

calendar set

To manually set the hardware clock (calendar), use one of the formats of the **calendar set** command in EXEC mode.

calendar set *hh:mm:ss day month year*

calendar set *hh:mm:ss month day year*

Syntax Description

<i>hh:mm:ss</i>	Current time in hours (using 24-hour notation), minutes, and seconds.
<i>day</i>	Current day (by date) in the month.
<i>month</i>	Current month (by name).
<i>year</i>	Current year (no abbreviation).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. In Cisco IOS software syntax, the hardware clock is called the “calendar.” The hardware clock is a battery-powered chip that runs continuously, even if the router is powered off or rebooted. After you set the hardware clock, the software clock will be automatically set from the hardware clock when the system is restarted or when the **clock read-calendar** EXEC command is issued. The time specified in this command is relative to the configured time zone.

Examples

The following example manually sets the hardware clock to 1:32 p.m. on May 19, 2003:

```
Router# calendar set 13:32:00 May 19 2003
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock set	Sets the software clock.
clock summer-time	Configures the system time to automatically switch to summer time (daylight saving time).

Command	Description
clock timezone	Sets the time zone for display purposes.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.

call-home request

To submit information about your system to Cisco for report and analysis information from the Cisco Output Interpreter tool, use the **call-home request** command in privileged EXEC mode. An analysis report will be sent by Cisco to a configured contact e-mail address.

call-home request { **output-analysis** “*show-command*” | **config-sanity** | **bugs-list** | **command-reference** | **product-advisory** } [**profile** *name*] [**ccoid** *user-id*]

Syntax Description	output-analysis “ <i>show-command</i> ”	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (“ ”).
	config-sanity bugs-list command-reference product-advisory	Specifies the type of report requested. Based on this keyword, the output of a predetermined set of commands such as the show running-config all , show version , and show module (standalone) or show module switch all (VS system) commands, will be sent to Cisco for analysis.
	profile <i>name</i>	Specifies an existing profile to which the request will be sent. If no profile is specified, the request will be sent to the Cisco TAC profile.
	ccoid <i>user-id</i>	Specifies the identifier of a registered Smart Call Home user. If a <i>user-id</i> is specified, the resulting analysis report will be sent to the e-mail address of the registered user. If no <i>user-id</i> is specified, the report will be sent to the contact e-mail address of the device.

Command Default This command has no default settings.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SXI	This command was introduced.

Usage Guidelines The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.

Based on the keyword specifying the type of report requested, the following information will be returned in response to the request:

- **config-sanity**—Information on best practices as related to the current running configuration.
- **bugs-list**—Known bugs in the running version and in the currently applied features.
- **command-reference**—Reference links to all commands in the running configuration.
- **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

Examples

This example shows a request for analysis of a user-specified show command:

```
Router# call-home request output-analysis "show diagnostic result module all" profile TG
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home send	Sends a CLI command to be executed, with the command output to be sent by e-mail.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send

To execute a CLI command and e-mail the command output, use the **call-home send** command in privileged EXEC mode.

call-home send "*cli-command*" {**email** *email-addr* [**service-number** *SR*] | **service-number** *SR*}

Syntax Description

"cli-command"	Specifies a CLI command to be executed. The command output will be sent by e-mail.
email <i>email-addr</i>	Specifies the e-mail address to which the CLI command output will be sent. If no e-mail address is specified, the command output will be sent to the Cisco TAC at attach@cisco.com.
service-number <i>SR</i>	Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The specified CLI command must be enclosed in quotes (""), and can be any run or show command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output will be sent to the Cisco TAC at attach@cisco.com. The e-mail will be sent in long text format with the service number, if specified, in the subject line.

Examples

This example shows how to send a CLI command and have the command output e-mailed:

```
Router# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

cdp advertise-v2

To enable Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality on a device, use the **cdp advertise-v2** command in global configuration mode. To disable advertising CDPv2 functionality, use the **no** form of the command.

cdp advertise-v2

no cdp advertise-v2

Syntax Description This command has no arguments or keywords.

Command Default Enabled

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines CDP Version 2 has three additional type-length values (TLVs): VTP Management Domain Name, Native VLAN, and full/half-Duplex.

Examples In the following example, CDP Version 2 advertisements are disabled on the router:

```
Router# show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no cdp advertise-v2
Router(config)# end
Router# show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is not enabled
```

Related Commands	Command	Description
	cdp enable	Enables CDP on a supported interface.
	cdp run	Reenables CDP on a Cisco device.

cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled at the global level and on all supported interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.



Note

The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP is disabled on the Ethernet 0 interface only:

```
Router# show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```


Related Commands	Command	Description
	cdp run	Reenables CDP on a Cisco device.
	cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
	router odr	Enables on-demand routing on a hub router.

cdp holdtime

To specify the amount of time the receiving device should hold a Cisco Discovery Protocol (CDP) packet from the router before discarding it, use the **cdp holdtime** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp holdtime *seconds*

no cdp holdtime

Syntax Description	<i>seconds</i>	Specifies the hold time to be sent in the CDP update packets. The default is 180 seconds.
---------------------------	----------------	---

Command Default	180 seconds
------------------------	-------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.3	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.
-------------------------	---

You can set the hold time lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more rapidly.

