured on the line card. For ES+ line cards, IPv6 HBH packets will bypass any QoS configured on the line card.

Examples

The following examples shows how to set the IPv6 with HBH header to be policed at 100000 kbps:

```
Router-dfc3# enable
Router-dfc3# test platform police ipv6 set 100000
```

Related Commands

Command	Description
test platform police get	Gets the IPv6 internal police rate.

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** commands in global configuration mode. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename.

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

```
tftp-server rom alias filename1 [access-list-number]
```

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

Cisco 1600 Series and Cisco 3600 Series Routers

```
tftp-server flash [device:][partition-number:]filename
```

```
no tftp-server flash [device:][partition-number:]filename
```

Cisco 7000 Family Routers

```
tftp-server flash device:filename
```

```
no tftp-server flash device:filename
```

Syntax Description

flash	Specifies TFTP service of a file in Flash memory.
rom	Specifies TFTP service of a file in ROM.
<i>filename1</i>	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
<i>filename2</i>	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.
<i>access-list-number</i>	(Optional) Basic IP access list number. Valid values are from 0 to 99.
<i>partition-number:</i>	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used. For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.

<i>device:</i>	<p>(Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows:</p> <ul style="list-style-type: none"> • flash—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers. • bootflash—Internal Flash memory in the Cisco 7000 family routers. • slot0—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. • slot1—Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family. • slavebootflash—Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA. • slaveslot0—First PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA. • slaveslot1—Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
<i>filename</i>	Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

On the Cisco 7000 family routers, the system sends a copy of the file contained on one of the Flash memory devices to any client that issues a TFTP Read Request with its filename.

Examples

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

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

In the following example, the system uses TFTP to send a copy of the ROM image *gs3-k.101* in response to a TFTP Read Request for the *gs3-k.101* file:

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

In the following example, the system uses TFTP to send a copy of the *version-11.0* file in response to a TFTP Read Request for that file. The file is located on the Flash memory card inserted in slot 0.

```
tftp-server flash slot0:version-11.0
```

The following example enables a Cisco 3600 series router to operate as a TFTP server. The source file *c3640-i-mz* is in the second partition of internal Flash memory.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c3640-i-mz
```

In the following example, the source file is in the second partition of the Flash memory PC card in slot 0 on a Cisco 3600 series:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# tftp-server flash slot0:2:dirt/gate/c3640-j-mz
```

The following example enables a Cisco 1600 series router to operate as a TFTP server. The source file *c1600-i-mz* is in the second partition of Flash memory:

```
router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# tftp-server flash flash:2:dirt/gate/c1600-i-mz
```

Related Commands

Command	Description
access-list	Creates an extended access list.

tftp-server system

The **tftp-server system** command has been replaced by the **tftp-server** command. See the description of the [tftp-server](#) command in this chapter for more information.

time-period

To set the time increment for automatically saving an archive file of the current running configuration in the Cisco IOS configuration archive, use the **time-period** command in archive configuration mode. To disable this function, use the **no** form of this command.

time-period *minutes*

no time-period *minutes*

Syntax Description

<i>minutes</i>	Specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive.
----------------	---

Command Default

By default, no time increment is set.

Command Modes

Archive configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.

Usage Guidelines



Note

Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the Cisco IOS configuration archive.

If this command is configured, an archive file of the current running configuration is automatically saved after the given time specified by the *minutes* argument. Archive files continue to be automatically saved at this given time increment until this function is disabled. Use the **maximum** command to set the maximum number of archive files of the running configuration to be saved.



Note

This command saves the current running configuration to the configuration archive whether or not the running configuration has been modified since the last archive file was saved.

Examples

In the following example, a value of 20 minutes is set as the time increment for which to automatically save an archive file of the current running configuration in the Cisco IOS configuration archive:

```
Router# configure terminal
!
Router(config)# archive
Router(config-archive)# path disk0:myconfig
Router(config-archive)# time-period 20
Router(config-archive)# end
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco IOS configuration archive.
configure confirm	Confirms replacement of the current running configuration with a saved Cisco IOS configuration file.
configure replace	Replaces the current running configuration with a saved Cisco IOS configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco IOS configuration archive.
path	Specifies the location and filename prefix for the files in the Cisco IOS configuration archive.
show archive	Displays information about the files saved in the Cisco IOS configuration archive.

trace (privileged)

To discover the routes that packets will actually take when traveling to their destination, use the **trace** command in privileged EXEC mode.

trace [*protocol*] [*destination*]

Syntax Description	
<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

Defaults The *protocol* argument is based on the Cisco IOS software examination of the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the *protocol* value defaults to **ip**.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, the **trace** command prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X** by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **trace** test, enter the command without a *destination* argument. You will be stepped through a dialog to select the desired parameters.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an “ICMP” message but they reuse the TTL of the incoming packet. Because this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the *ICMP* message can get back. For example, if the host is six hops away, the **trace** command will time out on responses 6 through 11.

Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0  DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 1  BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 2  EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 3  BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 4  SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 5  MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 6  ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 152 describes the significant fields shown in the display.

Table 152 trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
192.180.1.6	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Extended IP Trace Dialog

The following display shows a sample **trace** session involving the extended dialog of the **trace** command:

```
Router# trace

Protocol [ip]:
Target IP address: mit.edu
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to MIT.EDU (18.72.2.1)
```

