C commands

C commands

cd

To change the default directory or file system, use the **cd** command in user EXEC or privileged EXEC mode.

cd [*filesystem***:**][*directory*]

Syntax Description

filesystem **:**	(Optional) The URL or alias of the directory or file systems followed by a colon.
directory	(Optional) Name of the directory.

Command Default

The initial default file system is **flash:**. For platforms that do not have a physical device named **flash:**, the keyword **flash:** is aliased to the default Flash device.

For the Supervisor Engine, the initial default file system is **disk0 :**

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX, and support was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support was added for the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The valid values for *filesystem* **:**are as follows:

- For systems that are configured with a Supervisor Engine 2, valid values are **bootflash:**, **const_nvram:**, **disk0:**, **flash:**, **nvram:**, **slot0:**, **sup-slot0:**, and **sup-bootflash:**
- For systems that are configured with a Supervisor Engine 720, valid values are **disk0:** and **disk1:**

For all EXEC commands that have an optional *filesystem*argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem*argument. For example, the **dir**command, which displays a list of files on a file system, contains an optional *filesystem*argument. When you omit this argument, the system lists the files on the file system specified by the **cd** command.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Examples

In the following example, the **cd** command is used to set the default file system to the Flash memory card inserted in slot 0:

```
Router# pwd

bootflash:/
Router# cd slot0:

Router#
pwd

slot0:/
```

Examples

This example sets the default file system to the Flash PC card that is inserted in disk 0:

```
Router# cd disk0:
Router#
pwd
disk0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
mkdir disk0:	Creates a new directory in a Flash file system.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

clear archive log config

To purge the configuration logging database entries, use the **clear archive log config**command in privileged EXEC mode.

clear archive log config [**force**| **persistent**]

Syntax Description

force	(Optional) Eliminates the confirm step before the contents of the archive log are cleared.
persistent	(Optional) Purges the configuration logging persistent-command database entries.

Command Default

If this command is not used, the database entries accumulate in the archive log.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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.

Usage Guidelines

When the **clear archive log config**command is entered, only the entries in the configuration logging database file are deleted. The file itself is not deleted; it will be used in the future to log new entries as they occur.

Examples

The following example clears the database entries that have been saved to the config log without asking you to confirm the action before the entries are cleared:

```
Router# clear archive log config force
```

Related Commands

Command	Description
show archive log config all persistent	Displays the persisted commands in configlet format.

clear catalyst6000 traffic-meter

To clear the traffic meter counters, use the **clear catalyst6000 traffic-meter**command in privileged EXEC mode.

clear catalyst6000 traffic-meter

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the 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.

Examples

This example shows how to clear the traffic meter counters:

```
Router# clear catalyst6000 traffic-meter
Router#
```

clear configuration lock

To clear the lock on the running configuration file, use the **clear configuration lock**command in privileged EXEC mode.

clear configuration lock

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(14)T	This command was enhanced to allow the exclusive configuration lock to be cleared during erratic or abnormal behavior.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)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(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Examples

The following is sample output from the **clear configuration lock**command when the running configuration file is not locked by the **configure replace** command:

```
Router# clear configuration lock

Parser Config not locked.
```

The following is sample output from the **clear configuration lock**command when the running configuration file is locked by the **configure replace** command:

```
Router# clear configuration lock

Process <3> is holding the EXCLUSIVE lock !
Do you want to clear the lock?[confirm] y
```

The following example shows how to use the **clear configuration lock** command to display the owner or process ID of the lock and prompt the user for confirmation:

```
Router# clear configuration lock
Process <46> is holding the EXCLUSIVE lock.
Do you want to clear the lock?[confirm] y
```

After the lock is cleared, a message will be sent to the terminal if the owner of the lock is a TTY user:

```
Router(config)# The configuration lock was cleared by user <steve> from terminal <5>
```

Related Commands

Command	Description
configuration mode exclusive	Enables single-user (exclusive) access functionality for the Cisco IOS CLI.
debug configuration lock	Enables debugging of the Cisco IOS configuration lock.
show configuration lock	Displays information about the lock status of the running configuration file during a configuration replace operation.

clear diagnostic event-log

To clear the diagnostic event logs for a specific module or event type, use the **clear diagnostic event-log**command in privileged EXEC mode.

clear diagnostic event-log {**event-type** {**error| info| warning**}| **module** {*num*| *slot subslot*| **all**}}

Syntax Description

event-type error	Specifies clearing error events.
event-type info	Specifies clearing informative events.
event-type warning	Specifies clearing warning events.
module *num* | *slot subslot*	Specifies clearing events for a specific module.
module all	Specifies clearing all linecards.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

The **clear diagnostic event-log** command clears all the events for all the modules.

The **clear diagnostic event-log module** *num* command clears events only for a specific module.

The **clear diagnostic event-log event-type**command clears only specific event types such as error, informative, or warning events.

Examples

This example shows how to clear error event logs:

```
Router# clear diagnostic event-log event-type error
```

This example shows how to clear event logs on module 3:

```
Router# clear diagnostic event-log module 3
```

This example shows how to clear error event logs on all the modules:

```
Router# clear diagnostic event-log module all
```

Related Commands

Command	Description
show diagnostic events	Displays the diagnostic event log

clear ip http client cache

To remove information from the HTTP client cache, use the **clear ip http client cache** command in privileged EXEC mode.

clear ip http client cache {**all**| **session** *session-name*| **url** *complete-url*}

Syntax Description

cache all	Removes all HTTP client cache entries.
cache session *session-name*	Removes HTTP client cache entries of the HTTP client application session specified by the *session-name* argument.
cache url *complete-url*	Removes the HTTP client cache entry whose location is specified by the *complete-url* argument, a Cisco IOS File System (IFS) Uniform Resource Locator (URL), and that consists of HTML files used by an HTTP server.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

Use this command to clear entries from the HTTP client cache pool: all the entries, all the entries owned by a specific session, or only the entry associated with a specific request from an HTTP server.

Examples

The following example clears all entries in the HTTP client cache:

```
Router# clear ip http client cache all
```

The following example removes HTTP client cache entries that belong to the HTTP Client File System (CFS) application:

```
Router# clear ip http client cache session HTTP CFS
```

The following example removes HTTP client cache entries at the location http://myrouter.cisco.com/flash:/:

```
Router# clear ip http client cache url http://myrouter.cisco.com/flash:/
```

Related Commands

Command	Description
ip http path	Specifies the base path used to locate files for use by the HTTP server.
show ip http client	Displays a report about the HTTP client.

clear logging

To clear messages from the logging buffer, use the **clear logging** command in privileged EXEC mode.

clear logging [**persistent** [**url** *filesystem***:**/*directory*]]

Syntax Description

persistent	(Optional) Deletes persistent logging files.
url	(Optional) Specifies the URL for storing logging messages.
*filesystem***:**	The file system followed by a colon.
/*directory*	The directory on the filesystem. The slash is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.4	This command was modified. The **persistent**and **url** keywords, and the *filesystem***:**/*directory* arguments were added.

Usage Guidelines

The **clear logging persistent** command is used to remove stored audit records. This action can be performed by the audit administrator only. The **clear logging persistent**command clears only log files stored in the directory but does not remove the directory itself. If no log URL is not specified for logging, this command clears files from the location as specified in the **logging persistent** command.

Examples

In the following example, the logging buffer is cleared:

