N through T Commands

ntp access-group

To control access to Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group [**ipv4**| **ipv6**] {**peer**| **query-only**| **serve**| **serve-only**} {*access-list-number*| *access-list-number-expanded*| *access-list-name*} [**kod**]

no ntp access-group [**ipv4**| **ipv6**] {**peer**| **query-only**| **serve**| **serve-only**}

Syntax Description

ipv4	(Optional) Configures IPv4 access lists.
ipv6	(Optional) Configures IPv6 access lists.
peer	Allows time requests and NTP control queries and permits the system to synchronize with the remote system.
query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize with the remote system.
serve-only	Allows only time requests. **Note** You must configure the **ntp server** *ip-address* command before using the **serve-only** keyword.
access-list-number	Number (from 1 to 99) of a standard IPv4 or IPv6 access list.
access-list-number-expanded	Number (from 1300 to 1999) of an expanded range IPv4 or IPv6 access list.
access-list-name	Name of an access list.
kod	(Optional) Sends the “Kiss-of-Death” (KOD) packet to any host that tries to send a packet that is not compliant with the access-group policy.

Command Default

By default, there is no access control. Full access is granted to all systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.4(15)T	This command was modified in a release earlier than Cisco IOS Release 12.4(15)T. The *access-list-number-expanded* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 access list was added.
Cisco IOS XE Release 3.5S	This command was modified. The **ipv4** and **ipv6** keywords were added.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

The access group options are scanned in the following order from the least restrictive to the most restrictive:

1. **peer**
2. **query-only**
3. **serve**
4. **serve-only**

Access is granted for the first match that is found. If no access groups are specified, comprehensive access is granted to all sources. If you specify any access groups, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. For tighter security, use the NTP authentication facility.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp access-group** command, the NTP service is activated (if it has not already been activated) and access control to NTP services is configured simultaneously.

When you enter the **no ntp access-group** command, only the access control to NTP services is removed. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove the access control to NTP services, and all NTP functions from the device, use the **no ntp** command without any keywords.

If you do not specify the **ipv4** or **ipv6** keyword, the IPv4 access list is configured by default. In Cisco IOS XE Release 3.5S and later releases, the **show running-config** command displays only the last configured **ntp access-group** command configured on the router. However, in releases prior to Cisco IOS XE Release 3.5S, the **show running-config** command displays all **ntp access-group** commands configured on the router. For example, in Cisco IOS XE Release 3.5S and later releases, if you first configure the **ntp access-group serve 1** command and then configure the **ntp access-group serve 2** command on the router, the output of the **show running-config** displays only the **ntp access-group serve 1** command, shown below:

```
Router# configure terminal
Router(config)# ntp access-group serve 2
Router(config)# ntp access-group serve 1
Router(config)# exit
Router# show running-config | include ntp access-group
ntp access-group serve 1
Router#
```

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

In the following IPv6 example, a KOD packet is sent to any host that tries to send a packet that is not compliant with the access-group policy:

```
Router(config)# ntp access-group serve acl1 kod
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
ntp server	Allows the software clock to be synchronized by a time server.

ntp allow mode private

Note Effective with Cisco IOS Release 12.2(33)SXJ, the **ntp allow mode private** command is not available in Cisco IOS software.

To allow the processing of private mode Network Time Protocol (NTP) packets, use the **ntp allow mode private** command in global configuration mode. To disable the processing of private mode NTP packets, use the **no** form of this command.

ntp allow mode private

no ntp allow mode private

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the private mode NTP packets are not processed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH7	This command was introduced.
12.2(33)SXJ	This command was removed.

Usage Guidelines

The private mode NTP packets will be blocked if this command is not enabled. If you are using NTP version 4 (NTPv4), you need not configure this command. NTP private mode packet processing is enabled by default in NTPv4.

Examples

The following example shows how to enable the processing of private mode NTP packets:

```
Router(config)# ntp allow mode private
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in the global configuration mode. To disable NTP authentication, use the **no** form of this command.

ntp authenticate

no ntp [authenticate]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, NTP authentication is not enabled.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use this command to prevent the system from synchronizing with unauthenticated and unconfigured network peers. This command ensures authentication of packets that are automatically create new temporary, symmetric, broadcast or multicast associations with remote network hosts. If this command is used, when a packet is received from a symmetric, broadcast or multicast association, the system will synchronize with the corresponding peer by checking if the packet carries one of the authentication keys specified in the **ntp trusted-key** list. Use the **ntp trusted-key** command to get the list of authentication keys.

You must enable **ntp authenticate** when enabling the **ntp passive**, **ntp broadcast client**, or **ntp multicast client** commands unless you have other measures (such as using the **ntp access-group** command) to prevent unauthenticated network attackers from communicating with the device's NTP daemon.

Use the **no ntp authenticate** command to allow synchronizing with unauthenticated and unconfigured network peers

The **ntp authenticate** command does not ensure authentication of peer associations that are created using the **ntp server** and the **ntp peer** commands. When creating associations using the **ntp server** and the **ntp peer** commands, the **key** option for the respective commands must be used to ensure the authentication of packets that move to and from the remote peer.

The NTP service can be activated by using any **ntp** command. Hence, when you use the **ntp authenticate** command, the NTP service is activated (if it was not already activated) and NTP authentication is enabled simultaneously.