```

1 ICM-DC-2-V1.ICP.NET (192.108.209.17) 72 msec 72 msec 88 msec
2 ICM-FIX-E-H0-T3.ICP.NET (192.157.65.122) 80 msec 128 msec 80 msec
3 192.203.229.246 540 msec 88 msec 84 msec
4 T3-2.WASHINGTON-DC-CNSS58.T3.ANS.NET (140.222.58.3) 84 msec 116 msec 88 msec
5 T3-3.WASHINGTON-DC-CNSS56.T3.ANS.NET (140.222.56.4) 80 msec 132 msec 88 msec
6 T3-0.NEW-YORK-CNSS32.T3.ANS.NET (140.222.32.1) 92 msec 132 msec 88 msec
7 T3-0.HARTFORD-CNSS48.T3.ANS.NET (140.222.48.1) 88 msec 88 msec 88 msec
8 T3-0.HARTFORD-CNSS49.T3.ANS.NET (140.222.49.1) 96 msec 104 msec 96 msec
9 T3-0.ENSS134.T3.ANS.NET (140.222.134.1) 92 msec 128 msec 92 msec
10 W91-CISCO-EXTERNAL-FDDI.MIT.EDU (192.233.33.1) 92 msec 92 msec 112 msec
11 E40-RTR-FDDI.MIT.EDU (18.168.0.2) 92 msec 120 msec 96 msec
12 MIT.EDU (18.72.2.1) 96 msec 92 msec 96 msec

```

Table 153 describes the fields that are unique to the extended trace sequence, as shown in the display.

Table 153 trace Field Descriptions

Field	Description
Target IP address	You must enter a host name or an IP address. There is no default.
Source address	One of the interface addresses of the router to use as a source address for the probes. The router will normally pick what it feels is the best source address to use.
Numeric display	The default is to have both a symbolic and numeric display; however, you can suppress the symbolic display.
Timeout in seconds	The number of seconds to wait for a response to a probe packet. The default is 3 seconds.
Probe count	The number of probes to be sent at each TTL level. The default count is 3.
Minimum Time to Live [1]	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
Maximum Time to Live [30]	The largest TTL value that can be used. The default is 30. The trace command terminates when the destination is reached or when this value is reached.
Port Number	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
Loose, Strict, Record, Timestamp, Verbose	IP header options. You can specify any combination. The trace command issues prompts for the required fields. Note that the trace command will place the requested options in each probe; however, there is no guarantee that all routers (or end nodes) will process the options.
Loose	Allows you to specify a list of nodes that must be traversed when going to the destination.
Strict	Allows you to specify a list of nodes that must be the only nodes traversed when going to the destination.
Record	Allows you to specify the number of hops to leave room for.
Timestamp	Allows you to specify the number of time stamps to leave room for.
Verbose	If you select any option, the verbose mode is automatically selected and the trace command prints the contents of the option field in any incoming packets. You can prevent verbose mode by selecting it again, toggling its current setting.

Table 154 describes the characters that can appear in **trace** command output.

Table 154 *ip trace Text Characters*

Char	Description
<i>nn msec</i>	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

Related Commands

Command	Description
trace (user)	Discovers the CLNS routes that packets will actually take when traveling to their destination.

trace (user)

To discover the IP routes that packets will actually take when traveling to their destination, use the **trace** command in EXEC mode.

trace [*protocol*] [*destination*]

Syntax Description	
<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

Defaults The *protocol* argument is based on the Cisco IOS software examination of the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the *protocol* defaults to **ip**.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The **trace** command works by taking advantage of the error messages generated by routers when a datagram exceeds its time-to-live (TTL) value.

The **trace** command starts by sending probe datagrams with a TTL value of one. This causes the first router to discard the probe datagram and send back an error message. The **trace** command sends several probes at each TTL level and displays the round-trip time for each.

The **trace** command sends out one probe at a time. Each outgoing packet may result in one or two error messages. A “time exceeded” error message indicates that an intermediate router has seen and discarded the probe. A “destination unreachable” error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet. If the timer goes off before a response comes in, **trace** prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X** by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

Common Trace Problems

Due to bugs in the IP implementation of various hosts and routers, the IP **trace** command may behave in unexpected ways.

Not all destinations will respond correctly to a probe message by sending back an “ICMP port unreachable” message. A long sequence of TTL levels with only asterisks, terminating only when the maximum TTL has been reached, may indicate this problem.

There is a known problem with the way some hosts handle an “ICMP TTL exceeded” message. Some hosts generate an *ICMP* message but they reuse the TTL of the incoming packet. Since this is zero, the ICMP packets do not make it back. When you trace the path to such a host, you may see a set of TTL values with asterisks (*). Eventually the TTL gets high enough that the “ICMP” message can get back. For example, if the host is six hops away, **trace** will time out on responses 6 through 11.

Trace IP Routes

The following display shows sample IP **trace** output when a destination host name has been specified:

```
Router# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 1 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 2 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 3 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 4 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 5 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 6 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
```

Table 155 describes the significant fields shown in the display.

Table 155 trace Field Descriptions

Field	Description
1	Indicates the sequence number of the router in the path to the host.
DEBRIS.CISCO.COM	Host name of this router.
192.180.1.61	Internet address of this router.
1000 msec 8 msec 4 msec	Round-trip time for each of the three probes that are sent.

Table 156 describes the characters that can appear in **trace** output.

Table 156 ip trace Text Characters

Char	Description
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
*	The probe timed out.
?	Unknown packet type.
A	Administratively unreachable. Usually, this output indicates that an access list is blocking traffic.
H	Host unreachable.
N	Network unreachable.

Table 156 *ip trace Text Characters (continued)*

Char	Description
P	Protocol unreachable.
Q	Source quench.
U	Port unreachable.

Related Commands

Command	Description
trace (privileged)	Probes the routes that packets follow when traveling to their destination from the router.

traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