```
Router# clear logging
Clear logging buffer [confirm]
```

The following example shows how to clear persistent logging files:

```
Router# clear logging persistent
Delete persistent logging files from bootflash:/audit_log ? [confirm]
Router# dir bootflash:/audit_log
Directory of bootflash:/audit_log/
No files in directory
```

The following example shows how to clear persistent logging files from a specific directory:

```
Router# clear logging persistent url harddisk:/log-persistant
 Delete persistent logging files from harddisk:/log-persistent ? [confirm]
Router# dir harddisk:/log-persistant
Directory of harddisk:////log-persistent/
No files in directory
```

Related Commands

Command	Description
logging buffered	Logs messages to an internal buffer.
logging persistent	Enables the storage of logging messages on the router's ATA disk.
show logging	Displays the state of logging (syslog).

clear logging system

To clear event records stored in the System Event Archive (SEA) log file sea_log.dat, use the **clear logging system** command in user EXEC mode.

clear logging system [**disk** *name*]

Syntax Description

disk *name*	(Optional) Stores the system event log in the specified disk.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SCC	This command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.

Usage Guidelines

SEA is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

Cisco Universal Broadband Router 10012

The SEA feature is used to address debug trace and system console constraints. SEA is a logging feature that allows the modules in the system to report major and critical events to the route processor (RP). The events occurring on the line card or jacket card are also sent to the RP using Inter-Process Communication (IPC) capability. Use the **clear logging system** command to clear the event records stored in the SEA log file.

Note To store the system event logs, the SEA requires either the PCMCIA ATA disk or Compact Flash Disk in compact flash adapter for PRE2.

Examples

This example shows how to clear the SEA:

```
Router# clear logging system
Clear logging system operation will take a while.
Do you want to continue? [no]: yes
Router#
```

Related Commands

copy logging system	Copies the archived system events to another location.
logging system	Enables or disables the SEA logging system.
show logging system	Displays the SEA logging system disk.

clear logging xml

To clear the contents of the XML system message logging (syslog) buffer, use the **clear logging xml** command in User EXEC or Priviledged EXEC mode..

clear logging xml

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE .

Usage Guidelines

This command clears the contents of the XML-formatted logging buffer, but does not clear the contents of the standard logging buffer. The system will prompt you to confirm the action before clearing the buffer.

Examples

In the following example, the XML-specific buffer is cleared:

```
Router# clear logging xml
Clear XML logging buffer [confirm]?y
```

Related Commands

Command	Description
logging buffered xml	Enables system message logging (syslog) to the XML-specific buffer in XML format.
show logging xml	Displays the state of XML-formatted system message logging, followed by the contents of the XML-specific buffer.

clear memory low-water-mark

To clear the low-water-mark memory, use the **clear memory low-water-mark**command in privilegedEXEC mode.

clear memory low-water-mark

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced into a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command clears all processor threshold values and the input/output memory threshold values, if any.

Examples

The following example shows how to clear the low-water-mark memory:

```
Router# clear memory low-water-mark
```

Related Commands

Command	Description
memory free low-watermark	Configures a router to issue system logging message notifications when available memory falls below a specified threshold.

clear mls statistics

To reset the Multilayer Switching (MLS) statistics counters, use the **clear mls statistics** command in privileged EXEC mode.

clear mls statistics [**module** *num*]

Syntax Description

module *num*	(Optional) Specifies the module number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.(17d)SXB1	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(17d)SXB5	The module *num* keyword and argumen t pair were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command replaces the **clear mls stats** command, which was introduced on the Supervisor Engine 720 in Cisco IOS Release 12.2(17a)SX, and on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.

Examples

This example shows how to reset the MLS statistics counters for all modules:

```
Router#
clear mls statistics
Router#
```

This example shows how to reset the MLS statistics counters for a specific module:

```
Router#
clear mls statistics module 5
Router#
```

Related Commands

Command	Description
show mls statistics	Displays the MLS statistics for the IP, IPX, multicast, Layer 2 protocol, and QoS.

clear parser cache

To clear the parse cache entries and hit/miss statistics stored for the Parser Cache feature, use the **clear parser cache**command in privileged EXEC mode.

clear parser cache

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The Parser Cache feature optimizes the parsing (translation and execution) of Cisco IOS software configuration command lines by remembering how to parse recently encountered command lines, decreasing the time required to process large configuration files.

The **clear parser cache** command will free the system memory used by the Parser Cache feature and will erase the hit/miss statistics stored for the output of the **show parser statistics** EXEC command. This command is only effective when the Parser Cache feature is enabled.

Examples

The following example shows the clearing of the parser cache:

```
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:820 ms
Parser cache:enabled, 1460 hits, 26 misses
Router# clear parser cache
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:820 ms
Parser cache:enabled, 0 hits, 1 misses
```

Related Commands

Command	Description
parser cache	Enables or disables the Parser Cache feature.
show parser statistics	Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.

clear parser statistics

To clear the parser performance statistics, use the **clear parser statistics**command in privileged EXEC mode.

clear parser statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.0S	This command was introduced.

Usage Guidelines

The **clear parser statistics** command will free the system memory used for recording parser performance statistics stored for the output of the **show parser statistics** EXEC command..

Examples

The following example shows the clearing parser statistics:

```
Router# show parser statistics
Last configuration file parsed: Number of Commands: 1, Time: 31 ms

Parser cache: enabled, 129 hits, 46 misses

Active startup time: 0
Standby startup time: 186
Copy to running-config time:0
Bulksync time:0

Top 10 slowest command:
  Function   Time (ms) Command
  0xE71F90       7      shutdown
  0x1235280      11     no ip address
  0x1235280      11     no ip address
  0x1235280      11     no ip address
  0x1235280      11     no ip address
  0x1235280      12     no ip address
  0x1235280      12     no ip address
  0x1235280      12     no ip address
  0x1235280      12     no ip address
  0xD6C940       6170  show run

Parser last bootup cache hits:
  Bootup hits:125
  Bootup misses:43
  Bootup clear parser cache:0

Router# clear parser statistics
func=E01730, duration=0 cmd= clear parser statistics
```

```
Router# show parser statistics
Last configuration file parsed: Number of Commands: 0, Time: 0 ms

Parser cache: enabled, 130 hits, 47 misses

Active startup time: 0
Standby startup time: 0
Copy to running-config time:0
Bulksync time:0