The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

Examples	In the following example, the CDP packets being sent from the router are configured with a hold time of 60 seconds.
-----------------	---

```
Router(config)# cdp holdtime 60
```

Related Commands	Command	Description
	cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
	show cdp	Displays global CDP information, including timer and hold-time information.

cdp log mismatch duplex

To display the log of duplex mismatches generated by the Cisco Discovery Protocol on Ethernet interfaces, use the **cdp log mismatch duplex** command in global configuration mode or in interface configuration mode. To disable the display of duplex messages, use the **no** form of this command.

cdp log mismatch duplex

no cdp log mismatch duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Duplex mismatches are displayed for all Ethernet interfaces by default.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Duplex mismatches can occur only on Ethernet interfaces.

When you enter the **cdp log mismatch duplex** command in global configuration mode, duplex mismatches are displayed for all Ethernet interfaces on the device. If the command is disabled in global configuration mode, the command cannot be configured in interface configuration mode. When you enter the **cdp log mismatch duplex** command in interface configuration mode, only duplex mismatches for the specified Ethernet interface are displayed.

To enable reporting of duplex mismatches, issue the **cdp log mismatch duplex** command in global configuration mode. If the command was previously disabled under a specified interface, issue the command in interface configuration mode for that interface.

To disable reporting of duplex mismatches globally, issue the **no cdp log mismatch duplex** command in global configuration mode. To disable reporting duplex mismatches for a specified Ethernet interface, use the **no cdp log mismatch duplex** command in interface configuration mode.

Examples

The following example shows how to enable the display of duplex messages from all Ethernet interfaces on a router:

```
Router(config)# cdp log mismatch duplex
```

The following example shows how to enable the display of duplex messages that may be generated from only Ethernet interface 2/1:

```
Router(config)# interface ethernet2/1
Router(config-if)# cdp log mismatch duplex
```

The following is sample output from the **show running-config** command. The bold text in the output shows that the **cdp log mismatch duplex** command is disabled globally.

```
Router# show running-config
```

```
version 12.2
hostname Router
!
interface Ethernet2/0
no ip address
duplex half
interface Ethernet2/1
no ip address
duplex half
!
no cdp log mismatch duplex
!
line con 0
line aux 0
```

The following is sample output from the **show running-config** command. The bold text in the output shows that the **cdp log mismatch duplex** command is disabled under a specific interface.

```
Router# show running-config
```

```
version 12.2
hostname Router
!
interface Ethernet2/0
no ip address
duplex half
no cdp log mismatch duplex
interface Ethernet2/1
no ip address
duplex half
!!
line con 0
line aux 0
line vty 0 4
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp run	Reenables Cisco Discovery Protocol on a Cisco device.

cdp run

To enable Cisco Discovery Protocol, use the **cdp run** command in global configuration mode. To disable Cisco Discovery Protocol, use the **no** form of this command.

cdp run

no cdp run

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on all platforms except the Cisco 10000 Series Edge Services Router

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco Discovery Protocol is enabled by default on all platforms except the Cisco 10000 Series Edge Services Router, which means Cisco IOS software receives Cisco Discovery Protocol information. Cisco Discovery Protocol also is enabled on supported interfaces by default. To disable Cisco Discovery Protocol on an interface, use the **no cdp enable** command in interface configuration mode.

The **show running-config** command lists **no cdp run** when Cisco Discovery Protocol is disabled globally, which is not the default behavior. As a result of changes made for the Cisco 10000 platform, **show running-config** will list **cdp run** when Cisco Discovery Protocol is enabled globally.



Note

Because on-demand routing (ODR) uses Cisco Discovery Protocol, the **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the **router odr** global configuration command. For more information about the **router odr** command, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, Cisco Discovery Protocol is disabled globally, then the user attempts to enable it on the Ethernet 0 interface:

```
Router(config)# no cdp run
Router(config)# end
Router# show cdp
```

```
% CDP is not enabled
```

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# interface ethernet0
```

```
Router(config-if)# cdp enable
```

```
% Cannot enable CDP on this interface, since CDP is not running
```

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

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp holdtime	Specifies the amount of time a receiving device should hold a Cisco Discovery Protocol packet before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends Cisco Discovery Protocol updates.
router odr	Enables ODR on the hub router.

cdp source-interface

To configure the Cisco Discovery Protocol source interface, use the **cdp source-interface** command in global configuration mode.

cdp source-interface *type number*

no cdp source-interface

Syntax Description

<i>type</i>	Type of interface to be configured.
<i>number</i>	Port, connector, or interface card number. These numbers were assigned at the time of installation or when added to a system, and can be displayed with the show interfaces command.

Defaults

No Cisco Discovery Protocol source-interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use of this command ensures that Cisco Discovery Protocol packets use the IP address that has been previously assigned to an interface. Without this command, Cisco Discovery Protocol uses the IP address of the first available interface.

The conditions that an interface should satisfy to be the source interface are as follows:

- It should have an IP address.
- Its status should be UP.
- It should not be an IP unnumbered interface.

When Cisco Discovery Protocol is enabled and the Cisco Discovery Protocol source interface has not been configured, then Cisco Discovery Protocol uses the IP address of the first available interface.