```
traceroute [vrf vrf-name | topology topology-name] [protocol] destination
```

Syntax Description		
vrf <i>vrf-name</i>	(Optional) Specifies the name of a Virtual Private Network (VPN) routing and forwarding (VRF) instance table in which to find the destination address. The only keyword that you can select for the <i>protocol</i> argument when you use the vrf <i>vrf-name</i> keyword-argument pair is the ip keyword.	
topology <i>topology-name</i>	(Optional) Specifies the name of the topology instance. The <i>topology-name</i> argument is case-sensitive; “VOICE” and “voice” specify different topologies.	
<i>protocol</i>	(Optional) Protocol keyword, either appletalk , clns , ip , ipv6 , ipx , oldvines , or vines . When not specified, the <i>protocol</i> argument is based on an examination by the software of the format of the <i>destination</i> argument. The default protocol is IP.	
<i>destination</i>	(Optional in privileged EXEC mode; required in user EXEC mode) The destination address or hostname for which you want to trace the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.	

Command Default When not specified, the *protocol* argument is determined by the software examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(5)T	The vrf <i>vrf-name</i> keyword and argument were added.
	12.2(2)T	Support for IPv6 was added.
	12.0(21)ST	Support for IPv6 was added.
	12.0(22)S	Support for IPv6 was added.
	12.2(11)T	The traceroute command test characters for IPv6 were updated. A new error message was added.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.3(5)	A line was added to the interactive tracert vrf command, so that you can resolve the autonomous system number through the use of the global table or a VRF table, or you can choose not to resolve the autonomous system.
12.0(26)S1	Changes to the command were integrated into Cisco IOS Release 12.0(26)S1.
12.2(20)S	Changes to the command were integrated into Cisco IOS Release 12.2(20)S.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The topology topology-name keyword and argument were added to support Multi-Topology Routing (MTR).
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **tracert** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **tracert** command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **tracert** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **tracert** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **tracert** command prints an asterisk (*).

The **tracert** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **tracert** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You are stepped through a dialog to select the desired parameters. Extended **tracert** tests are not supported in user EXEC mode. The user-level **tracert** feature provides a basic trace facility for users who do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a hostname, it returns a “%No valid source address for destination” message.

If the **vrf vrf-name** keyword and argument are used, the **topology** option is not displayed because only the default VRF is supported. The **topology topology-name** keyword and argument and the DiffServ Code Point (DSCP) option in the extended **tracert** system dialog are displayed only if a topology is configured on the router.

Examples

After you enter the **traceroute** command in privileged EXEC mode, the system prompts you for a protocol. The default protocol is IP.

If you enter a hostname or address on the same line as the **traceroute** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **traceroute** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# traceroute

Protocol [ip]:
Target IP address:
Source address:
DSCP Value [0]: ! Only displayed if a topology is configured on the router.
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]:
```

Related Commands

Command	Description
ping (MTR)	Pings a destination within a specific topology.

tracroute mac

To display the Layer 2 path taken by the packets from the specified source to the specified destination, use the **tracroute mac** command in privileged EXEC mode.

```
tracroute mac source-mac-address { destination-mac-address | interface type interface-number
destination-mac-address } [vlan vlan-id] [detail]
```

```
tracroute mac interface type interface-number source-mac-address { destination-mac-address |
interface type interface-number destination-mac-address } [vlan vlan-id] [detail]
```

```
tracroute mac ip { source-ip-address | source-hostname } { destination-ip-address |
destination-hostname } [detail]
```

Syntax Description

<i>source-mac-address</i>	Media Access Control (MAC) address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	MAC address of the destination switch in hexadecimal format.
interface <i>type</i>	Specifies the interface where the MAC address resides; valid values are FastEthernet , GigabitEthernet , and Port-channel .
<i>interface-number</i>	Module and port number or the port-channel number; valid values for the port channel are from 1 to 282.
vlan <i>vlan-id</i>	(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.
<i>source-ip-address</i>	IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	IP hostname of the source switch.
<i>destination-ip-address</i>	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>destination-hostname</i>	IP hostname of the destination switch.

Defaults

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 tracertoute to function 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 tracertoute, 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 tracertoute 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 **tracertoute 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 tracertoute 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# tracertoute 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# tracertoute 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# tracert 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# tracert 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# tracert 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# tracert 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# tracert 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# tracert 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# tracertoute 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# tracertoute mac ip 10.2.66.66 10.2.77.77
```

```
Arp failed for destination 10.2.77.77.  
Layer2 trace aborted.  
Router#
```

undelete

To recover a file marked “deleted” on a Class A Flash file system, use the **undelete** command in user EXEC or privileged EXEC mode.

```
undelete index [filesystem:]
```

Syntax Description

<i>index</i>	A number that indexes the file in the dir command output.
<i>filesystem:</i>	(Optional) A file system containing the file to undelete, followed by a colon.

Defaults

The default file system is the one specified by the **cd** command.

Command Modes

user EXEC
privileged EXEC

Command History

Release	Modification
11.0	This command was introduced for Class A Flash File Systems (platforms include the Cisco 7500 series and Cisco 12000 series).
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For Class A Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a “deleted” file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked “deleted” on a Flash memory device, use the **squeeze** EXEC command.

For further information on Flash File System types (classes), see <http://www.cisco.com/warp/public/63/pcmciatrix.html>.

Examples

In the following example, the deleted file at index 1 is recovered:

```
Router# show flash

System flash directory:
File Length Name/status
  1  8972116 c7000-js56i-mz.121-5.T [deleted]
  2  6765916 c7000-ds-mz.CSCds70452
[15738160 bytes used, 1039056 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)

Router# undelete 1 flash:
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.

upgrade automatic abortversion

To cancel the scheduled reloading of the router with a new Cisco IOS software image, use the **upgrade automatic abortversion** command in privileged EXEC mode.

upgrade automatic abortversion

no upgrade automatic abortversion

Syntax Description This command has no arguments or keywords.

Command Default The reload of the router with the Cisco IOS software image is not scheduled. The disk-management utility is disabled.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.4(15)T	This command was introduced.

Usage Guidelines Use the **upgrade automatic abortversion** command to cancel a reload that has already been scheduled with either the **upgrade automatic getversion** command or the **upgrade automatic runversion** command.