Top 10 slowest command:
  Function   Time (ms) Command

Parser last bootup cache hits:
  Bootup hits:0
  Bootup misses:0
  Bootup clear parser cache:0
```

Related Commands

Command	Description
parser cache	Enables or disables the Parser Cache feature.
show parser statistics	Displays statistics about the last configuration file parsed and the status of the Parser Cache feature.

clear platform netint

To clear the interrupt-throttling counters for the platform, use the **clear platform netint** command in privileged EXEC mode.

clear platform netint

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	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.

Examples

This example shows how to clear the interrupt-throttling counters for the platform:

```
Router#
clear platform netint
Router#
```

Related Commands

Command	Description
show platform netint	Displays the platform network-interrupt information.

clear processes interrupt mask

To clear interrupt mask details for all processes in the interrupt mask buffer, use the **clear processes interrupt mask detail**command in privileged EXEC mode.

clear processes interrupt mask detail

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)T	This command was introduced as part of the Process Interrupt Mask Profiler Enhancement feature.

Usage Guidelines

See the documentation of the **scheduler interrupt mask** commands (listed in the Related Commands table) for further details on process interrupt mask profiling.

Examples

The following example demonstrates how to the clear interrupt mask statistics from system memory for all processes:

```
Router# clear processes interrupt mask detail
```

Related Commands

Command	Description
scheduler interrupt mask profile	Starts interrupt mask profiling for all processes running on the system
scheduler interrupt mask size	Configures the maximum number of entries that can exist in the interrupt mask buffer.
scheduler interrupt mask time	Configures the maximum time that a process can run with interrupts masked.
show process interrupt mask buffer	Displays the information stored in the interrupt mask buffer.
show processes interrupt mask detail	Displays interrupt masked details for the specified processes or all processes in the system.

clear scp accounting

To clear the Switch-Module Configuration Protocol (SCP) accounting information, use the **clear scp accounting**command in privilegedEXEC mode.

clear scp accounting

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced into a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to clear the SCP accounting information:

```
Router# clear scp accounting
```

Related Commands

Command	Description
show scp	Displays SCP information.

clear tcp

To clear a TCP connection, use the **clear tcp**command in privileged EXEC mode.

clear tcp {**line** *line-number*| **local** *hostname port* **remote** *hostname port*| **tcb** *address*}

Syntax Description

line *line-number*	Line number of the TCP connection to clear.
local *hostname port* **remote** *hostname port*	Host name of the local router and port and host name of the remote router and port of the TCP connection to clear.
tcb *address*	Transmission Control Block (TCB) address of the TCP connection to clear. The TCB address is an internal identifier for the endpoint.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **clear tcp** command is particularly useful for clearing hung TCP connections.

The **clear tcp line** *line-number*command terminates the TCP connection on the specified tty line. Additionally, all TCP sessions initiated from that tty line are terminated.

The **clear tcp local** *hostname port* **remote** *hostname port*command terminates the specific TCP connection identified by the host name and port pair of the local and remote router.

The **clear tcp tcb** *address* command terminates the specific TCP connection identified by the TCB address.

Examples

The following example clears a TCP connection using its tty line number. The **show tcp** command displays the line number (tty2) that is used in the **clear tcp** command.

```
Router# show tcp

    tty2, virtual tty from host router20.cisco.com
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Local host: 171.69.233.7, Local port: 23
    Foreign host: 171.69.61.75, Foreign port: 1058

    Enqueued packets for retransmit: 0, input: 0, saved: 0
```

```
    Event Timers (current time is 0x36144):
    Timer          Starts    Wakeups            Next
    Retrans             4          0             0x0
    TimeWait            0          0             0x0
    AckHold             7          4             0x0
       SendWnd             0          0             0x0
    KeepAlive           0          0             0x0
    GiveUp              0          0             0x0
    PmtuAger            0          0             0x0

    iss: 4151109680  snduna: 4151109752  sndnxt: 4151109752     sndwnd:  24576
    irs: 1249472001  rcvnxt: 1249472032  rcvwnd:       4258  delrcvwnd:     30

    SRTT: 710 ms, RTTO: 4442 ms, RTV: 1511 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 300 ms

Router# clear tcp line 2
    [confirm]
     [OK]
```

The following example clears a TCP connection by specifying its local router host name and port and its remote router host name and port. The **show tcp brief** command displays the local (Local Address) and remote (Foreign Address) host names and ports to use in the **clear tcp** command.

```
Router# show tcp brief
TCB       Local Address           Foreign Address        (state)
    60A34E9C  router1.cisco.com.23      router20.cisco.1055  ESTAB

Router# clear tcp local router1 23 remote router20 1055
    [confirm]
     [OK]
```

The following example clears a TCP connection using its TCB address. The **show tcp brief** command displays the TCB address to use in the **clear tcp** command.

```
Router# show tcp brief
    TCB       Local Address           Foreign Address        (state)
    60B75E48  router1.cisco.com.23      router20.cisco.1054  ESTAB

Router# clear tcp tcb 60B75E48
    [confirm]
     [OK]
```

Related Commands

Command	Description
show tcp	Displays the status of TCP connections.
show tcp brief	Displays a concise description of TCP connection endpoints.

clear vlan counters

To clear the software-cached counter values to start from zero again for a specified VLAN or all existing VLANs, use the **clear vlan counters** command in privileged EXEC mode.

clear vlan [*vlan-id*] **counters**

Syntax Description

vlan-id	(Optional) The ID of a specific VLAN. Range: 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If you do not specify a *vlan-id*; the software-cached counter values for all existing VLANs are cleared.

Examples

This example shows how to clear the software-cached counter values for a specific VLAN:

```
Router# clear vlan 10 counters
Clear "show vlan" counters on this vlan [confirm]y
Router#
```

Related Commands

Command	Description
show vlan counters	Displays the software-cached counter values.

clock

To configure the port clocking mode for the 1000BASE-T transceivers, use the **clock** command in interface configuration mode. To return to the default settings,use the **no** form of this command.

clock {**auto**| **active [prefer]**| **passive [prefer]**}

no clock

Syntax Description

auto	Enables the automatic-clock configuration.
active	Enables the active operation.
prefer	(Optional) Negotiates the specified mode with the far end of the link.
passive	Enables the passive operation.

Command Default

auto

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17a)SX	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 supported on the 1000BASE-T transceivers only.

If the clock mode of the near end of a link does not match the clock mode of the far end, the line protocol does not come up.

The active and passive clock status is determined during the auto negotiation process before the transmission link is established.

The **clock** command supports the following configurations:

- **auto** --Auto negotiates with the far end of the link but preference is given to the active-clock switch.
- **active** --Uses a local clock to determine transmitter-operation timing.
- **passive** --Recovers the clock from the received signal and uses the recovered clock to determine transmitter-operation timing.

- **active prefer** --Auto negotiates with the far end of the link but preference is given to the active-clock switch.
- **passive prefer** --Auto negotiates with the far end of the link but preference is given to the passive-clock switch.

Enter the **show running-config interface** command to display the current clock mode.

Enter the **show interfaces** command to display the clock mode that is negotiated by the firmware.

Examples

This example shows how to enable the active-clock operation:

```
Router(config-if)# clock active
Router(config-if)#
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.
show running-config interface	Displays the status and configuration of the module or Layer 2 VLAN.

clock initialize nvram

To restart the system clock from the last known system clock value, use the **clock initialize nvram**command in global configuration mode. To disable the restart of the system clock from the last known system clock value, use the **no** form of this command.

clock initialize nvram

no clock initialize nvram

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the system clock is set to restart from the last known system clock value for platforms that have no hardware calendar.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

For platforms that have hardware calendars, the **clock initialize nvram** command is not available. When the **no** form of the command is configured, the system clock gets initialized to default standard values. The default values can be either 1MAR1993 or 1MAR2002.