Examples

The following example configures Cisco Discovery Protocol to use the IP address that has been assigned to interface loopback 1.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cdp source-interface loopback 1
```

```
Router(config)# exit  
Router#
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol on a supported interface.
cdp run	Reenables Cisco Discovery Protocol on a Cisco device.

cdp timer

To specify how often the Cisco IOS software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

no cdp timer

Syntax Description

<i>seconds</i>	Integer that specifies how often, in seconds, the Cisco IOS software sends CDP updates. The default is 60 seconds.
----------------	--

Command Default

The default setting is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The trade-off with sending more frequent CDP updates to provide up-to-date information, is that bandwidth is used more often.



Note

The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP updates are sent every 80 seconds, less frequently than the default setting of 60 seconds. You might want to make this change if you are concerned about preserving bandwidth.

```
cdp timer 80
```

Related Commands	Command	Description
	cdp enable	Enables CDP on a supported interface.
	cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
	cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
	router odr	Enables ODR on the hub router.
	show cdp	Displays global CDP information, including timer and hold-time information.

cdp tlv

To configure location support in Cisco Discovery Protocol (CDP), use the **cdp tlv** command in global configuration mode or interface configuration mode. To disable the location support configuration, use the **no** form of this command.

Command Syntax in Global Configuration Mode

cdp tlv { **app** | **location** | **location-server** }

no cdp tlv { **app** | **location** | **location-server** }

Command Syntax in Interface Configuration Mode

cdp tlv { **app** [*tlvtype tlvtype value value*] | **location** | **location-server** }

no cdp tlv { **app** [*tlvtype tlvtype value value*] | **location** | **location-server** }

Syntax Description

app	Enables application Type-Length-Values (TLVs).
location	Enables location TLVs on CDP messages.
location-server	Enables location-server TLVs on CDP messages.
tlvtype <i>tlvtype</i>	(Optional) Configures application TLV type information. The range is from 1001 to 65535.
value <i>value</i>	Configures application TLV value information.

Command Default

Application TLVs, location TLVs, and location-server TLVs in CDP are enabled.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.2(55)SE	This command was introduced.

Usage Guidelines

To enable location-based services, information on the exact location of endpoint devices in the network is very essential. The information on the location of endpoint devices is delivered through Cisco devices using the CDP mechanism. To enable location support at the global level, use the **cdp tlv** command in global configuration mode. To enable location support on interfaces, use the **cdp tlv** command in interface configuration mode. If application TLVs are enabled on all interfaces, the TLVs are sent on all interfaces. Location TLVs in CDP are enabled by default. You can disable the storage of location TLVs by using the **no cdp tlv location** command. When you use the **cdp tlv location** command in global configuration mode, CDP starts sending periodic location information when the location TLV is enabled and the location information is available. When you use the **cdp tlv location** command in interface configuration mode, TLVs are sent along with the CDP messages periodically.

Examples

The following example shows how to configure location support for application TLVs in CDP at the global level:

```
Router(config)# cdp tlv app
```

The following example shows how to configure location support for application TLVs in CDP at an interface level:

```
Router(config)# interface fastethernet 0
Router(config-if)# cdp tlv app tlvtype 1002 value loc1
```

Related Commands

Command	Description
<code>show cdp tlv</code>	Displays information about CDP TLVs.

clear cdp counters

To reset Cisco Discovery Protocol (CDP) traffic counters to zero, use the **clear cdp counters** command in privileged EXEC mode.

clear cdp counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the CDP counters. The **show cdp traffic** output shows that all of the traffic counters have been reset to zero.

```
Router# clear cdp counters
```

```
Router# show cdp traffic
```

CDP counters:

Packets output: 0, Input: 0

Hdr syntax: 0, Chksum error: 0, Encaps failed: 0

No memory: 0, Invalid packet: 0, Fragmented: 0

Related Commands

Command	Description
clear cdp table	Clears the table that contains CDP information about neighbors.
show cdp traffic	Displays traffic information from the CDP table.

clear cdp table

To clear the table that contains Cisco Discovery Protocol (CDP) information about neighbors, use the **clear cdp table** command in privileged EXEC mode.

clear cdp table

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following example clears the CDP table. The output of the **show cdp neighbors** command shows that all information has been deleted from the table.

```
Router# clear cdp table
```

```
CDP-AD: Deleted table entry for neon.cisco.com, interface Ethernet0
```

```
CDP-AD: Deleted table entry for neon.cisco.com, interface Serial0
```

```
Router# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP
```

```
Device ID      Local Intrfce    Holdtme    Capability  Platform  Port ID
```

Related Commands	Command	Description
	show cdp neighbors	Displays information about neighbors.

clear cns config stats

To clear the statistics about the Cisco Networking Services (CNS) configuration agent, use the **clear cns config stats** command in privileged EXEC mode.

clear cns config stats

Syntax Description This command has no arguments or keywords.

Defaults No statistics are cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines The **clear cns config stats** command clears all the statistics displayed by the **show cns config stats** command.