Keywords are optional when you use the **no** form of any **ntp** command. When you enter the **no ntp authenticate** command, the NTP authentication is removed from the NTP service, which remains active with additional functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in the global configuration mode. For example, if you previously issued the **ntp authenticate** command and you now want to disable not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems that provide the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp access-group	Controls access to NTP services on the system.
ntp authentication-key	Defines an authentication key for NTP.
ntp broadcast client	Configures a device to receive NTP broadcast messages on a specified interface.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.
ntp passive	Configures passive NTP associations.
ntp server	Configures a device to allow its software clock to be synchronized with the software clock of a NTP time server.

Command	Description
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *key* [*encryption-type*]

no ntp [**authentication-key** *number*]

Syntax Description

number	Key number from 1 to 4294967295.
md5	Specifies the authentication key. Message authentication support is provided using the message digest 5 (MD5) algorithm. The key type **md5** is the only key type supported.
key	Character string of up to 32 characters that is the value of the MD5 key. **Note** In auto secure mode, an error is displayed on the console and the authentication key is not configured if the character string length exceeds 32.
encryption-type	(Optional) Authentication key encryption type. Range: 0 to 4294967295.

Command Default

No authentication key is defined for NTP.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.

Release	Modification
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed in the configuration.

When you configure the authentication key using the **ntp authentication-key** command or using the **auto secure ntp** command, if the length of the MD5 key exceeds 32 characters, an error message is displayed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authentication-key**command, the NTP service is activated (if it has not already been activated) and the NTP authentication key is defined simultaneously.

When you enter the **no ntp authentication-key**command, only the NTP authentication key is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

Note If a specific authentication key configuration is removed, the NTP process is not stopped until all the authentication key configurations are removed.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

The following example shows the error message displayed when the authentication key character string length exceeds 32:

```
Router(config)# ntp authentication-key 23 md5 11111111111111111111111111111111
%NTP: Key too long
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast

To configure the options for broadcasting Network Time Protocol (NTP) traffic, use the **ntp broadcast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast [**client**| [**destination** {*ip-address*| *hostname*}] [**key** [*broadcast-key*]] [**version** *number*]]

no ntp [**broadcast** [**client**| [**destination** {*ip-address*| *hostname*}] [**key** [*broadcast-key*]] [**version** *number*]]]

Syntax Description

client	(Optional) Configures a device to listen to NTP broadcast messages.
destination	(Optional) Configures a device to receive broadcast messages.
ip-address | *hostname*	(Optional) IP address or hostname of the device to send NTP broadcast messages to.
key	(Optional) Configures a broadcast authentication key.
broadcast-key	(Optional) Integer from 1 to 4294967295 that is the key number. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
version	(Optional) Indicates that an NTP version is configured.
number	(Optional) Integer from 2 to 4 indicating the NTP version. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Command Default

NTP broadcasting is disabled.

Command Modes

Interface configuration (config-if)

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.
12.4(20T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast**command, the NTP service is activated (if it has not already been activated) and the options are configured for sending NTP traffic simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast**command, only the configuration to send NTP broadcast packets on a specified interface is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp broadcast** command and you now want to remove not only the broadcast capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configures Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp broadcast version 2
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcast client

To configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client

no ntp [**broadcast [client]**]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, an interface is not configured to receive NTP broadcast messages.

Command Modes

Interface configuration (config-if)

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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The **novolley** keyword was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. The **novolley** keyword was removed.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast client** command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast client** command, only the broadcast client configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To prevent synchronization with unauthorized systems, whenever this command is specified, authentication should be enabled with the **ntp authenticate** command or access should be restricted to authorized systems using the **ntp access-group** command.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords. For example, if you previously issued the **ntp broadcast client** command and you now want to remove not only the broadcast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp access-group	Controls access to NTP services on the system.
ntp authenticate	Enables NTP authentication.
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp [broadcastdelay]

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Command Default

By default, the round-trip delay between the Cisco IOS software and an NTP broadcast server is 3000 microseconds.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S

Usage Guidelines

Use the **ntp broadcastdelay** command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds. In IPv6, the value set by this command should be used only when the **ntp broadcast client** and **ntp multicast client** commands have the **novolley** keyword enabled.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcastdelay**command, the NTP service is activated (if it has not already been activated) and the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is set simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcastdelay**command, only the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp broadcastdelay** command and you now want to remove not only the delay setting, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to set the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp clear drift

To reset the drift value stored in the persistent data file, use the **ntp clear drift**command in privileged EXEC mode.

ntp clear drift

Syntax Description

This command has no arguments or keywords.

Command Default

The drift value stored in the persistent data file is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

The **ntp clear drift**command is used to reset the local clock drift value in the persistent data file. The drift is the frequency offset between the local clock hardware and the authoritative time from the Network Time Protocol version 4 (NTPv4) servers. NTPv4 automatically computes this drift and uses it to compensate permanently for local clock imperfections.

This command is available only when the NTP service is activated using any **ntp** command in global configuration mode.

Examples

The following example shows how to reset the drift value in the persistent data file:

```
Router# ntp clear drift
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp clock-period

Caution Do not use this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

Note Effective with Cisco IOS Release 15.0(1)M, the **ntp clock-period** command is not available in Cisco IOS software.