Examples

The following example shows how to set the system clock to restart from the last known system clock value:

```
Router(config)# clock initialize nvram
```

config-register

To change the configuration register settings, use the **config-register** command in global configuration mode.

config-register *value*

Syntax Description

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

Command Default

Refer to the documentation for your platform for the default configuration register value. For many newer platforms, the default is 0x2102, which causes the router to boot from Flash memory and the Break key to be ignored.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Usage Guidelines

This command applies only to platforms that use a software configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

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

- If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the **boot** command.
- If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.
- If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

Note In a virtual switch application, If you have configured your config-register with a value that would skip file parsing during the bootup process, your change to either a standalone or virtual switch will not take place until you reconfigure your config-register. The config-register must be allowed to parse files in order to ensure the conversion from either a standalone or virtual switch.

Examples

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

```
config-register 0x2102
```

Related Commands

Command	Description
boot system	Specifies the system image that the router loads at startup.
confreg	Changes the configuration register settings while in ROM monitor mode.
o	Lists the value of the boot field (bits 0 to 3) in the configuration register.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

configure check syntax

To check the syntax configuration, use the **configure check syntax** commandinprivilegedEXEC mode.

configure check syntax [*source-location*]

Syntax Description

source-location	(Optional) Location or the address of the source to be checked.

Command Default

The syntax configuration is not checked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.

Examples

The following example shows how to check the syntax configuration using the **configure check syntax** command:

```
Router# configure check syntax revrcsf:
```

Related Commands

Command	Description
configure revert	Cancels the timed rollback and triggers the rollback immediately, or resets the parameters for the timed rollback.

configuration mode exclusive

Note Effective with Cisco IOS XE Release 3.1S, the **configuration mode exclusive** command is replaced by the **parser command serializer** command. See the **parser command serializer** command for more information.

To enable single-user (exclusive) access functionality for the Cisco CLI, use the **configuration mode exclusive** command in global configuration mode. To disable the single-user access (configuration locking) feature, use the **no** form of this command.

configuration mode exclusive {**auto**| **manual**} [**expire** *seconds*] **[lock-show] [interleave] [terminate]** [**config-wait** *seconds*] [**retry-wait** *seconds*]

no configuration mode exclusive

Syntax Description

auto	Automatically limits configuration to single-user mode.
manual	Allows you to manually limit the configuration file to single-user mode.
expire *seconds*	(Optional) Specifies the number of seconds in which the configuration lock is released after the user stops making configuration changes.
lock-show	(Optional) Gives priority to configuration commands being executed from the exclusive configuration session, and prevents the execution of **show** commands.
interleave	(Optional) Allows **show** commands from sessions that are not holding the configuration lock to be executed when the user in the session holding the configuration lock is not making configuration changes. **Note** If you entered the **lock-show**keyword, you should enter this keyword.
terminate	(Optional) Causes the configuration command executed from the exclusive configuration session to terminate **show** and **clear** commands being executed in other sessions.

config-wait *seconds*	(Optional) Specifies the amount of time, in seconds, that a configuration command entered by a user in single user mode waits for **show** commands entered by other users to finish being executed. If the **show** command is still being executed when the timer expires and if the **terminate** option is set, the configuration command terminates the **show** command. If the configuration command completes execution before the specified number of seconds, the **show** command begins execution.
retry-wait *seconds*	(Optional) Specifies the amount of time, in seconds, that **show** and **clear** EXEC commands will wait for a configuration command entered by a user in exclusive configuration mode to complete execution. If the configuration command is still being executed when the specified amount of time has passed, the EXEC commands generate an error message and are terminated. If execution of the configuration command is completed before the specified number of seconds, the EXEC commands are executed.

Command Default

Single-user mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S. The following keywords were added: **config-wait**, **expire**, **interleave, lock-show**,**retry-wait,**and **terminate**. New functionality was added, including Access Session Locking.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
15.0(1)S	This command was deprecated for Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was replaced by the **parser command serializer** command.

Usage Guidelines

Note As of the 15.0 release, the configuration mode exclusive command is no longer available on the S and T trains.

The **configuration mode exclusive** command enables the exclusive configuration lock feature. The exclusive configuration lock allows single-user access to configuration modes using single-user configuration mode. While the device configuration is locked, no other users can enter configuration commands.

Users accessing the device using the state-full, session-based transports (telnet, Secure Shell (SSH) are able to enter single-user configuration mode. The user enters single-user configuration mode by acquiring the exclusive configuration lock using the **configure terminal lock** privileged EXEC mode command. The configuration lock is released when the user exits configuration mode by using the **end** or **exit** command, or by pressing Ctrl-Z. While a user is in single-user configuration mode, no other users can configure the device. Users accessing Command Line Interface (CLI) options through stateless protocols (that is, the HTTP web-based user interface) cannot access single-user configuration mode. (However, an Application Programming Interface (API) allows the stateless transports to lock the configuration mode, complete its operations, and release the lock.)

Examples

The following example shows how to configure the configuration file for single-user autoconfiguration mode by using the **configuration mode exclusive auto** command. Use the **configuration terminal** command to enter global configuration mode and lock the configuration mode exclusively. After the Cisco configuration mode is locked exclusively, you can verify this configuration by entering the **show configuration lock** command.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# configuration mode exclusive auto
Device(config)# end
Device# show running-configuration
 | include config


Building configuration...
Current configuration : 2296 bytes
configuration mode exclusive auto <========== auto policy
Device# configure terminal ?
 <======== lock option not displayed when in auto policy
Device# configure terminal
 <======= acquires the lock
```

The configuration mode is locked exclusively. The lock is cleared after you exit from configuration mode by entering the **end** or **exit** command.

```
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
Device(config)# show configuration lock


Parser Configure Lock
---------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
```

```
Count : 1
Pending Requests : 0
User debug info : configure terminal
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 6
Lock Expiration timer (in Sec) : 593
Device(config)#
Device(config)# end
 <========= releases the lock
Device#
Device# show configuration lock


Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
```

The following example shows how to enable the exclusive locking feature in manual mode by using the **configuration mode exclusive manual** command. Once you have configured manual exclusive mode, you can lock the configuration mode by using the **configure terminal lock** command. In this mode, the **configure terminal** command does not automatically lock the parser configuration mode. The lock is cleared after you exit from configuration mode by entering the **end** or **exit** command.