Examples The following example shows how to cancel a reload that is scheduled within one hour and 15 minutes. The reload was scheduled by using the **upgrade automatic runversion** command.

```
Router# upgrade automatic runversion in 01:15

Upgrading to "flash:c1841-adventerprisek9-mz.calvin-build-20060714". Wait..

Reload scheduled for 09:51:38 UTC Thu Aug 3 2006 (in 1 hour and 15 minutes) with image -
flash:c1841-adventerprisek9-mz.calvin-build-20060714 by console
Reload reason: Auto upgrade
Device will WARM UPGRADE in 1:15:00
To cancel the upgrade, enter the command "upgrade automatic abortversion"
Aug 3 08:36:38.072: %SYS-5-SCHEDULED_RELOAD: Reload requested for 09:51:38 UTC Thu Aug 3
2006 at 08:36:38 UTC Thu Aug 3 2006 by console. Reload Reason: Auto upgrade.

Router# upgrade automatic abortversion

Auto upgrade of image which was scheduled earlier is aborted!

***
*** --- SHUTDOWN ABORTED ---
***
```

```
Aug  3 08:37:02.292: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at
08:37:02 UTC Thu Aug 3 2006
```

Related Commands

Command	Description
upgrade automatic getversion	Downloads a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server.
upgrade automatic runversion	Reloads the router with a new Cisco IOS software image.

upgrade automatic getversion

To download a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server, use the **upgrade automatic getversion** command in privileged EXEC mode.

```
upgrade automatic getversion { cisco username username password password image image |
url } [at hh:mm | now | in hh:mm] [disk-management { auto | confirm | no }]
```

Syntax Description

cisco	Downloads the image from www.cisco.com .
username <i>username</i>	Username for logging in to www.cisco.com .
password <i>password</i>	Password for logging in to www.cisco.com .
image	Specifies the Cisco IOS software image to which the router is to be upgraded.
<i>image</i>	Name of the Cisco IOS software image to which the router is to be upgraded.
<i>url</i>	URL from where the Cisco IOS Auto-Upgrade Manager can download the image that has already been downloaded to a non-Cisco server.
at	(Optional) Schedules a reload at a specified time. Use either of the following arguments with this keyword: <ul style="list-style-type: none"> <i>hh:mm</i>—Hour and minute. The time entered must be in 24-hour format. <i>now</i>—Immediately after the download of the Cisco IOS software image.
in <i>hh:mm</i>	(Optional) Schedules a reload in a specified length of time after downloading the Cisco IOS software image.
disk-management	(Optional) Cisco IOS Auto-Upgrade Manager disk cleanup utility. You must configure one of the following keywords: <ul style="list-style-type: none"> auto—Deletes the files without asking for confirmation. confirm—Asks for confirmation before deleting a file. no—Never deletes any file.

Command Default

The reload of the router with the Cisco IOS software image is not scheduled. The disk-management utility is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **upgrade automatic getversion** command to download the Cisco IOS software image to a router. You can either download the image from the Cisco website (www.cisco.com) or from a non-Cisco server to which the Cisco IOS software image has already been downloaded from the Cisco website.

You can also use this command to schedule a reload. Additionally, this command can use the disk cleanup utility to delete files if there is not enough space to download the new Cisco IOS software image.

Examples

Downloading the Cisco IOS Image from the Cisco Website

The following example shows how to download a Cisco IOS software image from the Cisco website (www.cisco.com). Here, the reloading of the router with the downloaded Cisco IOS software image is not scheduled. Also, the disk-cleanup utility is not enabled.

```
Router# upgrade automatic getversion cisco username myusername password mypassword image
c3825-adventerprisek9-mz.124-2.XA.bin
```

Downloading the Cisco IOS Image from a Non-Cisco TFTP Server

The following example shows how to download the Cisco IOS software image from a non-Cisco TFTP server and reload the router immediately after the download. It also shows how to delete the files automatically if there is not enough disk space.

```
Router# upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin
at now disk-management auto
```

Downloading the Cisco IOS Image from a Non-Cisco TFTP Server Using the Interactive Mode

The following example shows how to use this command in interactive mode to download a Cisco IOS software image from a non-Cisco server. Here, the reloading of the device with the downloaded Cisco IOS software image is not scheduled.

```
Router# upgrade automatic
#####
Welcome to the Cisco IOS Auto Upgrade Manager. To upgrade your device, please answer the
following questions. To accept the default value for a question, simply hit <ENTER>
#####
Would you like to download an image directly from Cisco Server over the Internet? A valid
Cisco login will be required.

Download from Cisco server? [yes]: no
Image location:tftp://10.1.0.1/emailid/c3825-adventerprisek9-mz_pi6_aum_review
Image Found: c3825-adventerprisek9-mz_pi6_aum_review (42245860 bytes)
Memory Available: 851Mb Main Memory (RAM) - 71335936 bytes of flash space
New image will be downloaded to flash:c3825-adventerprisek9-mz_pi6_aum_review

Reload and upgrade the device immediately after image download is complete? [yes]: no
When would you like to reload your device? Use hh:mm format or specify "Manual" to not
schedule a reload time. Use 'upgrade automatic runversion' to reload manually.
Time to reload the box [Manual]?

Proceed with device image upgrade from
[tftp://10.1.0.1/emailid/c3825-adventerprisek9-mz_pi6_aum_review] to
[c3825-adventerprisek9-mz_pi6_aum_review]? [yes]:

Downloading Image from user specified url:

Loading emailid/c3825-adventerprisek9-mz_pi6_aum_review from 172.16.0.0(via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 42245860 bytes]
[download complete]

Verifying the image: .....
Done!
Image Verification: PASS
Use 'upgrade automatic runversion' command to reload manually.
```