As NTP compensates for the error in the software clock, it keeps track of the correction factor for this error. When the value for the clock period needs to be adjusted, the system automatically enters the correct value into the running configuration. To remove the automatically generated value for the clock period, use the **no** form of this command.

ntp clock-period *value*

no ntp [clock-period]

Syntax Description

value	Amount of time to add to the software clock for each clock hardware tick (this value is multiplied by 2 -32). The default value is 17179869 2 -32 seconds (4 milliseconds).

Command Default

The clock period value is automatically generated.

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.
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 removed.

Usage Guidelines

Do not manually set a value for the NTP clock period.

If the system has automatically entered a value for the clock period into the running configuration, NTP synchronizes faster after the system is restarted when the **copy running-config startup-config** command has been entered to save the configuration to NVRAM.

The NTP service can be activated by entering any **ntp** command. In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp clock-period**command, only the automatically generated value is removed. You should remove this command line when copying configuration files to other devices.The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you want to remove not only the clock period, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

If the system has automatically entered a value for the clock period into the running configuration, NTP synchronizes faster after the system is restarted when the **copy running-config startup-config** command has been entered to save the configuration to NVRAM. The following example shows a typical difference between the values of the NTP clock-period setting in the running configuration and in the startup configuration:

```
Router# show startup-config | include clock-period
ntp clock-period 17180239
Router# show running-config | include clock-period
ntp clock-period 17180255
```

The following example shows how to remove the automatically generated value for the clock period from the running configuration:

```
Router(config)# no ntp clock-period
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable the receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable [**ip**| **ipv6**]

no ntp disable [**ip**| **ipv6**]

Syntax Description

ip	(Optional) Disables IP-based NTP traffic.
ipv6	(Optional) Disables IPv6-based NTP traffic.

Command Default

By default, interfaces receive NTP packets.

Command Modes

Interface configuration (config-if)

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.
12.4(20)T	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

This command provides a simple method of access control.

Use the **ntp disable** command in interface configuration mode to configure an interface to reject NTP packets. If the **ntp disable** command is configured on an interface that does not have any NTP service running, the interface remains disabled even after the NTP service is started by another NTP configuration. When you use the **ntp disable** command without the **ip** or **ipv6** keyword, NTP is disabled on the interface for all the address families.

When you enter the **no ntp disable**command in interface configuration mode, the interface that was configured to reject NTP packets is enabled to receive NTP packets.

Note Remove all NTP commands from an interface before entering the **ntp disabl**e command on that interface.

Configuring the **ntp disable** command on an interface does not stop the NTP service. To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to prevent Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

The following example shows the message displayed when you try to execute the **ntp disable** command on an interface that has other NTP commands configured on it:

```
Router(config-if)# ntp disable
%NTP: Unconfigure other NTP commands on this interface before executing 'ntp disable'
```

If you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without keywords in global configuration mode. The following example shows how to disable the NTP service on a device:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp logging

To enable Network Time Protocol (NTP) message logging, use the **ntp logging** command in global configuration mode. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp [logging]

Syntax Description

This command has no arguments or keywords.

Command Default

NTP message logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use the **ntp logging** command to control the display of NTP logging messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp logging**command, the NTP service is activated (if it has not already been activated) and message logging is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp logging**command, only message logging is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp logging** command and you now want to disable not only the message logging,

but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to enable NTP message logging and verify that it is enabled:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ntp logging
Router(config)# end
Router# show running-config | include ntp
ntp logging
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to disable NTP message logging and verify to that it is disabled:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no
 ntp logging
Router# end
Router(config)# show running-config | include ntp
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no**form of this command.

ntp master [*stratum*]

no ntp [master]

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Command Default

By default, the master clock function is disabled. When enabled, the default stratum is 8.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelin

Caution Use this command with caution. Valid time sources can be easily overridden using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

A system with the **ntp master** command configured that cannot reach any clock with a lower stratum number will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manual setting, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp master**command, the NTP service is activated (if it has not already been activated) and the Cisco IOS software is configured as an NTP master clock simultaneously. When you enter the **no ntp master** command, only the NTP master clock configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp master** command and you now want to remove not only the master clock function, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Note Use the **ntp master** command to configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available. When the external NTP source is available again, NTP selects the best router as the NTP master.

Examples

The following example shows how to configure a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock that is an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for a routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp [max-associations]

Syntax Description

number	Number of NTP associations. The range is from 1 to 4294967295. The default is 100. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.

Command Default

The maximum association value of NTP peers and clients is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. Use the **ntp max-associations** command to set the maximum number of NTP peer and client associations that the router will serve.

The **ntp max-associations**command is useful for ensuring that the router is not overwhelmed by NTP synchronization requests. For an NTP master server, this command is useful for allowing numerous devices to synchronize to a router.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp max-associations**command, the NTP service is activated (if it has not already been activated) and the maximum number of NTP peers and clients is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp max-associations**command, only the maximum number value is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp max-associations**command and you now want to remove not only that maximum value, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Note By default, the previous configuration values are retained when the last valid configuration (configuration for which the NTP service needs to run) is removed. Only the configuration values related to the maximum number of NTP peer and client associations are reset to the default value when the NTP process is disabled.

Examples

In the following example, the router is configured to act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays all current NTP associations for the device.

ntp maxdistance

To configure a maximum distance threshold value to govern the number of packets required for synchronization of peers in Network Time Protocol version 4 (NTPv4), use the **ntp maxdistance** command in global configuration mode. To set the maximum distance threshold to the default value, use the **no** form of this command.

ntp maxdistance *threshold-value*

no ntp [maxdistance]

Syntax Description

threshold-value	Maximum distance threshold value. Range: 1 to 16. Default: 8.

Command Default

A maximum distance threshold value of 8 is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXJ	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(1)S1	This command was modified. The default value for the *threshold-value* argument was changed from 1 to 8.

Usage Guidelines

Use the **ntp maxdistance** command to configure the maximum distance threshold for NTPv4. The maximum distance threshold is a selection threshold that is configured for determining the number of packets required for synchronization of Network Time Protocol (NTP) peers.

The number of packets is determined by the synchronization distance for each association and a limit called the distance threshold. The synchronization distance starts at 16, then drops by a factor of about 2 when each packet is received. The default distance threshold is 1. Use the **ntp maxdistance** command to change the number of packets required.

When you enter the **no ntp maxdistance** command, only the NTP maxdistance threshold value is reset to the default value. The NTP service itself remains active, along with any other previously configured NTP functions.

If you had issued the **ntp maxdistance** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords or arguments.

Note If you use the **no ntp** command without any keywords or arguments in global configuration mode, all NTP configurations are removed and the NTP service on the device is disabled.

Examples

The following example shows how to set the maxdistance threshold value to 10:

```
Router(config)# ntp maxdistance 10
```

The following example shows the default setting of the maxdistance threshold:

```
Router# show running-config | include ntp
ntp max-associations 100
ntp maxdistance 10
Router#
```

ntp multicast

To configure a system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address*| *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp [**multicast** [**ip-address**| **ipv6-address**] [**key** *key-id*] [**ttl** *value*] [**version** *number*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 2 to 4. Default version number for IPv4 is 3, and default number for IPv6 is 4. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Command Default

NTP multicast capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address*argument was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address*argument was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast**command, the NTP service is activated (if it has not already been activated) and the interface on which to send multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast** command, only the multicast capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command in global configuration mode without keywords. For example, if you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

If you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. The following example shows how to remove the **ntp multicast** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the**ntp multicast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address*| *ipv6-address*]

no ntp [**multicast client** [*ip-address*| *ipv6-address*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.

Command Default

NTP multicast client capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for IPv6 was added. The *ipv6-address*argument and **novolley** keyword were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The *ipv6-address*argument and **novolley** keyword were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S. The **novolley** keyword was removed.

Release	Modification
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use the **ntp multicast client** command to allow the system to listen to multicast packets on an interface-by-interface basis.

This command enables the multicast client mode on the local NTP host. In this mode, the host is ready to receive mode 5 (broadcast) NTP messages sent to the specified multicast address. After receiving the first packet, the client measures the nominal propagation delay using a brief client/server association with the server. After this initial phase, the client enters the broadcast client mode, in which it synchronizes its clock to the received multicast messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast client** command, the NTP service is activated (if it has not already been activated) and the interface on which to receive multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast client** command, only the multicast client capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To prevent synchronization with unauthorized systems, whenever this command is specified, authentication should be enabled with the **ntp authenticate** command or access should be restricted to authorized systems using the **ntp access-group** command.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

If you had previously issued the **ntp multicast client**command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. The following example shows how to remove the **ntp multicast client**command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp access-group	Controls access to NTP services on the system.
ntp authenticate	Enables NTP authentication.

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp orphan

To enable a group of Network Time Protocol (NTP) devices to select one among them to be the simulated Coordinated Universal Time (UTC) source if all real-time clock sources become inaccessible, use the **ntp orphan** command in global configuration mode. To disable the orphan mode, use the **no** form of this command.

ntp orphan *stratum*

no ntp orphan

Syntax Description

stratum	The orphan stratum value. The device is prevented from switching to orphan mode, as long as no stratum values the servers to which this device is connected exceed this value. Range: 1 to 16. Default: 0.

Command Default

The orphan mode is set to stratum 0.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

To enable orphan mode in a host, use the **ntp orphan** command. The value of the *stratum* argument should be less than 16 and greater than the stratum occurring in the Internet time servers to which the host is connected. Provide an adequate number of available stratums so that every subnet host relying on the orphan children, which are the devices that depend on the the core server that simulates the UTC source, has a stratum that is less than 16. Set the value of the *stratum* argument to 0 if no association is configured with other servers or reference clocks. Configure the **ntp orphan** command with the same value for the *stratum* argument in all the core servers and orphan children. Configure each orphan child with all the root servers.

Examples

The following example shows how to configure NTP such that it does not switch to orphan mode as long as a time source of stratum value 1 to 5 is accessible:

```
Device(config)# ntp server 10.1.1.1
Device(config)# ntp peer 172.16.0.1
Device(config)# ntp orphan 6
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize with a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp panic update

To configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds, use the **ntp panic update**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ntp panic update

no ntp panic update

Syntax Description

This command has no arguments or keywords.

Command Default

NTP is not configured to reject time updates greater than the panic threshold value.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T3	This command was introduced.