```
Device# configure terminal

Configuration mode locked exclusively. The lock will be cleared once you exit out of
configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# configuration mode exclusive manual

Device(config)# end

Device#
Device# show running-configuration
 | include configuration

Building configuration...
Current configuration : 2298 bytes
configuration mode exclusive manual <==== 'manual' policy
Device# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
```

```
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#
Device# configure terminal ?

lock Lock configuration mode <========= 'lock' option displayed in 'manual' policy
Device# configure terminal <============ ‘configure terminal’ won't acquire lock automatically
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# show configuration lock

Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device(config)# end

Device# show configuration lock


Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#
Device# configure

Device# configure terminal

Device# configure terminal ?

lock Lock configuration mode <======= 'lock' option displayed when in 'manual' policy
Device# configure terminal lock

Device# configure terminal lock
 <============ acquires exclusive configuration lock
```

Configuration mode is locked exclusively. The lock is cleared after you exit from configuration mode by entering the **end** or **exit** command. Enter configuration commands, one per line. End with CNTL/Z.

```
Device(config)# show configuration lock

Parser Configure Lock
---------------------
Owner PID : 3
User : unknown
TTY : 0
Type : EXCLUSIVE
State : LOCKED
Class : EXPOSED
Count : 1
Pending Requests : 0
User debug info : configure terminal lock
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 5
Lock Expiration timer (in Sec) : 594
Device(config)# end
 <================ 'end' releases exclusive configuration lock
Device# show configuration lock


Parser Configure Lock
---------------------
Owner PID : -1
User : unknown
TTY : -1
Type : NO LOCK
State : FREE
Class : unknown
Count : 0
Pending Requests : 0
User debug info :
Session idle state : TRUE
No of exec cmds getting executed : 0
No of exec cmds blocked : 0
Config wait for show completion : FALSE
Remote ip address : Unknown
Lock active time (in Sec) : 0
Lock Expiration timer (in Sec) : 0
Device#
```

Related Commands

Command	Description
configure terminal	Enters global configuration mode.
debug configuration lock	Enables debugging of the Cisco configuration lock.
show configuration lock	Displays information about the lock status of the running configuration file during a configuration replace operation.

configure confirm

To confirm replacement of the current running configuration with a saved Cisco configuration file, use the **configure confirm** command in privileged EXEC mode.

configure confirm

Syntax Description

This command has no arguments or keywords.

Command Default

The replacement of the current running configuration with a saved configuration file is not confirmed.

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 Cisco IOS Release 12.2S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2SR.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2SX.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **configure confirm** command is used only if the **time** *seconds* keyword and argument of the **configure replace** command are specified. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command).

Examples

The following example shows the use of the **configure replace** command with the **time** *seconds* keyword and argument. You must enter the **configure confirm** command within the specified time limit to confirm replacement of the current running configuration file:

```
Device# configure replace nvram:startup-config time 120
```

```
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco configuration archive.
configure replace	Replaces the current running configuration with a saved Cisco configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.
path (config-archive)	Specifies the location and filename prefix for the files in the Cisco configuration archive.
show archive	Displays information about the files saved in the Cisco configuration archive.
time-period	Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.

configure memory

To configure the system from the system memory, use the **configure memory** command in privileged EXEC mode.

configure memory

Syntax Description

This command has no arguments or keywords.

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

On all platforms except Class A Flash file system platforms, this command executes the commands located in the configuration file in NVRAM (the "startup configuration file").

On Class A Flash file system platforms, if you specify the **configure memory** command, the router executes the commands pointed to by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable specifies the location of the configuration file that the router uses to configure itself during initialization. The file can be located in NVRAM or any of the Flash file systems supported by the platform.

When the CONFIG_FILE environment variable specifies NVRAM, the router executes the NVRAM configuration only if it is an entire configuration, not a distilled version. A distilled configuration is one that does not contain access lists.

To view the contents of the CONFIG_FILE environment variable, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** command and then save your changes by issuing the **copy system:running-config nvram:startup-config** command.

Examples

In the following example, a router is configured from the configuration file in the memory location pointed to by the CONFIG_FILE environment variable:

```
Router# configure memory
```

Related Commands

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

Command	Description
copy system:running-config nvram:startup-config	Saves the running configuration as the startup configuration file.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

configure network

The **configure network** command was replaced by the **copy**{**rcp**| **tftp**} **running-config** command in Cisco IOS Release 11.0. To maintain backward compatibility, the **configure network** command continues to function in Cisco IOS Release 12.2(11)T for most systems, but support for this command may be removed in a future release.

The **copy**{**rcp**| **tftp**} **running-config** command was replaced by the **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system: running-config** command in Cisco IOS Release 12.1.

The **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system: running-config** command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the **copy** command in this chapter for more information.

configure overwrite-network

The **configure overwrite-network** has been replaced by the **copy** {*ftp-url* | *rcp-url* | *tftp-url* **nvram:startup-config** command. See the description of the **copy**command in the Cisco IOS File System Commands chapter for more information.

configure replace

To replace the current running configuration with a saved Cisco configuration file, use the **configure replace** command in privileged EXEC mode.

configure replace *target-url* **[nolock] list force ignorecase** [**revert trigger [error]** [**timer** *minutes*]| **time** *minutes*]

Syntax Description

target-url	URL (accessible by the Cisco file system) of the saved Cisco configuration file that is to replace the current running configuration.
nolock	(Optional) Disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replace operation.
list	(Optional) Displays a list of the command lines applied by the Cisco software parser during each pass of the configuration replace operation. The total number of passes performed is also displayed.
force	(Optional) Replaces the current running configuration file with the specified saved Cisco configuration file without prompting you for confirmation.
ignorecase	(Optional) Instructs the configuration to ignore the case of the configuration confirmation.
revert trigger	(Optional) Sets the triggers for reverting to the original configuration. • **error** --Reverts to the original configuration upon error. • **timer** *minutes* --Reverts to the original configuration if the specified time elapses.
time *minutes*	(Optional) Time (in minutes) within which you must enter the **configure confirm** command to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command).

Command Modes Privileged EXEC (#)

Command Default The current running configuration is not replaced with a saved configuration file.

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	The **nolock** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(20)T	The **revert** and **trigger** keywords were added.
12.2(33)SRC	The **ignorecase** keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines When configuring more than one keyword option, the following rules apply:

- The **list** keyword must be entered before the **force** and **time** keywords.
- The **force** keyword must be entered before the **time** keyword.

If the current running configuration is replaced with a saved Cisco configuration file that contains commands unaccepted by the Cisco software parser, an error message is displayed listing the commands that were unaccepted. The total number of passes performed in the configuration replace operation is also displayed.

In Cisco IOS Release 12.2(25)S, a locking feature for the configuration replace operation was introduced. When the **configure replace** command is enabled, the Cisco running configuration file is locked by default for the duration of the configuration replace operation. This locking mechanism prevents other users from changing the running configuration while the replace operation is taking place, which might otherwise cause the replace operation to terminate unsuccessfully. You can disable the locking of the running configuration using the **configure replace nolock** command.