Related Commands

Command	Description
upgrade automatic abortversion	Cancels upgrading the router with a new Cisco IOS software image.
upgrade automatic runversion	Reloads the router with a new Cisco IOS software image.

upgrade automatic runversion

To reload the router with a new Cisco IOS software image, use the **upgrade automatic runversion** command in privileged EXEC mode.

upgrade automatic runversion [**at** *hh:mm* | **now** | **in** *hh:mm*]

Syntax Description

at	Schedules a reload at a specified time. Use either of the following arguments with this keyword: <ul style="list-style-type: none"> <i>hh:mm</i>—Hour and minute. The time entered must be in 24-hour format. <i>now</i>—Immediately after the download of the Cisco IOS software image.
in <i>hh:mm</i>	Schedules a reload in a specified length of time after downloading the Cisco IOS software image.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **upgrade automatic runversion** command to schedule a reload after downloading a Cisco IOS software image using the **upgrade automatic getversion** command.



Note

You can also use the **upgrade automatic getversion** command to reload the router with the new Cisco IOS software image. However, if you have already downloaded the Cisco IOS software image using the **upgrade automatic getversion** command, you should use the **upgrade automatic runversion** command to reload the router.

Examples

The following example shows how to schedule a reload after downloading a Cisco IOS software image:

```
Router# show clock

09:01:36.124 UTC Thu Aug 3 2006

Router# upgrade automatic runversion at 10:20

Upgrading to "flash:c1841-adventerprisek9-mz.calvin-build-20060714". Wait..
Reload scheduled for 10:20:00 UTC Thu Aug 3 2006 (in 1 hour and 18 minutes) with image -
flash:c1841-adventerprisek9-mz.calvin-build-20060714 by console
Reload reason: Auto upgrade
Device will WARM UPGRADE at 10:20:00
To cancel the upgrade, enter the command "upgrade automatic abortversion"
Router#
Aug 3 09:01:58.116: %SYS-5-SCHEDULED_RELOAD: Reload requested for 10:20:00 UTC Thu Aug 3
2006 at 09:01:58 UTC Thu Aug 3 2006 by console. Reload Reason: Auto upgrade.
```

Related Commands

Command	Description
upgrade automatic abortversion	Cancels upgrading the router with a new Cisco IOS software image.
upgrade automatic getversion	Downloads a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server.

upgrade filesystem monlib

To upgrade the ATA ROM monitor library (monlib) file without erasing file system data, use the **upgrade filesystem monlib** command in privileged EXEC mode.

```
upgrade filesystem monlib { disk0 | disk1 }
```

Syntax Description

disk0	Selects disk 0 as the file system to be formatted.
disk1	Selects disk 1 as the file system to be formatted.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into the Cisco IOS Release 12.2(25)S.

Usage Guidelines

If you attempt to upgrade the ATA monlib file on a disk that has not been formatted on a router running Cisco IOS software, the upgrade operation will fail.

If the amount of space available on the disk for the monlib image is smaller than the monlib image you are trying to upgrade to, the upgrade operation will fail. The amount of space available for the monlib file can be determined by issuing the **show disk** command with the **all** keyword specified. The “Disk monlib size” field displays the number of bytes available for the ATA monlib file.

Examples

The following example shows how to upgrade the ATA monlib file on disk 0:

```
Router# upgrade filesystem monlib disk0
```

```
Writing Monlib sectors.
```

```
.....
```

```
Monlib write complete
```

Related Commands

Command	Description
format	Formats a Class A or Class C flash file system.
show disk	Displays flash or file system information for a disk.

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 ASR1000 Series Routers

upgrade rom-monitor filename *URL slot*

Syntax Description	
slot <i>num</i>	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 <i>filename</i>	Specifies the name of the 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.
<i>URL</i>	The URL to a ROMmon file. The URL always begins with a filesystem, such as bootflash: , harddisk: , obfl: , stby-harddisk: , or usb[0-1] , then specifies the path to the file.
<i>slot</i>	Specifies the slot that contains the hardware that will receive the ROMmon upgrade. Options include: <ul style="list-style-type: none"> • <i>number</i>—the number of the 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

Defaults This command has no default settings.

Command Modes Privileged EXEC (#)
Diagnostic (diag)

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.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.

Usage Guidelines**Caution**

If you enter the **upgrade rom-monitor** command with no parameters, service may be interrupted.

**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** 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** include the following:

- **bootflash:**
- **disk0:**
- **disk1:**
- **flash:**
- **ftp:**
- **rcp:**
- **sup-bootflash:**
- **sup-slot0:**
- **tftp:**

On the Cisco ASR 1000 Series Routers, this command can be used to upgrade ROMmon in privileged EXEC and diagnostic mode.

On the Cisco ASR 1000 Series Router, the hardware receiving the ROMmon upgrade must be reloaded to complete the upgrade.

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://dir1/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 the 12.2(33r)XN1 ROMmon release on a Cisco ASR 1000 Series Router using a 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	nvrाम_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-adviserservicesk9.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.

upgrade rom-monitor file

To upgrade the ROM monitor (ROMmon) image, use the **upgrade rom-monitor file** command in privileged EXEC mode.