Usage Guidelines

If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

```
NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000. seconds;
set clock manually to the correct UTC time.
```

Examples

The following example shows how to configure NTP to reject time updates greater than the panic threshold:

```
Router(config)# ntp panic update
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp passive

To configure passive Network Time Protocol (NTP) associations, use the **ntp passive** command in global configuration mode. To disable the passive NTP associations, use the **no** form of this command.

ntp passive

no ntp [passive]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, passive NTP associations are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXJ	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp passive** command to configure passive NTP associations. By default, passive NTP associations are accepted only when configured using the **ntp passive** command. Use the **no ntp passive** command to change the configuration to the default, that is, not to accept passive associations.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp passive** command, the NTP service is activated (if it has not already been activated) and the passive NTP associations are configured simultaneously.

When you enter the **no ntp passive** command, only the passive NTP association configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To prevent synchronization with unauthorized systems, whenever this command is specified, authentication should be enabled with the **ntp authenticate** command or access should be restricted to authorized systems using the **ntp access-group** command.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp passive** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure passive NTP associations:

```
Router> enable
Router# configure terminal
Router(config)# ntp passive
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.
ntp access-group	Controls access to NTP services on the system.
ntp authenticate	Enables NTP authentication.

ntp peer

To configure a router to allow its software clock to be synchronized with the software clock of a Network Time Protocol (NTP) peer or to allow the software clock of a NTP peer to be synchronized with the software clock of the router, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer [**vrf** *vrf-name*] {*ip-address*| *ipv6-address*| [**ip**| **ipv6**] *hostname*} **[normal-sync]** [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] **[prefer]** [**maxpoll** *number*] [**minpoll** *number*] **[burst] [iburst]**

no ntp [**peer** [**vrf** *vrf-name*] {*ip-address*| *ipv6-address*| [**ip**| **ipv6**] *hostname*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the VPN routing and forwarding (VRF) instance that the NTP peer should use for routing to the destination server instead of using the global routing table.
ip-address	IPv4 address of the NTP peer providing or being provided the software clock synchronization.
ipv6-address	IPv6 address of the NTP peer providing or being provided the clock synchronization.
ip	(Optional) Forces Domain Name System (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the NTP peer that is providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization of the NTP peer with the software clock startup.
version	(Optional) Specifies the NTP version number.
number	(Optional) NTP version number. The range is from 2 to 4. **Note** In Cisco IOS Release 12.2(33)SX. The range is from 1 to 4.
key	(Optional) Specifies the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this NTP peer.
source	(Optional) Specifies that the source address of the server must be taken from the specified interface.

interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface- number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this NTP peer the preferred peer that provides the clock synchronization.
maxpoll *number*	(Optional) Configures the maximum time intervals, in seconds, between client requests sent to the server. The range is from 4 to 17. The default is 10.
minpoll *number*	(Optional) Configures the minimum time intervals, in seconds, between client requests sent to the server. The range is from 4 to 17. The default is 6.
burst	(Optional) Enables burst mode. The burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval to reduce the effects of network jitter. **Note** Effective with Cisco IOS Release 15.2(1)S1 the burst mode is enabled by default. However, the **burst** keyword is retained in the command.
iburst	(Optional) Enables initial burst (iburst) mode. The iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This keyword allows rapid time setting at system startup or when an association is configured. **Note** Effective with Cisco IOS Release 15.2(1)S1 and 15.2(2)T1, the iburst mode is enabled by default. However, the **iburst** keyword is retained in the command.

Command Default

The software clock on a router is not configured to synchronize with the NTP peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **normal-sync** keyword was added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added. The command behavior was modified to display a message when an unsupported NTP version is selected.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

When a peer is configured, the default NTP version number is 4, no authentication key is used, and the source address is taken from the outgoing interface.

Use this command to allow a device software clock to synchronize with a peer software clock or vice versa. Use the **prefer** keyword to reduce switching between peers.

If you are using the NTP version 3 (NTPv3) and NTP synchronization does not occur, try using NTP version 2 (NTPv2). For IPv6, use NTP version 4 (NTPv4).

If you select an NTP version that is not supported, a message is displayed.

If you are using NTPv4, the NTP synchronization takes more time to complete when compared to NTPv3, which synchronizes in seconds or within 1 to 2 minutes. The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword, respectively. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

Multiple configurations are not allowed for the same peer or server. If a configuration exists for a peer and you use the **ntp peer** command to configure the same peer, the new configuration will replace the old one.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp peer** command, the NTP service is activated (if it has not already been activated) and the NTP peer is configured simultaneously.

When you enter the **no ntp peer** command, only the NTP peer configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

If you had issued the **ntp peer** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords or arguments.