The running configuration lock is automatically cleared at the end of the configuration replace operation. It is not expected that you should need to clear the lock manually during the replace operation, but as a protection against any unforeseen circumstances, you can manually clear the lock using the **clear configuration lock** command. You can also display any locks that may be currently applied to the running configuration using the **show configuration lock** command.

Examples

This section contains the following examples:

- Replacing the Current Running Configuration with a Saved Cisco Configuration File
- Reverting to the Startup Configuration File
- Performing a Configuration Replace Operation with the configure confirm Command
- Performing a Configuration Rollback Operation

Examples

The following example shows how to replace the current running configuration with a saved Cisco configuration file named disk0:myconfig. Note that the **configure replace** command interactively prompts you to confirm the operation.

```
Device# configure replace disk0:myconfig
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
```

In the following example, the **list** keyword is specified to display the command lines that were applied during the configuration replace operation:

```
Device# configure replace disk0:myconfig list
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
!Pass 1
!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro

end
Total number of passes: 1
Rollback Done
```

Examples

The following example shows how to revert to the Cisco startup configuration file. This example also shows the use of the optional **force** keyword to override the interactive user prompt.

```
Device# configure replace nvram:startup-config force
Total number of passes: 1
Rollback Done
```

Examples

The following example shows the use of the **configure replace** command with the **time** *seconds* keyword and argument. You must enter the **configure confirm** command within the specified time limit to confirm replacement of the current running configuration file. If the **configure confirm** command is not entered within

the specified time limit, the configuration replace operation is automatically reversed (in other words, the current running configuration file is restored to the configuration state that existed prior to entering the **configure replace** command).

```
Device# configure replace nvram:startup-config time 120
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y
Total number of passes: 1
Rollback Done
Device# configure confirm
```

Examples

The following example shows how to make changes to the current running configuration and then roll back the changes. As part of the configuration rollback operation, you must save the current running configuration before making changes to the file. In this example, the **archive config** command is used to save the current running configuration. Note that the generated output of the **configure replace** command indicates that only one pass was performed to complete the rollback operation.

Note The **path** command must be configured before using the **archive config** command.

You first save the current running configuration in the configuration archive as follows:

```
Device# archive config
```

You then enter configuration changes as shown in the following example:

```
Device# configure terminal
Device(config)# user netops2 password rain
Device(config)# user netops3 password snow
Device(config)# exit
```

After making changes to the running configuration file, you might want to roll back these changes and revert to the configuration that existed before the changes were made. The **show archive** command is used to verify the version of the configuration to be used as a target file. The **configure replace** command is then used to revert to the target configuration file as shown in the following example:

```
Device# show archive
There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
 Archive #  Name
   0
   1       disk0:myconfig-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
Device# configure replace disk0:myconfig-1
Total number of passes: 1
Rollback Done
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco configuration archive.
configure confirm	Confirms replacement of the current running configuration with a saved Cisco configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.
path	Specifies the location and filename prefix for the files in the Cisco configuration archive.
show archive	Displays information about the files saved in the Cisco configuration archive.
time-period	Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.

configure revert

To cancel the timed rollback and trigger the rollback immediately, or to reset the parameters for the timed rollback, use the **configure revert** command in privileged EXEC mode.

configure revert {**now**| **timer** {*minutes*| **idle** *minutes*}}

Syntax Description

now	Cancels the timed rollback and reverts immediately.
timer	Resets the confirmation timer.
minutes	Time in minutes (1-120).
idle *minutes*	Idle time in minutes (1-120) for which to wait before rollback.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

In order to use the **configure revert** command to configure a timed rollback, the Configuration Archive functionality must be enable first. The Configuration Archive APIs are used to store the current configuration before applying any changes or rolling back to the previous configuration.

In case of multi-user environments, only the user who enabled the timed rollback functionality will have the permission to perform the following operations:

- Confirm the configuration change
- Reset the timer
- Cancel the timer and trigger rollback immediately

Examples

The following example shows how to cancel the timed rollback and revert to the saved configuration immediately:

```
Device(config)# archive
Device(config-archive)# path disk0:abc
Device# configure revert now
```

Related Commands

Command	Description
archive config	Saves a copy of the current running configuration to the Cisco configuration archive.
configure replace	Replaces the current running configuration with a saved Cisco configuration file.
maximum	Sets the maximum number of archive files of the running configuration to be saved in the Cisco configuration archive.
path (config-archive)	Specifies the location and filename prefix for the files in the Cisco configuration archive.
show archive	Displays information about the files saved in the Cisco configuration archive.
time-period	Sets the time increment for automatically saving an archive file of the current running configuration in the Cisco configuration archive.

configure terminal

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

configure terminal

Cisco IOS Releases 12.3(14)T and Subsequent Releases:

configure terminal [lock]

Cisco IOS Releases 12.2(33)SRC and Subsequent Releases:

configure terminal [**revert** {**timer** *minutes*| **idle** *minutes*}]

Syntax Description

lock	(Optional) Locks the running configuration into exclusive configuration mode for the duration of your configuration session. This keyword only functions if the **configuration mode exclusive** command was previously enabled.
revert	(Optional) Sets the parameters for reverting the configuration if confirmation of the new configuration is not received.
timer *minutes*	Time in minutes (1-120) for which to wait for confirmation.
idle *minutes*	Idle time in minutes (1-120) for which to wait for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	The **lock** keyword option was added.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	The **revert** keyword option was added, along with the timer parameters of **idle** and *minutes*.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

Use this command to enter global configuration mode. Note that commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).

After you enter the **configure terminal** command, the system prompt changes from <device-name># to <device-name>(config)# , indicating that the device is in global configuration mode. To leave global configuration mode and return to privileged EXEC mode, type **exit** or press **Ctrl-Z**.

To view the changes to the configuration you have made, use the **more system:running-config** command or **show running-config** command in user EXEC or privileged EXEC mode.

Configuration Locking

The first user to enter the **configure terminal lock** command acquires the configuration lock (exclusive configuration mode).

Examples

The following example shows how to enter global configuration mode and lock the Cisco software in exclusive mode:

```
Device(config)# configure terminal lock
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the device configures itself during initialization (startup).
configuration mode exclusive	Enables locking of the configuration file for single user access.
copy running-config startup-config or **copy system:running-config nvram:startup-config**	Saves the running configuration as the startup configuration file.
show running-config or **more system:running-config**	Displays the currently running configuration.

confreg

To change the configuration register settings while in ROM monitor mode, use the **confreg** command in ROM monitor mode.

confreg [*value*]

Syntax Description

value	(Optional) Hexadecimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF.

Command Default

Refer to your platform documentation for the default configuration register value.

Command Modes

ROM monitor

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

Not all versions in the ROM monitor support this command. Refer to your platform documentation for more information on ROM monitor mode.