Cisco 7200 VXR Router with NPE-G1

```
upgrade rom-monitor file { bootflash: [file-path] | disk0: [file-path] | disk1: [file-path] | disk2:
[file-path] | flash: [file-path] | ftp: [file-path] | slot0: [file-path] | slot1: [file-path] | tftp:
[file-path]}
```

Cisco 7301 Router

```
upgrade rom-monitor file { flash: [file-path] | ftp: [file-path] | disk0: [file-path] | tftp: [file-path]}
```

Cisco 7304 Router

```
upgrade rom-monitor { rom0 | rom1 | rom2 } file { bootdisk: [file-path] | disk0: [file-path] | flash:
[file-path] | ftp: [file-path] | rcp: [file-path] | tftp: [file-path]}
```

Cisco 10008 Router (PRE3 only)

```
upgrade { rom-monitor | fpga }
```

Syntax Description		
	<i>file-path</i>	Directory path name or filename where the Upgrade ROMmon image is located.
bootflash:		Filename location of Upgrade ROMmon image in boot flash memory.
disk0:		Disk 0 is only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in disk 0 of the router chassis.
disk1:		Disk 1 is only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in disk 1 of the router chassis.
disk2:		Disk 2 is always present on a Cisco 7200 VXR. The filename location of the Upgrade ROMmon image in disk 2 of the router chassis.
flash:		Filename location of Upgrade ROMmon image in Flash memory.
fpga		(Cisco 10008 router only) Upgradable field-programmable gate array (FPGA).
ftp:		Filename location of the Upgrade ROMmon image using File Transfer Protocol (FTP).
rom-monitor		(Cisco 10008 router only) Upgradeable ROM monitor.
slot0:, slot1:		Slot 0 and slot 1 are only present on a Cisco 7200 VXR that has an I/O controller. The filename location of the Upgrade ROMmon image in slot 0 and slot 1 of the router chassis.
tftp:		Filename location of the Upgrade ROMmon image on the TFTP server.
rom0		One-time programmable, always there “golden” ROMmon.
rom1		Upgradable ROM monitor 1.
rom2		Upgradable ROM monitor 2.

bootdisk:	Filename location of Upgrade ROMmon image in the boot disk.
rep:	Filename location of the Upgrade ROMmon image using Remote Copy Protocol (RCP).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(28)S	This command was introduced on the Cisco 7200 VXR router.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S and supported on the Cisco 7304 router.
12.0S	This command was introduced on the PRE2 for the Cisco 10000 series router.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

You can use the **upgrade rom-monitor file** command to download a new ROMmon image instead of having to replace the processor to obtain a new image.



Note

Images are marked as invalid if the first bootup is not completed. Do not reset the router when it is doing an initial bootup.

Cisco 7200 VXR Router

A Cisco 7200 VXR that has an I/O controller card installed has the following additional devices on its chassis: disk 0, disk 1, slot 0, and slot 1.

Cisco 7304 Router

There are three ROMmon images. ROM 0 is a one-time programmable, always-there ROMmon image, referred to as the “golden” ROMmon. ROM 1 and ROM 2 are upgradable ROMmon images. At bootup, the system uses the golden ROMmon by default. If either ROM 1 or ROM 2 are configured, the system still begins bootup with the golden ROMmon, then switches to the configured ROMmon. If a new configured ROMmon image fails to boot up Cisco IOS software, the router marks this ROMmon image as invalid and reverts to the golden image for the next Cisco IOS bootup.

After downloading a new ROMmon image to the writable ROMmon, you must reload Cisco IOS software for the new ROMmon to take effect. The first time a new ROMmon image is loaded, you must allow the system to boot up Cisco IOS before doing any resets or power cycling. If the ROMmon loading process is interrupted, the system interprets this as a bootup failure of the new ROMmon image and reverts the ROMmon back to the golden ROMmon image in ROM 0.

Cisco 10008 Router

The PRE2 does not allow you to upgrade the ROM monitor image. However, the PRE3 does allow this using the **upgrade rom-monitor** command.

Examples

The following example of a Cisco 7200 VXR using an I/O controller loads the Upgrade ROMmon image from a disk 1 filename:

```
Router# upgrade rom-monitor file disk1:C7200_NPEG1_RMFUR.srec.123-4r.T1
```

```
This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.
```

```
Erasing boot flash eeeeeeeeeeeeeeeeeee
Programming boot flash pppppp
Now Reloading via hard watchdog timeout
```

The following example on a Cisco 7301 router loads the Upgrade ROMmon image from a specified TFTP file location:

```
Router# upgrade rom-monitor file tftp://00.0.00.0/biff/C7301_RMFUR.srec
```

```
Loading biff/C7301_RMFUR.srec from 00.0.00.0 (via GigabitEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 392348 bytes]
```

```
This command will reload the router. Continue? [yes/no]:yes
ROMMON image upgrade in progress.
```

```
Erasing boot flash eeeeeeeeeeeeeeeeeee
Programming boot flash ppppp
Now Reloading via hard watchdog timeout
```

```
Unexpected exception, CP
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.
```

```
Running new upgrade for first time
```

```
System Bootstrap, Version 12.2(20031011:151758) [biff]
Copyright (c) 2004 by cisco Systems, Inc.
```

```
ROM:Rebooted by watchdog hard reset
C7301 platform with 1048576 Kbytes of main memory
```

```
Upgrade ROMMON initialized
rommon 1 >
```

The following example configures the system to install a file called “rommonfile” as ROM 1 from the bootdisk:

```
Router# upgrade rom-monitor rom1 file bootdisk:rommonfile
```

```
ROM 1 upgrade in progress
Erasing (this may take a while)...
Programming...
CC
Do you want to verify this image (may take a few minutes)? [yes/no]: y
```

```
Verifying ROM 1
  Reading from ROM 1....Done
  Comparing with the source file...Passed
```

Set this ROMMON image as the default (will take effect on next reload/reset)? **y**

Related Commands

Command	Description
show diag	Displays hardware information for any slot or the chassis.

upgrade rom-monitor preference

To select a ReadOnly or Upgrade ROMmon image to be booted on the next reload of a Cisco 7200 VXR or Cisco 7301 router, use the **upgrade rom-monitor preference** command in privileged EXEC mode.

upgrade rom-monitor preference [readonly | upgrade]

Syntax Description	readonly	Selects the ReadOnly ROMmon image to be booted on the next reload.
	upgrade	Selects the Upgrade second ROMmon image to be booted on the next reload.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(28)S	This command was introduced on the Cisco 7200 VXR router.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T and supported on the Cisco 7200 VXR router and Cisco 7301 router.
	12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) and supported on the Cisco 7200 VXR router and Cisco 7301 router.