Examples The following example shows how to clear all of the statistics for the CNS configuration agent:

```
Router# clear cns config stats
```

Related Commands	Command	Description
	show cns config stats	Displays statistics about the CNS configuration agent.

clear cns counters

To clear all Cisco Networking Services (CNS) statistics, use the **clear cns counters** command in privileged EXEC mode.

clear cns counters

Syntax Description This command has no arguments or keywords.

Defaults No statistics are cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines The **clear cns counters** command clears all the statistics tracked and displayed by CNS agents.

Examples The following example shows how to clear all of the statistics used by CNS:

```
Router# clear cns counters
```

Related Commands	Command	Description
	show cns config stats	Displays statistics about the CNS configuration agent.
	show cns event stats	Displays statistics about the CNS event agent.
	show cns image stats	Displays statistics about the CNS image agent.

clear cns event stats

To clear the statistics about the Cisco Networking Services (CNS) event agent, use the **clear cns event stats** command in privileged EXEC mode.

clear cns event stats

Syntax Description This command has no arguments or keywords.

Defaults No statistics are cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines The **clear cns event stats** command clears all the statistics displayed by the **show cns event stats** command.

Examples The following example shows how to clear all of the statistics for the CNS event agent:

```
Router# clear cns event stats
```

Related Commands	Command	Description
	show cns event stats	Displays statistics about the CNS event agent.

clear cns image connections

To clear the Cisco Networking Services (CNS) image agent connections statistics, use the **clear cns image connections** command in privileged EXEC mode.

clear cns image connections

Syntax Description This command has no arguments or keywords.

Command Default No statistics are cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines The **clear cns image connections** command clears all the statistics displayed by the **show cns image connections** command.

Examples The following example shows how to clear all of the connection statistics for the CNS image agent:

```
Router# clear cns image connections
```

Related Commands	Command	Description
	show cns image connections	Displays connection information for the CNS image agent.

clear cns image status

To clear the Cisco Networking Services (CNS) image agent status statistics, use the **clear cns image status** command in privileged EXEC mode.

clear cns image status

Syntax Description This command has no arguments or keywords.

Command Default No statistics are cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines The **clear cns image status** command clears all the statistics displayed by the **show cns image status** command.

Examples The following example shows how to clear all the status statistics for the CNS image agent:

```
Router# clear cns image status
```

Related Commands	Command	Description
	show cns image status	Displays status information for the CNS image agent.

clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** command in privileged EXEC mode.

clear ip drp

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following example clears all DRP statistics:

```
Router# clear ip drp
```

Related Commands	Command	Description
	ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
	ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.

clear ip http client cookie

To remove the HTTP client cookies, use the **clear ip http client cookie** command in privileged EXEC mode.

```
clear ip http client cookie [domain cookie-domain | name cookie-name | session session-name]
```

Syntax Description	domain	(Optional) Specifies all cookies in a domain.
	<i>cookie-domain</i>	(Optional) Client cookie domain or hostname.
	name	(Optional) Specifies cookies matching a specific name.
	<i>cookie-name</i>	(Optional) Client cookie name.
	session	(Optional) Specifies cookies specific to a client session.
	<i>session-name</i>	(Optional) Client session name.

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	12.4(20)T	This command was introduced.

Examples	The following example shows how to remove the HTTP client cookie named test: <pre>Device# clear ip http client cookie name test</pre>
----------	--

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.
	<i>filesystem:</i>	The file system followed by a colon.
	<i>/directory</i>	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 <i>filesystem:/directory</i> argument and keyword 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-persistent
```

```
Delete persistent logging files from harddisk:/log-persistent ? [confirm]
```

```
Router# dir harddisk:/log-persistent
```

```
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 onboard (Cat 6K)

To clear the onboard failure logs (OBFL) on Cisco Catalyst 6000 series switches, use the **clear logging onboard** command in privileged EXEC mode.

clear logging onboard [**module** *module-number*]

Syntax Description

module *module-number* (Optional) Specifies a particular module.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to clear all OBFL logs or only the logs in the module specified by the **module** *module-number* option.



Note

Use this command with care: Important data could be lost when the logs are cleared. Make sure the logs have been transferred to a file before using this command.

Examples

The following example shows how to clear the logs from module 2:

```
Router# clear logging onboard module 2
```

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing commands on that card.
copy logging onboard module (Cat 6K)	Copies OBFL data from the target OBFL-enabled module to a local or remote file system.
[no] hw-module logging onboard (Cat 6K)	Disables and enables OBFL.
show logging onboard (Cat 6K)	Displays onboard failure logs.

clear netconf

To clear network configuration protocol (NETCONF) statistics counters or NETCONF sessions and to free associated resources and locks, use the **clear netconf** command in privileged EXEC mode.

clear netconf {counters | sessions}

Syntax Description

counters	Clears the NETCONF statistics counters to zero.
sessions	Clears currently connected NETCONF sessions.

Command Default

NETCONF statistics counters are incremented and configured NETCONF sessions remain active.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to clear NETCONF statistics counters to zero, to clear all or specified NETCONF sessions and to disconnect and free associated resources and locks.