Note If you use the **no ntp** command without keywords or arguments in global configuration mode, all NTP configurations are removed and the NTP service on the device is disabled.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the software clock of a peer (or vice versa) at the IPv4 address 192.168.22.33 using NTPv2. The source IPv4 address is the address of Ethernet 0:

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

The following example shows how to configure a router to allow its software clock to be synchronized with the software clock of a peer (or vice versa) at IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp peer 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to disable rapid software clock synchronization at startup:

```
Router(config)# ntp peer 192.168.22.33 normal-sync
```

The following example shows the message displayed when you try to configure an unsupported NTP version:

```
Router(config)# ntp peer 192.168.22.33 version 1
NTP version 4 supports backward compatibility to only version 2 and 3
 Please re-enter version[2-4]
 Setting NTP version 4 as default
```

The following example shows how to remove all the configured NTP options and disable the NTP service:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by an NTP time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external clock source, use the **no** form of this command.

ntp refclock {**trimble**| **telecom-solutions**} **pps** {**cts**| **ri**| **none**} **[inverted]** [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp [refclock]

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions Global Positioning System (GPS) device. **Note** Effective with Cisco IOS Release 15.2(2)T, this keyword is deprecated.
pps	Enables a pulse per second (PPS) signal line. Indicates PPS pulse reference clock support. The options are **cts**, **ri**, or **none**.
cts	Enables PPS on the Clear To Send (CTS) line.
ri	Enables PPS on the Ring Indicator (RI) line.
none	Specifies that no PPS signal is available.
inverted	(Optional) Specifies that the PPS signal is inverted.
pps-offset *milliseconds*	(Optional) Specifies the offset of the PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Indicates the NTP stratum number that the system will claim. The number range is from 0 to 14.
timestamp-offset *number*	(Optional) Specifies the offset of time stamp. The number is the offset (in milliseconds).

Command Default

By default, an external clock source for use with NTP services is not configured.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
12.1	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.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(2)T	This command was modified. The **telecom-solutions** keyword was deprecated.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock trimble pps {**cts** | **ri**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

When two or more servers are configured with the same stratum number, the client will never synchronize with any of the servers. This is because the client is not able to identify the device with which to synchronize. When two or more servers are configured with the same stratum number, and if the client is in synchronization with one of the servers, the synchronization is lost if the settings on one server are changed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp refclock** command, the NTP service is activated (if it has not already been activated) and the external clock source is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp refclock** command, only the external clock source is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To terminate the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows how to configure a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows how to configure a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

If you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords in global configuration mode. The following example shows how to remove the **ntp reflcock** command along with all the configured NTP options and how to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To configure a router to allow its software clock to be synchronized with the software clock of a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server [**vrf** *vrf-name*] {*ip-address*| *ipv6-address*| [**ip**| **ipv6**] *hostname*} **[normal-sync]** [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] **[prefer]** [**maxpoll** *number*] [**minpoll** *number*] **[burst] [iburst]**

no ntp [**server** [**vrf** *vrf-name*] {*ip-address*| *ipv6-address*| [**ip**| **ipv6**] *hostname*}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the VPN routing and forwarding (VRF) instance that the NTP peer should use for routing to the destination server instead of using the global routing table.
ip-address	IPv4 address of the NTP peer providing or being provided the software clock synchronization.
ipv6-address	IPv6 address of the NTP peer providing or being provided the software clock synchronization.
ip	(Optional) Forces domain name server (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the NTP peer providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization of the NTP peer with the software clock at startup.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number. The range is from 2 to 4. **Note** In Cisco IOS Release 12.2SX, the number range is from 1 to 4.
key	(Optional) Specifies the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this NTP peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.

interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this NTP peer the preferred peer that provides the clock synchronization.
maxpoll *number*	(Optional) Configures the maximum time intervals, in seconds, between client requests sent to the server. The range is from 4 to 17. The default is 10.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The range is from 4 to 17. The default is 6.
burst	(Optional) Enables burst mode. The burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter. **Note** Effective with Cisco IOS Release 15.2(1)S1, the **burst** keywords is enabled by default.
iburst	(Optional) Enables initial burst (iburst) mode. The iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This keyword allows rapid time setting at system startup or when an association is configured. **Note** Effective with Cisco IOS Release 15.2(1)S1, the **iburst** keyword is enabled by default.

Command Default

No servers are configured by default. When a server is configured, the default NTP version number is 3, an authentication key is not used, and the source IPv4 or IPv6 address is taken from the outgoing interface. Effective with Cisco IOS Release 15.2(1)S1, the **burst** and the **iburst** keywords are enabled by default.

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 was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added to NTP version 4. The**burst ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use this command if you want to allow the system to synchronize the system software clock with the specified NTP server.

When you use the *hostname* argument, the router performs a DNS lookup on that name and stores the IPv4 or IPv6 address in the configuration. For example, if you enter the **ntp server** *hostname* command and then check the running configuration, the output shows ntp server *a.b.c.d*, where *a.b.c.d* is the IP address of the host, assuming that the router is correctly configured as a DNS client.

Use the **prefer** keyword if you need to use this command multiple times and you want to set a preferred server. Using the **prefer** keyword reduces switching between servers.

If you are using the default NTP version 3 and NTP synchronization does not occur, try Network TimeProtocol version 2 (NTPv2). Some NTP servers on the Internet run version 2. For IPv6, use NTP version 4 (NTPv4).

If you are using NTPv4, the NTP synchronization takes more time to complete when compared to NTPv3, which synchronizes in seconds or within of 1 to 2 minutes. The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword, respectively. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

Note Effective with Cisco IOS Release 15.2(1)S1, the burst and iburst modes are enabled by default. However, the **burst** and **iburst** keywords are retained in the command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp server** command, the NTP service is activated (if it has not already been activated) and software clock synchronization is configured simultaneously.