Usage Guidelines After running the **upgrade rom-monitor preference** command, you must reload the router for the selected ROMmon image to take effect.

Use the **rommon-pref** command when you are in ROMmon mode.

Examples The following example applicable to both the Cisco 7200 VXR and Cisco 7301 routers selects the ReadOnly ROMmon image to be booted on the next reload of the router:

```
Router# upgrade rom-monitor preference readonly
You are about to mark ReadOnly region of ROMMON for the highest boot preference.
Proceed? [confirm]
Done! Router must be reloaded for this to take effect.
```

Related Commands	Command	Description
	rommon-pref	Selects a ReadOnly or Upgrade ROMmon image to be booted on the next reload when you are in ROMmon mode.

vacant-message

To display an idle terminal message, use the **vacant-message** command in line configuration mode. To remove the default vacant message or any other vacant message that may have been set, use the **no** form of this command.

vacant-message [*d message d*]

no vacant-message

Syntax Description

<i>d</i>	(Optional) Delimiting character that marks the beginning and end of the vacant-message. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), or tilde (~). ^C is reserved for special use and should not be used in the message.
<i>message</i>	(Optional) Vacant terminal message.

Defaults

The format of the default vacant message is as follows:

```
<blank lines>
hostname tty# is now available
<blank lines>
Press RETURN to get started.
```

This message is generated by the system.

Command Modes

Line configuration

Command History

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

Usage Guidelines

This command enables the banner to be displayed on the screen of an idle terminal. The **vacant-message** command without any arguments restores the default message.

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.



Note

For a rotary group, you need to define only the message for the first line in the group.

Examples

The following example turns on the system banner and displays this message:

```
Router(config)# line 0
Router(config-line)# vacant-message %
                Welcome to Cisco Systems, Inc.
                Press Return to get started.
%
```

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.
<i>md5-value</i>	(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.
<i>filesystem:</i>	File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are flash: and bootflash: .
<i>file-url</i>	(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	
<i>/md5 flash-filesystem</i>	Computes an MD5 signature for a file; valid values are bootflash: , disk0: , disk1: , flash: , or sup-bootflash: .
<i>expected-md5-signature</i>	(Optional) MD5 signature.
<i>/ios flash-filesystem</i>	Verifies the compressed Cisco IOS image checksum; valid values are bootflash: , disk0: , disk1: , flash: , or sup-bootflash: .
<i>flash-filesystem</i>	Device where the Flash memory resides; valid values are bootflash: , disk0: , disk1: , flash: , or sup-bootflash: .

Defaults

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.

Release	Modification
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:filename 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.
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 } | password password-value | pruning | version { 1 | 2 } }
```

```
no vtp
```

Syntax Description

domain <i>domain-name</i>	Sets the VTP-administrative domain name.
file <i>filename</i>	Sets the ASCII name of the IFS-file system file where the VTP configuration is stored.
interface <i>interface-name</i>	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.
password <i>password-value</i>	Specifies the administrative-domain password.
pruning	Enables the administrative domain to permit pruning.
version { 1 2 }	Specifies the administrative-domain VTP-version number.

Defaults

The defaults are as follows:

- **vtp domain** and **vtp interface** commands have no default settings.
- *filename* is **const-nvram:vlan.dat**.
- VTP mode is **mode server**.
- 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.

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 domain 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.

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.

warm-reboot

To enable a router to do a warm-reboot, use the **warm-reboot** command in global configuration mode. To disable warm rebooting, use the **no** form of this command.

warm-reboot [**count** *number*] [**uptime** *minutes*]

no warm-reboot **count** *number* **uptime** *minutes*

Syntax Description

count <i>number</i>	(Optional) Maximum number of warm reboots allowed between any intervening cold reboot. Valid values range from 1 to 50. The default value is 5 times.
uptime <i>minutes</i>	(Optional) Minimum number of minutes that must elapse between initial system configuration and an exception before a warm reboot is attempted. If the system crashes before the specified time elapses, a warm reboot is not attempted. Valid values range from 0 to 120. The default value is 5 minutes.

Defaults

Warm rebooting is disabled.

If warm rebooting is enabled, the default value for the **count** *number* option is 5 times, and the default value for the **uptime** *minutes* option is 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **warm-reboot** command to enable the router to reload a Cisco IOS image without ROM monitor mode (ROMMON) intervention, in which the image restores read-write data from a previously saved copy in the RAM and starts execution from that point. Unlike a cold reboot, this process does not involve a flash to RAM copy or self-decompression of the image.



Note

After a warm reboot is enabled, it will not become active until after the next cold reboot because a warm reboot requires a copy of the initialized memory.



Note

If the system crashes before the image completes the warm reboot process, a cold reboot is initiated.

Examples

The following example shows how to enable a warm reboot on the router:

```
Router#(config) warm-reboot count 10 uptime 10
```

Related Commands

Command	Description
show warm-reboot	Displays the statistics for attempted warm reboots.

where

To list the open sessions, use the **where** command in EXEC mode.

where

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The **where** command displays all open sessions associated with the current terminal line. The break (Ctrl-Shift-6, x), **where**, and **resume** commands are available with all supported connection protocols.

Examples The following is sample output from the **where** command:

```
Router# where
Conn Host                Address                Byte    Idle  Conn Name
  1 MATHOM                192.31.7.21           0       0    MATHOM
*  2 CHAFF                131.108.12.19         0       0    CHAFF
```

The asterisk (*) indicates the current terminal session.

[Table 157](#) describes the fields shown in the display.

Table 157 *where* Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval (in minutes) since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands	Command	Description
	show line	Displays information about all lines on the system or the specified line.
	show sessions	Displays information about open LAT, Telnet, or rlogin connections.

width

To set the terminal screen width, use the **width** command in line configuration mode. To return to the default screen width, use the **no width** form of this command.

width *characters*

no width

Syntax Description	<i>characters</i>	Number of character columns displayed on the terminal. The default is 80 characters.
---------------------------	-------------------	--

Defaults	80 character columns
-----------------	----------------------

Command Modes	Line configuration
----------------------	--------------------

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

Usage Guidelines	<p>By default, the route provides a screen display width of 80 characters. You can reset this value for the current session if it does not meet the needs of your terminal.</p> <p>The rlogin protocol uses the value of the <i>characters</i> argument to set up terminal parameters on a remote host.</p>
-------------------------	---

Examples	In the following example the location for line 7 is defined as “console terminal” and the display is set to 132 columns wide:
-----------------	---

```
Router(config)# line 7
Router(config-line)# location console terminal
Router(config-line)# width 132
```

Related Commands	Command	Description
	terminal width	Sets the number of character columns on the terminal screen for the current session.

write core

To test the configuration of a core dump setup, use the **write core** command in privileged EXEC mode.

write core [*hostname* [LINE] | *destination-address* [LINE]]

Syntax Description

<i>hostname</i>	(Optional) Host name of the remote server where the core dump file is to be written.
<i>destination-address</i>	(Optional) IP address of the remote server where the core dump file is to be written.
LINE	(Optional) Assigns the name “LINE” to the core dump file.

Defaults

If the *hostname* or *destination* arguments are not specified, the core dump file is written to the IP address or hostname specified by the **exception dump** command.

If the **LINE** keyword is not specified, the name of the core dump file is assigned as the host name of the remote server followed by the word “-core.”

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

When a router reloads, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the reload. Core dumps are generally useful to your technical support representative. Not all types of router reloads will produce a core dump.

The **write core** command causes the router to generate a core dump without reloading, which may be useful if the router is malfunctioning but has not reloaded. The core dump files will be the size of the respective memory regions. It is important to remember that the entire memory region is dumped, not just the memory that is in use.



Caution

Use the **write core** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. When using this command, the router will not reload until the content of its memory is dumped. This event might take some time, depending on the amount of DRAM present on the router. Also, the resulting binary file, which is very large, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel who have access to source code and detailed memory maps.

Depending on your TFTP server, you might need to create an empty target file to which the router can write the core dump.

Examples

The following example shows how to test the configuration of a core dump setup. In this example, the core dump file is written to the remote server with the host name test.

```
write core test
```

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command for more information.

write terminal

This command is deprecated. Deprecated commands are considered obsolete, and their use is discouraged. Support for this command may be removed.

The **write terminal** command is now enabled only as a command alias for the **show running-config** command.

The **show running-config** command offers additional options not available for the **write terminal** command; see the documentation of the **show running-config** command for details.

Command Modes

Privileged EXEC

Command History

Release	Modification
8.0	This command was introduced in a release prior to 8.0.
11.0	The show running-config command was introduced as a replacement for the write terminal command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

xmodem

To copy a Cisco IOS image to a router using the ROM monitor and the Xmodem or Ymodem protocol, use the **xmodem** command in ROM monitor mode.

```
xmodem [-c] [-y] [-e] [-f] [-r] [-x] [-s data-rate] [filename]
```

Syntax Description

-c	(Optional) CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming.
-y	(Optional) Uses the Ymodem protocol for higher throughput.
-e	(Optional) Erases the first partition in Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-f	(Optional) Erases all of Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-r	(Optional) Downloads the file to DRAM. The default is Flash memory.
-x	(Optional) Do not execute Cisco IOS image on completion of the download.
-s <i>data-rate</i>	(Optional) Sets the console port's data rate during file transfer. Values are 1200 , 2400 , 4800 , 9600 , 19200 , 38400 , and 115200 bps . The default rate is specified in the configuration register. This option is only valid for the Cisco 1600 series.
<i>filename</i>	(Optional) Filename to copy. This argument is ignored when the -r keyword is specified, because only one file can be copied to DRAM. On the Cisco 1600 series routers, files are loaded to the ROM for execution.

Defaults

Xmodem protocol with 8-bit CRC, file downloaded into Flash memory and executed on completion.

Command Modes

ROM monitor

Command History

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

Usage Guidelines

The Cisco 3600 series routers does not support XBOOT functionality. If your Cisco IOS image is erased or damaged, you cannot load a new image over the network.

Use the **xmodem** ROM monitor command to download a new system image to your router from a local personal computer (such as a PC, Mac, or UNIX workstation), or a remote computer over a modem connection, to the router's console port. The computer must have a terminal emulation application that supports these protocols.

Cisco 3600 Series Routers

Your router must have enough DRAM to hold the file being transferred, even if you are copying to Flash memory. The image is copied to the first file in internal Flash memory. Any existing files in Flash memory are erased. There is no support for partitions or copying as a second file.

Cisco 1600 Series Routers

If you include the **-r** option, your router must have enough DRAM to hold the file being transferred. To run from Flash, an image must be positioned as the first file in Flash memory. If you are copying a new image to boot from Flash, erase all existing files first.

**Caution**

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

**Note**

If the file to be downloaded is not a valid router image, the copy operation is automatically terminated.

Examples

The following example uses the **xmodem -c filename** ROM monitor command to copy the file named new-ios-image from a remote or local computer:

```
rommon > xmodem -c new-ios-image

Do not start the sending program yet...
      File size      Checksum  File name
1738244 bytes (0x1a8604)  0xdd25 george-admin/c3600-i-mz

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

Related Commands

Command	Description
copy xmodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol.
copy ymodem:	Copies a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol.