If you use this command without specifying the configuration register value, the router prompts for each bit of the configuration register.

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.

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

- If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the **boot** command.
- If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.
- If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.

For more information about the configuration register bit settings and default filenames, refer to the appropriate router hardware installation guide.

Examples

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

```
confreg 0x210F
```

In the following example, no configuration value is entered, so the system prompts for each bit in the register:

```
rommon 7 > confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

     Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:
You must reset or power cycle for new config to take effect.
rommon 8>
```

continue (ROM monitor)

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

continue

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

ROM monitor

Command History

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

Usage Guidelines

Use this command to return to EXEC mode from ROM monitor mode, to use the system image instead of reloading. On older platforms, the angle bracket (< >) indicates that the router is in ROM monitor mode. On newer platforms, rommon number> is the default ROM monitor prompt. Typically, the router is in ROM monitor mode when you manually load a system image or perform diagnostic tests. Otherwise, the router will most likely never be in this mode.

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

Examples

In the following example, the **continue** command switches the router from ROM monitor to EXEC mode:

```
> continue
Router#
```

Related Commands

Command	Description
boot	Boots the router manually.

copy

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

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

Syntax Description

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

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

The table below shows two keyword shortcuts to URLs.

Table 1: Common Keyword Aliases to URLs

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

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

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

Table 2: URL Prefix Keywords for Special File Systems

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

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

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

Table 3: URL Prefix Keywords for Remote File Systems

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

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

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

Table 4: URL Prefix Keywords for Local Writable Storage File Systems

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

Alias	Source or Destination
slot0:	Source or destination URL of the first PCMCIA flash memory card.
slot1:	Source or destination URL of the second PCMCIA flash memory card.
stby-bootflash:	Source or destination URL for boot flash memory in standby RP.
stby-harddisk:	Source or destination URL for the standby harddisk.
stby-usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the standby RP.
usb [0-1] :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router and is located on the active RP.
usbflash 0 9 :	Source or destination URL for the Universal Serial Bus (USB) flash drive that has been plugged into the router.
usbtoken [**0 9**] :	Source or destination URL for the USB eToken that has been plugged into the router.

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

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

Release	Modification
12.3(4)T	The /**verify**and /**noverify** keywords were integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	The **http://** and **https://** keywords were enhanced to support file uploads.
12.3(14)T	The **usbflash 0 9 :**and **usbtoken 0 9 :**keywords were added to support USB storage.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	The Cisco ASR1000 series routers became available, and introduced the **copy** command in diagnostic mode.
Cisco IOS XE Release 3.9S	The command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

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

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

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

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

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

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

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

The following sections contain usage guidelines for the following topics:

Understanding Invalid Combinations of Source and Destination

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

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

Understanding Character Descriptions

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

Table 5: copy Character Descriptions

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

Understanding Partitions

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

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

Using rcp

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

1 The remote username specified in the **copy** command, if a username is specified.

2 The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.

3 The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.

4 The router host name.

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

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

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

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

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

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

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

Using FTP

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

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

1 The username specified in the **copy** command, if a username is specified.

2 The username set by the **ip ftp username** command, if the command is configured.

3 Anonymous.

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

1 The password specified in the **copy** command, if a password is specified.

2 The password set by the **ip ftp password** command, if the command is configured.

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

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

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

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

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

Using HTTP or HTTPS

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

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

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

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

1 The username specified in the **copy** command, if a username is specified.

2 The username set by the **ip http client username** command, if the command is configured.

3 Anonymous.

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

1 The password specified in the **copy** command, if a password is specified.

2 The password set by the **ip http client password** command, if the command is configured.

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

Storing Images on Servers

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

Copying from a Server to Flash Memory

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

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

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

Verifying Images

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

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

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

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

Copying a Configuration File from a Server to the Running Configuration

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

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

Copying a Configuration File from a Server to the Startup Configuration

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

Storing the Running or Startup Configuration on a Server

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

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

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

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

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

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

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

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

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

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

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

To view the contents of environment variables, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT

environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config**command.

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

Using the Copy Command with the Dual RSP Feature

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

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

Using the copy command with the ASR1000 Series Routers

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

Using the copy command with the Cisco 4400 Series ISRs

Use the **copy** command in both privileged EXEC and diagnostic mode on the Cisco 4400 Series Integrated Services Routers (ISRs) to copy all types of files between directories and remote locations.

Examples

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

Examples

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

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

Examples

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

Examples

The following example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to flash memory. On Class B file system platforms, the Cisco IOS software allows you to

first erase the contents of flash memory to ensure that enough flash memory is available to accommodate the system image.

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

Examples

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

```
Router# copy tftp: flash:

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

Source file name? master/igs-bfpx-100.4.3

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

Examples

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses,

the Cisco IOS software prompts you to erase the files on the flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

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

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

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

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

Examples

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

Examples

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

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

Examples

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

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

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

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

Examples

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

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

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

Examples

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

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

Examples

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

```
Router#
copy bootflash:file1 tftp://192.168.117.23/file1
Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
  as 'file1'? [yes/no]y
```

```
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Examples

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

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

Examples

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

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

Examples

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

```
Router# configure terminal

Router(config)# ip rcmd remote-username netadmin1

Router(config)#
end

Router#
copy system:running-config rcp:

Remote host[]? 172.16.101.101

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

Examples

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

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

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

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

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

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

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

Enter no to escape writing the configuration information to memory.

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

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

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

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

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

Building configuration...

5267 bytes copied in 0.720 secs
```

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

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

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

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

Examples

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

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

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

Examples

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

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

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

```
Router# configure terminal

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

Router(config)# end

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

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

```
Router# configure terminal

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

Router(config)# end

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

Examples

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

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

Related Commands

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

copy erase flash

The **copy erase flash** command has been replaced by the **erase flash:**command. See the description of the **erase** command for more information.

O n some platforms, use can use the **copy /erase** *source-url* **flash:** syntax to erase the local Flash file system before copying a new file into Flash. See the desciption of the **copy** command for details on this option.

copy http

The **copy http://** command is documented as part of the **copy** command.

copy https

The **copy https://** command is documented as part of the **copy** command.

copy logging system

To copy archived system events to a destination file system, use the **copy logging system**command in privileged EXEC mode. To stop copying the archived system events, use the **no** form of the command.

copy logging system *target***:** *filename*

no copy logging system

Syntax Description

target **:**	Specifies the destination file system; Valid values are as follows: • **bootflash:** • **disk0:** • **disk1:** • **ftp:** • **http:** • **https:** • **rcp:** • **slavebootflash:** • **slavedisk0:** • **slavedisk1:** • **slavesup-bootdisk:** • **slavesup-bootflash:** • **sup-bootdisk:** • **sup-bootflash:** • **tftp:**
filename	Name of the file.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SCC	The command was introduced for the Cisco uBR10012 router in the Cisco IOS Software Release 12.2(33)SCC.