When you enter the **no ntp server** command, only the server synchronization capability is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

If you had issued the **ntp server** command and you now want to remove not only server synchronization capability, but also all NTP functions from the device, use the **no ntp** command without any keywords or arguments.

Note If you use the **no ntp** command without keywords or arguments in global configuration mode, all NTP configurations are removed and the NTP service on the device is disabled.

If you want to disable an NTP server or a peer configured with a particular source interface, you must specify the interface type and number in the **no** form of the command.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the software clock of an NTP server by using the device at the IPv4 address 172.16.22.44 using NTPv2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

The following example shows how to configure a router to allow its software clock to be synchronized with the software clock of an NTP server by using the device at the IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp server 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to configure software clock synchronization with an NTP server with a particular source interface:

```
Router(config)# ntp server 209.165.200.231 source ethernet 0/1
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *interface-type interface-number*

no ntp [source]

Syntax Description

interface-type	Type of interface.
interface-number	Number of the interface.

Command Default

Source address is determined by the outgoing interface.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
12.2(33)SXJ	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Use this command when you want to use a particular source IPv4 or IPv6 address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be

used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp source** command, the NTP service is activated (if it has not already been activated) and the source address is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp source** command, only the source address is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp source**command and you now want to remove not only the configured source address, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If the NTP source is not set explicitly, and a link fails or an interface state changes, the NTP packets are sourced from the next best interface and the momentarily lost synchronization is regained.

Examples

The following example shows how to configure a router to use the IPv4 or IPv6 address of Ethernet interface 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable the authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number* [**-** *end-key-number*]

no ntp trusted-key *key-number* [**-** *end-key-number*]

Syntax Description

key-number	Specifies the key number of the authentication key to be trusted. Valid values are from 1 to 65535.
- *end-key-number*	(Optional) Ending key number of the range of authentication keys to be trusted. Valid values are from 1 to 65535.

Command Default

Authentication of the identity of the system is disabled.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S. The - *end-key-number* argument was added.
Cisco IOS XE Release 3.5S	This command was modified. The - *end-key-number* argument was added.

Release	Modification
15.2(3)T	This command was modified. The - *end-key-number* argument was added.

Usage Guidelines

If authentication is enabled, use the **ntp trusted-key** command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets for synchronization. This authentication function provides protection against accidentally synchronizing the system to another system that is not trusted, because the other system must know the correct authentication key. You can also enter the desired range of key numbers by entering the *key-number* argument followed by a space and a hyphen (-), and then a space and the *end-key-number* argument.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp trusted-key** command, the NTP service is activated (if it has not already been activated) and the system to which NTP will synchronize is authenticated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp trusted-key** command, only the authentication is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp trusted-key** command and you now want to remove not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication keys 1 to 3 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 1 md5 key1
Router(config)# ntp authentication-key 2 md5 key2
Router(config)# ntp authentication-key 3 md5 key3
Router(config)# ntp trusted-key 1 - 3
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp [update-calendar]

Syntax Description

This command has no arguments or keywords.

Command Default

The hardware clock (calendar) is not updated.

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the CLI as the calendar, in addition to the software-based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may lose synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time

specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** command in user EXEC mode.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp update-calendar** command, the NTP service is activated (if it has not already been activated) and the hardware clock is updated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp update-calendar** command, only the clock updates are stopped in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp update-calendar** command and you now want to disable not only the periodic updates, but also all NTP functions running on the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.

show buffers leak

To display the details of all the buffers that are older than one minute in the system, use the **show buffers leak**command in user EXEC or privileged EXEC mode.

show buffers leak [**resource user**]

Syntax Description

resource user	(Optional) Displays the resource user information to which the leaked buffers belong to.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers leak** command:

```
Router# show buffers leak
Header   DataArea Pool    Size  Link Enc    Flags      Input     Output   User
6488F464  E000084 Small    74    0    0       10       None       None EEM ED Sy
6488FB5C  E000304 Small    74    0    0       10       None       None EEM ED Sy
648905D0  E0006C4 Small    61    0    0        0       None       None EEM ED Sy
648913C0  E000BC4 Small    74    0    0       10       None       None EEM ED Sy
6489173C  E000D04 Small    74    0    0       10       None       None EEM ED Sy
648921B0  E0010C4 Small    60    0    0        0       None       None Init
6489252C  E001204 Small   103    0    0       10       None       None EEM ED Sy
64892C24  E001484 Small    74    0    0       10       None       None EEM ED Sy
64892FA0  E0015C4 Small    74    0    0       10       None       None EEM ED Sy
64893A14  E001984 Small    74    0    0       10       None       None EEM ED Sy
64893D90  E001AC4 Small    61    0    0        0       None       None EEM ED Sy
64894804  E001E84 Small    61    0    0        0       None       None EEM ED Sy
6517CB64  E32F944 Small    74    0    0       10       None       None EEM ED Sy
6517D25C  E176D44 Small    74    0    0       10       None       None EEM ED Sy
6517D5D8  E176E84 Small    74    0    0       10       None       None EEM ED Sy
6517D954  E209A84 Small    74    0    0       10       None       None EEM ED Sy
6517E744  E209D04 Small    61    0    0        0       None       None EEM ED Sy
6517EE3C  E29CBC4 Small    61    0    0        0       None       None EEM ED Sy
65180324  E177844 Small    74    0    0       10       None       None EEM ED Sy
65180D98  E177C04 Small    61    0    0        0       None       None EEM ED Sy
65E1F3A0  E4431A4 Small   102    0    0        0       None       None EEM ED Sy
64895278  E002644 Middl   191    0    0       10       None       None EEM ED Sy
64895CEC  E003004 Middl   173    0    0       10       None       None EEM ED Sy
64896068  E003344 Middl   176    0    0       10       None       None EEM ED Sy
648963E4  E003684 Middl   191    0    0       10       None       None EEM ED Sy
64896E58  E004044 Middl   109    0    0       10       None       None EEM ED Sy
64897C48  E004D44 Middl   194    0    0       10       None       None EEM ED Sy
65181F04  E330844 Middl   173    0    0       10       None       None EEM ED Sy
65183070  E3C3644 Middl   105    0    0       10       None       None EEM ED Sy
```