Examples

The following example shows how to clear all NETCONF counters:

```
Router# clear netconf counters
```

Related Commands

Command	Description
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

clear platform hardware capacity rewrite-engine counter

To clear the packet drop and performance counters of the central rewrite engine on supervisors and line cards, use the **clear platform hardware capacity rewrite-engine counter** command in privileged EXEC mode.

clear platform hardware capacity rewrite-engine counter [*slot number*]

Syntax Description

slot number	Clears the packet drop and performance counters on the module in the specified slot. If no slot is specified, the counters are cleared on all slots.
--------------------	--

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Examples

This example shows how to clear the packet drop and performance counters for the module in slot 6:

```
Router# clear platform hardware capacity rewrite-engine counter slot 6
Router#
```

Related Commands

Command	Description
show platform hardware capacity rewrite-engine	Displays the packet drop and performance counters of the central rewrite engine on supervisors and line cards.

clear wsma agent

To clear the required Web Services Management Agents (WSMAs), use the **clear wsma agent** command in privileged EXEC mode.

clear wsma agent [**config** | **exec** | **filesys** | **notify**] **counters**

Syntax Description

config	(Optional) Clears the counters for a config agent.
exec	(Optional) Clears the counters for an exec agent.
filesys	(Optional) Clears the counters for a filesys agent.
notify	(Optional) Clears the counters for a notify agent.
counters	Clears counters for the agents specified. If no filters are specified, counters for all the agents are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example shows how to clear a WSMA:

```
Router# clear wsma agent filesys counters
Router#
```

Related Commands

Command	Description
clear wsma profile	Clears the requires WSMA profiles.

clear wsma profile

To clear the configured Web Services Management Agent (WSMA) profiles, use the **clear wsma profile** command in privileged EXEC mode.

clear wsma profile [*name name*] {**connections** | **counters**}

Syntax Description

name <i>name</i>	(Optional) Defines the name of the profile to be cleared. If a profile name is not specified, all the WSMA profiles are cleared.
connections	Closes all the data connections for the listener and initiator profiles.
counters	Clears all the counters for the listener and initiator profiles.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for WSMA initiator configuration mode.

Examples

The following example shows how to clear the profile counters for the WSMA profile prof1:

```
Router# clear wsma profile name prof1 counters
```

Related Commands

Command	Description
clear wsma agent	Clears the required WSMA.

clear xsm

To clear XML Subscription Manager (XSM) client sessions, use the **clear xsm** command in privileged EXEC mode.

clear xsm [*session number*]

Syntax Description

session	(Optional) Specifies an XSM client session to clear.
number	(Optional) ID number of the specific XSM client session to be cleared.

Command Default

No XSM client sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command disconnects all active client sessions (such as with a VPN Device Manager [VDM]) on the XSM server, unless you state a specific session number. This command allows troubleshooting of the XSM server and its active clients by allowing individual clients to be disconnected. Use the **show xsm status** command to obtain specific session numbers.

When the optional **session number** keyword and argument are not used, the **clear xsm** command clears all XSM client sessions.

Examples

The following example shows how to clear all XSM client sessions:

```
Router# clear xsm
```

The following example shows how to clear XSM client session 10:

```
Router# clear xsm session 10
```

Related Commands

Command	Description
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

cli

To specify EXEC command-line interface (CLI) commands within a Command Scheduler policy list, use the **cli** command in kron-policy configuration mode. To delete a CLI command from the current policy list, use the **no** form of this command.

cli *command*

no cli *command*

Syntax Description

<i>command</i>	EXEC-mode CLI command that must not generate a prompt or allow interruption by a keystroke.
----------------	---

Command Default

No CLI commands are specified.

Command Modes

Kron-policy configuration (config-kron-policy)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **cli** command in conjunction with the **kron policy-list** command to create a policy list containing EXEC CLI commands to be scheduled to run on the router at a specified time. Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

The Command Scheduler process is useful to automate the running of EXEC commands at recurring intervals, and it can be used in remote routers to minimize manual intervention.

Examples

The following example shows how to configure the EXEC command **cns image retrieve** within the policy list named three-day-list:

```
Router(config)# kron policy-list three-day-list
Router(config-kron-policy)# cli cns image retrieve server https://10.19.2.3/cns/image/
status https://10.19.2.3/cnsstatus/imageinfo/
```

Related Commands

Command	Description
kron occurrence	Specifies schedule parameters for a Command Scheduler occurrence and enters kron-occurrence configuration mode.

Command	Description
kron policy-list	Specifies a name for a Command Scheduler policy and enters kron-policy configuration mode.
policy-list	Specifies the policy list associated with a Command Scheduler occurrence.

cli (cns)

To specify the command lines of a Cisco Networking Services (CNS) connect template, use the **cli** command in CNS template connect configuration mode. To disable this configuration, use the **no** form of this command.

cli *config-text*

no cli *config-text*

Syntax Description

<i>config-text</i>	Command line to be included in a CNS connect template.
--------------------	--

Command Default

No command lines are specified in the CNS connect template.

Command Modes

CNS template connect configuration

Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9). The CNS connect variable \${dlci} is not supported in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

First use the **cns template connect** command to enter CNS template connect configuration mode and define the name of the CNS connect template to be configured. Then use the **cli** command to specify the command lines of the CNS connect template.