Usage Guidelines

System Event Archive (SEA) is supported on switches that have a Supervisor Engine 32 or Supervisor Engine 720 with a compact flash adapter and a Compact Flash card (WS-CF-UPG= for Supervisor Engine 720).

Cisco Universal Broadband Router 10012

The System Event Archive (SEA) feature is used to address the debug trace and system console constraints. Use the **copy logging system**command to copy the major and critical events stored in the sea_log.dat file, to the destination file system.

Note To store the system event logs, the SEA requires either the PCMCIA ATA disk or Compact Flash Disk in compact flash adapter for PRE2.

The following example shows how to copy the SEA to the file system of disk0:

```
Router# copy logging system disk0:
Destination filename [sea_log.dat]?
```

The following example shows how to copy the SEA using the remote file copy function (rcp):

```
Router# copy logging system rcp:

Address or name of remote host []? 192.0.2.1
Destination username [Router]? username1
Destination filename [sea_log.dat]? /auto/tftpboot-users/username1/sea_log.dat
```

Related Commands

clear logging system	Clears the event records stored in the SEA.
logging system	Enables or disables SEA logging system.
show logging system	Displays the SEA logging system disk.

copy xmodem

To copy 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, use the **copy xmodem:** command in EXEC mode.

copy xmodem: *flashfilesystem***:**

Syntax Description

flash-filesystem **:**	Destination of the copied file, followed by a colon.

Command Modes

EXEC

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is a form of the **copy** command. The **copy xmodem:** and **copy xmodem** commands are identical. See the description of the **copy** command for more information.

Copying a file using FTP, rcp, or TFTP is much faster than copying a file using Xmodem. Use the **copy xmodem:** command only if you do not have access to an FTP, TFTP, or rcp server.

This copy operation is performed through the console or AUX port. The AUX port, which supports hardware flow control, is recommended.

No output is displayed on the port over which the transfer is occurring. You can use the **logging buffered** command to log all router messages sent to the console port during the file transfer.

Examples

The following example initiates a file transfer from a local or remote computer to the router's internal Flash memory using the Xmodem protocol:

```
copy xmodem: flash:
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.

Command	Description
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.

copy ymodem

To copy 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, use the **copy ymodem:** command in EXEC mode.

copy ymodem: *flashfilesystem***:**

Syntax Description

flash-filesystem **:**	Destination of the copied file, followed by a colon.

Command Modes

EXEC

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **copy ymodem:** and **copy ymodem** commands are identical. See the description of the **copy**command for more information.

Copying a file using FTP, rcp, or TFTP is much faster than copying a file using Ymodem. Use the **copy ymodem:** command only if you do not have access to an FTP, rcp, or TFTP server.

This copy operation is performed through the console or AUX port. The AUX port, which supports hardware flow control, is recommended.

No output is displayed on the port over which the transfer is occurring. You can use the **logging buffered** command to log all router messages sent to the console port during the file transfer.

Examples

The following example initiates a file transfer from a local or remote computer to the router's internal Flash memory using the Ymodem protocol:

```
copy ymodem: flash:
```

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 noverify

To disable the automatic image verification for the current copy operation, use the **copy /noverify**command.

copy /noverify *source-url destination-url*

Syntax Description

source-url	Location URL or alias of the source file or directory to be copied; see the “Usage Guidelines” section for additional information.
destination-url	Destination URL or alias of the copied file or directory; see the “Usage Guidelines” section for additional information.

Command Default

Verification is done automatically after completion of a copy operation.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).

Timesaver

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

The table below shows two keyword shortcuts to URLs.

Table 6: Common Keyword Aliases to URLs

Keyword	Source or Destination
running-config	(Optional) Specifies the alias for the **system:running-config** URL. This keyword does not work in the **more** and **show file** command syntaxes.
startup-config	(Optional) Specifies the alias for the **nvram:startup-config URL.**The **nvram:startup-config** keyword represents the configuration file that is used during initialization (startup). This file is contained in NVRAM. This keyword does not work in **more** and **show file** EXEC command syntaxes.

The following tables list aliases by file system type. If you do not specify an alias, the system looks for a file in the current directory.

The table below lists the URL prefix aliases for special (opaque) file systems.

Table 7: URL Prefix Aliases for Special File Systems

Alias	Source or Destination
flh:	Source URL for Flash load helper log files.
nvram:	Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.
system:	Source or destination URL for system memory, which includes the running configuration.
xmodem:	Source destination for the file from a network device that uses the Xmodem protocol.
ymodem:	Source destination for the file from a network device that uses the Ymodem protocol.

The table below lists the URL prefix aliases for network file systems.

Table 8: URL Prefix Aliases for Network File Systems

Alias	Source or Destination
ftp:	Source or destination URL for an FTP network server. The syntax for this alias is as follows:**ftp:**[[[//username [:password]@]location]/directory]/filename.
rcp:	Source or destination URL for an rcp network server. The syntax for this alias is as follows: **rcp:**[[[//username@] location]/directory]/filename.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**[[//location]/directory]/filename.

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

Table 9: URL Prefix Aliases for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of rotating media.
flash:	Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a Flash: device, note that flash: is aliased to slot0:, allowing you to refer to the main Flash memory storage area on all platforms.
slavebootflash:	Source or destination URL for internal Flash memory on the slave RSP card of a device that is configured for HSA.
slaveram:	NVRAM on a slave RSP card of a device that is configured for HSA.
slavedisk0:	Source or destination URL of the first PCMCIA card on a slave RSP card of a device that is configured for HSA.
slavedisk1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a device that is configured for HSA.

Alias	Source or Destination
slaveslot0:	Source or destination URL of the first PCMCIA card on a slave RSP card of a router configured for HSA--Available on systems that are configured with a Supervisor Engine 2.
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA--Available on systems that are configured with a Supervisor Engine 2.
slot0:	Source or destination URL of the first PCMCIA Flash memory card--Available on systems that are configured with a Supervisor Engine 2.
slot1:	Source or destination URL of the second PCMCIA Flash memory card--Available on systems that are configured with a Supervisor Engine 2.

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

If you enter information, choose one of the following three options: **running-config**, **startup-config**, or a file system alias (see the tables above). The location of a file system dictates the format of the source or destination URL.

The colon is required after the alias. However, earlier commands that do not require a colon remain supported but are unavailable in context-sensitive help.

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

In the alias syntax for **ftp:**, **rcp:**, and **tftp:**, the location is either an IP address or a hostname. The filename is specified for the directory that is used for file transfers.

Enter the **file verify auto**command to set up verification globally.

Examples

This example shows how to disable the automatic image verification for the current copy operation:

```
Router# copy /noverify tftp: sup-bootflash:
.............................................
[OK - 24301348 bytes]
24301348 bytes copied in 157.328 secs (154463 bytes/sec)
Router#
```

Related Commands

Command	Description
file verify auto	Verifies the compressed Cisco IOS image checksum.

Command	Description
verify	Verifies the checksum of a file on a Flash memory file system or compute an MD5 signature for a file.