Note

Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), and 12.2(33)SRA the **config-cli** and **line-cli** commands are replaced by the **cli (cns)** command.

The command lines specified using the **cli** command can include CNS connect variables (see [Table 22](#)). These variables act as placeholders within the command lines of a CNS connect template. Each variable is defined by an associated **discover** command. Before a CNS connect template that contains these variables is applied to a router's configuration, the variables are replaced by the values defined by their associated **discover** command. For example, if the **discover interface serial** command was configured, and you were able to connect to the CNS configuration engine using Serial0/0, then the **cli ip route 0.0.0.0 0.0.0.0 \${interface}** command would generate the **cli ip route 0.0.0.0 0.0.0.0 serial0/0** command.

**Note**

When creating a CNS connect template, you must enter the **exit** command to complete the configuration of the template and exit from CNS template connect configuration mode. This requirement was implemented to prevent accidentally entering a command without the **cli** command.

Table 22 **Summary of the CNS Connect Variables**

Variable	Description
\${line}	The line type defined by the associated discover line <i>line-type</i> command.
\${controller}	The controller type defined by the associated discover controller <i>controller-type</i> command.
\${interface}	The interface type defined by the associated discover interface command.
\${dlci}	The active DLCI defined by the associated discover dlci command.
\${next-hop}	The next hop interface. This variable is identical to the \${interface} variable unless the discover dlci command has been configured. In this case, the \${next-hop} variable is identical to the \${interface}.\${subinterface} variable, where the {subinterface} variable is specified by the discover dlci command. The \${next-hop} variable should only be used in the CNS connect templates after the last discover command has been entered. A typical use of this variable is to allow the default IP route to be configured to send traffic towards the CNS configuration engine. Note that the CNS configuration engine may not be on the same LAN as the router. Therefore, configuring a route to the CNS configuration engine may require deployment-specific knowledge. Common practice is to define a default route to the interface using the ip route command (for example, cli ip route 0.0.0.0 0.0.0.0 \${next-hop}).
\$\$	A literal substitution of the \$ symbol.

**Note**

Effective with Cisco IOS Releases 12.3(8)T and 12.3(9), the **&** variable is replaced by the **\${interface}** variable.

Examples

The following example shows how to configure a CNS connect template named template1:

```
Router(config)# cns template connect template-1
Router(config-templ-conn)# cli command-1
Router(config-templ-conn)# cli command-2
Router(config-templ-conn)# cli no command-3
Router(config-templ-conn)# exit
Router(config)#
```

When the template1 template is applied, the following commands are sent to the router's parser:

```
command-1
command-2
no command-3
```

When the template1 template is removed from the router's configuration after an unsuccessful ping attempt to the CNS configuration engine, the following commands are sent to the router's parser:

```
no command-1
no command-2
command-3
```

Related Commands

Command	Description
cns connect	Enters CNS connect configuration mode and defines the parameters of a CNS connect profile for connecting to the CNS configuration engine.
cns template connect	Enters CNS template connect configuration mode and defines the name of a CNS connect template.
discover (cns)	Defines the interface parameters within a CNS connect profile for connecting to the CNS configuration engine.
template (cns)	Specifies a list of CNS connect templates within a CNS connect profile to be applied to a router's configuration.

clock calendar-valid

To configure a system as an authoritative time source for a network based on its hardware clock (calendar), use the **clock calendar-valid** command in global configuration mode. To specify that the hardware clock is not an authoritative time source, use the **no** form of this command.

clock calendar-valid

no clock calendar-valid

Syntax Description This command has no arguments or keywords.

Defaults The router is not configured as a time source.

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.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. If no outside time source is available on your network, use this command to make the hardware clock an authoritative time source.

Because the hardware clock is not as accurate as other time sources, you should configure this command only when a more accurate time source (such as NTP) is not available.

Examples The following example configures a router as the time source for a network based on its hardware clock:

```
Router(config)# clock calendar-valid
```

Related Commands	Command	Description
	ntp master	Configures the Cisco IOS software as an NTP master clock to which peers synchronize themselves when an external NTP source is not available.
	vines time use-system	Sets VINES network time based on the system time.

clock read-calendar

To manually read the hardware clock (calendar) settings into the software clock, use the **clock read-calendar** command in EXEC mode.

clock read-calendar

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. When the router is rebooted, the hardware clock is automatically read into the software clock. However, you may use this command to manually read the hardware clock setting into the software clock. This command is useful if the **calendar set** command has been used to change the setting of the hardware clock.

Examples The following example configures the software clock to set its date and time by the hardware clock setting:

```
Router> clock read-calendar
```

Related Commands	Command	Description
	calendar set	Sets the hardware clock.
	clock set	Manually sets the software clock.
	clock update-calendar	Performs a one-time update of the hardware clock from the software clock.
	ntp update-calendar	Periodically updates the hardware clock from the software clock.

clock save interval

To preserve recent date and time information in NVRAM for when a Cisco IOS device without a battery-backed calendar is power-cycled or reloaded, use the **clock save interval** command in global configuration mode. To return to the default disabled state, use the **no** form of this command.

clock save interval *hours*

no clock save interval *hours*

Syntax Description	<i>hours</i>	Interval at which the time will be stored in NVRAM. Accepted intervals range from 8 to 24 hours.
---------------------------	--------------	--

Defaults	This function is disabled by default.
-----------------	---------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.3(2)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines	The benefit of using this command is that upon returning from a system reload or power cycle, the system clock will be set to a time and date near the current time and date instead of being reset to the system default time and date. In the absence of better information, Cisco IOS devices will initially set their system clocks to <i>epoch start</i> , which will typically be midnight (UTC) March 1, 1993 or 2002.
-------------------------	---

When this command is entered, the date and time are saved to NVRAM at the interval specified by this command, and also during any shutdown process. When the system starts up, the system clock is set to the last time and date saved to NVRAM.

All Cisco IOS devices support Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to learn the time from the network, and some Cisco IOS devices have built-in battery-backed clocks to maintain that time. The **clock save interval** command is for those Cisco IOS devices that do not have battery-backed clocks and need to know the time and date before they can start communicating with a network. Because the March 1 system default date will likely occur before the valid date of any recently issued certificate, communications attempted with almost any certificate will fail because it is not yet valid according to the local clock.

Saving the time at a 24-hour interval should work well for most networks, unless there is a certificate that maintains a shorter life span.

Being aware of the time and date is critical for networking devices, and it becomes an issue when communication to a network requires use of a time-based credential, such as a certificate that has start and end dates and times. NTP and SNTP are the proper ways to set the time of a network device. The **clock save interval** command is intended to complement use of NTP and SNTP, so this command is useful only when a certificate is required to initiate communication to an NTP server, and the Cisco IOS device does not have a battery-back hardware clock, but does have NVRAM.

The system time will only be saved to NVRAM when set by an authoritative source such as NTP or SNTP; the system will not save the time entered through the **set clock** command. Additionally, a clock is considered valid only when the following criteria apply:

- The clock was set by the user using the **set clock** command and declared authoritative by the **clock calendar-valid** command.
- The clock time was learned through NTP or SNTP.

Through a confluence of events, there is no means to authoritatively declare a user-entered time as valid unless the calendar (battery-backed date and time) is declared valid. Since there is no actual calendar in a system with this command, the **clock calendar-valid** command is unavailable, and therefore a user-entered time can never be considered authoritative on platforms without a battery-backed calendar. This state is intentional because a battery-backed clock continues to run, and an NVRAM clock will stay the same. And again, for these reasons the **clock save interval** command must complement the use of NTP and SNTP.

Examples

The following example shows how to configure a Cisco IOS device to save the time at 24-hour intervals:

```
Router(config)# clock save interval 24
```

clock set

To manually set the system software clock, use one of the following formats of the **clock set** command in privileged EXEC mode.

clock set *hh:mm:ss day month year*

clock set *hh:mm:ss month day year*

Syntax Description

<i>hh:mm:ss</i>	Current time in hours (24-hour format), minutes, and seconds.
<i>day</i>	Current day (by date) in the month.
<i>month</i>	Current month (by name).
<i>year</i>	Current year (no abbreviation).

Command Modes

Privileged EXEC mode

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) or VINES clock source, or if you have a router with a hardware clock, you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command.

Examples

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

```
Router# clock set 19:29:00 13 May 2003
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.

clock summer-time

To configure the system to automatically switch to summer time (daylight saving time), use one of the formats of the **clock summer-time** command in global configuration mode. To configure the Cisco IOS software not to automatically switch to summer time, use the **no** form of this command.

clock summer-time *zone* {**date** *start-date start-month start-year hh:mm end-date end-month end-year hh:mm [offset]* | **recurring** [*week* | **first** | **last**] *start-date start-month hh:mm {end-week | first | last} end-day end-month hh:mm [offset]*}

no clock summer-time

Syntax Description

<i>zone</i>	Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the <i>zone</i> argument is limited to seven characters.
date	Configures summer time based on the date.
<i>start-date</i>	Start day of the week (Sunday, Monday, and so on).
<i>start-month</i>	Start month of the year.
<i>start-year</i>	Start year.
<i>hh:mm</i>	(Optional) Time (military format) in hours and minutes. The colon is required.
<i>end-date</i>	End date of the month (1 to 31).
<i>end-month</i>	(Optional) End month (January, February, and so on) of the year.
<i>end-year</i>	End year (1993 to 2035).
<i>offset</i>	(Optional) Number of minutes to add during summer time (default is 60). The range is 1 to 1440.
recurring	Configures a recurring start and end of summer time.
<i>week</i>	(Optional) Week of the month (1 to 4). Use first to specify the first week and last to specify the last week
first	(Optional) Specifies the first week of the month
last	(Optional) Specifies the last week of the month
<i>end-day</i>	(Optional) End day of the week (Sunday, Monday, and so on).

Command Default

Summer time is disabled. If the **clock summer-time zone recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the *offset* argument is 60.

Command Modes

Global configuration (config)

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.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The first and last keywords were added.

Usage Guidelines

Use this command if you want to automatically switch to summer time (for display purposes only). Use the **recurring** form of the command if the local summer time rules are of this form. Use the **date** keyword to specify a start and end date for summer time if you cannot use the **recurring** keyword.

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

Examples

The following example specifies that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.:

```
Router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

If you live in a place where summer time does not follow the pattern in the first example, you can specify the exact date and times. In the following example, daylight saving time (summer time) is configured to start on October 12, 1997 at 2 a.m., and end on April 26, 1998 at 2 a.m.:

```
Router(config)# clock summer-time PDT date 12 October 1997 2:00 26 April 1998 2:00
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock timezone	Sets the time zone for display purposes.

clock timezone

To set the time zone for display purposes, use the **clock timezone** command in global configuration mode. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command.

clock timezone *zone* *hours-offset* [*minutes-offset*]

no clock timezone

Syntax Description	<i>zone</i>	Name of the time zone to be displayed when standard time is in effect. The length of the <i>zone</i> argument is limited to 7 characters.
	<i>hours-offset</i>	Hours difference from UTC.
	<i>minutes-offset</i>	(Optional) Minutes difference from UTC.

Defaults UTC

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.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

[Table 23](#) lists common time zone acronyms used for the *zone* argument.

Table 23 Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	
GMT	Greenwich Mean Time, as UTC
BST	British Summer Time, as UTC + 1 hour
IST	Irish Summer Time, as UTC + 1 hour
WET	Western Europe Time, as UTC
WEST	Western Europe Summer Time, as UTC + 1 hour
CET	Central Europe Time, as UTC + 1
CEST	Central Europe Summer Time, as UTC + 2

Table 23 Common Time Zone Acronyms (continued)

Acronym	Time Zone Name and UTC Offset
EET	Eastern Europe Time, as UTC + 2
EEST	Eastern Europe Summer Time, as UTC + 3
MSK	Moscow Time, as UTC + 3
MSD	Moscow Summer Time, as UTC + 4
United States and Canada	
AST	Atlantic Standard Time, as UTC –4 hours
ADT	Atlantic Daylight Time, as UTC –3 hours
ET	Eastern Time, either as EST or EDT, depending on place and time of year
EST	Eastern Standard Time, as UTC –5 hours
EDT	Eastern Daylight Saving Time, as UTC –4 hours
CT	Central Time, either as CST or CDT, depending on place and time of year
CST	Central Standard Time, as UTC –6 hours
CDT	Central Daylight Saving Time, as UTC –5 hours
MT	Mountain Time, either as MST or MDT, depending on place and time of year
MST	Mountain Standard Time, as UTC –7 hours
MDT	Mountain Daylight Saving Time, as UTC –6 hours
PT	Pacific Time, either as PST or PDT, depending on place and time of year
PST	Pacific Standard Time, as UTC –8 hours
PDT	Pacific Daylight Saving Time, as UTC –7 hours
AKST	Alaska Standard Time, as UTC –9 hours
AKDT	Alaska Standard Daylight Saving Time, as UTC –8 hours
HST	Hawaiian Standard Time, as UTC –10 hours
Australia	
WST	Western Standard Time, as UTC + 8 hours
CST	Central Standard Time, as UTC + 9.5 hours
EST	Eastern Standard/Summer Time, as UTC + 10 hours (+11 hours during summer time)

Table 24 lists an alternative method for referring to time zones, in which single letters are used to refer to the time zone difference from UTC. Using this method, the letter Z is used to indicate the zero meridian, equivalent to UTC, and the letter J (Juliet) is used to refer to the local time zone. Using this method, the International Date Line is between time zones M and Y.

Table 24 *Single-Letter Time Zone Designators*

Letter Designator	Word Designator	Difference from UTC
Y	Yankee	UTC -12 hours
X	Xray	UTC -11 hours
W	Whiskey	UTC -10 hours
V	Victor	UTC -9 hours
U	Uniform	UTC -8 hours
T	Tango	UTC -7 hours
S	Sierra	UTC -6 hours
R	Romeo	UTC -5 hours
Q	Quebec	UTC -4 hours
P	Papa	UTC -3 hours
O	Oscar	UTC -2 hours
N	November	UTC -1 hour
Z	Zulu	Same as UTC
A	Alpha	UTC +1 hour
B	Bravo	UTC +2 hours
C	Charlie	UTC +3 hours
D	Delta	UTC +4 hours
E	Echo	UTC +5 hours
F	Foxtrot	UTC +6 hours
G	Golf	UTC +7 hours
H	Hotel	UTC +8 hours
I	India	UTC +9 hours
K	Kilo	UTC +10 hours
L	Lima	UTC +11 hours
M	Mike	UTC +12 hours

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Router(config)# clock timezone PST -8
```

The following example sets the time zone to Atlantic Time (AT) for Newfoundland, Canada, which is 3.5 hours behind UTC:

```
Router(config)# clock timezone AT -3 30
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually set the software clock.

Command	Description
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
show clock	Displays the software clock.

clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the **clock update-calendar** command in user EXEC or privileged EXEC mode.

clock update-calendar

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
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.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines Some platforms have a hardware clock (calendar) in addition to a software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use this command to update the hardware clock to the correct date and time.

Examples The following example copies the current date and time from the software clock to the hardware clock:

```
Router> clock update-calendar
```

Related Commands	Command	Description
	clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
	ntp update-calendar	Periodically updates the hardware clock from the software clock.