```
65DF9558  E4746E4 Middl   107    0    0        0       None       None EEM ED Sy
65DFA6C4  E475724 Middl   116    0    0        0       None       None EEM ED Sy
65DFADBC  E475DA4 Middl   115    0    0        0       None       None EEM ED Sy
65DFC620  E477464 Middl   110    0    0        0       None       None EEM ED Sy
64C64AE0        0 FS He     0    0    3        0       None       None Init
64C64E5C        0 FS He     0    0    3        0       None       None Init
64C651D8        0 FS He     0    0    3        0       None       None Init
64C65554        0 FS He     0    0    0        0       None       None Init
64C658D0        0 FS He     0    0    0        0       None       None Init
64C65C4C        0 FS He     0    0    0        0       None       None Init
64C65FC8        0 FS He     0    0    0        0       None       None Init
64C66344        0 FS He     0    0    0        0       None       None Init
64D6164C        0 FS He     0    0    0        0       None       None Init
64EB9D10        0 FS He     0    0    0        0       None       None Init
6523EE14        0 FS He     0    0    0        0       None       None Init
65413648        0 FS He     0    0    0        0       None       None Init
```

The following is sample output from the **show buffers leak resource user**command:

```
Router# show buffers leak resource user
Resource User:  EEM ED Syslog count:       32
Resource User:           Init count:        2
Resource User:         *Dead* count:        2
Resource User: IPC Seat Manag count:       11
Resource User:      XDR mcast count:        2
```

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

Table 1: show buffers leak Field Descriptions

Field	Description
Header	Buffer header.
DataArea	The area where the data is available.
Pool	The different buffer pools such as ipc, header, fs header, small, middle, big, very big, large, or huge buffers.
Size	Size of the buffer pool. For example, small buffers are less than or equal to 104 bytes long. Middle buffers are in the range of 105 to 600 bytes long.
Flags	Flags of a packet. The flag indicates whether a particular packet is an incoming packet or is generated by the router.
User	The resource user name.

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
buffer tune automatic	Enables automatic buffer tuning.

show buffers tune

To display the details of automatic tuning of buffers, use the **show buffers tune**command in user EXEC or privileged EXEC mode.

show buffers tune

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers tune** command:

```
Router# show buffers tune
Tuning happened for the pool Small
Tuning happened at 20:47:25
Oldvalues
permanent:50  minfree:20  maxfree:150
Newvalues
permanent:61  minfree:15  maxfree:76
Tuning happened for the pool Middle
Tuning happened at 20:47:25
Oldvalues
permanent:25  minfree:10  maxfree:150
Newvalues
permanet:36  minfree:9  maxfree:45
```

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

Table 2: show buffers tune Field Descriptions

Field	Description
Oldvalues	The minimum and maximum free buffers before automatic tuning was enabled.
Newvalues	The minimum and maximum free buffers after automatic tuning was enabled.

Related Commands

Command	Description
buffer tune automatic	Enables automatic tuning of buffers.

show buffers usage

To display the details of the buffer usage pattern in a specified buffer pool, use the **show buffers usage**command in user EXEC or privileged EXEC mode.

show buffers usage [**pool** *pool-name*]

Syntax Description

pool	(Optional) Displays the details of a specified pool.
pool-name	(Optional) Specified pool. If a pool is not specified, details of all the pools are displayed. Valid values are ipc, header, fs header, small, middle, big, verybig, large, and huge.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers usage** command:

```
Router# show buffers usage
Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0
Statistics for the Middle pool
Caller pc    : 0x626BA9E0 count:       12
Resource User: EEM ED Sys count:       12
Number of Buffers used by packets generated by system:   41
Number of Buffers used by incoming packets:               0
Statistics for the Big pool
Number of Buffers used by packets generated by system:   50
Number of Buffers used by incoming packets:               0
Statistics for the VeryBig pool
Number of Buffers used by packets generated by system:   10
Number of Buffers used by incoming packets:               0
Statistics for the Large pool
Number of Buffers used by packets generated by system:    0
Number of Buffers used by incoming packets:               0
Statistics for the Huge pool
Number of Buffers used by packets generated by system:    0
Number of Buffers used by incoming packets:               0
Statistics for the IPC pool
```

```
Number of Buffers used by packets generated by system:    2
Number of Buffers used by incoming packets:               0
Statistics for the Header pool
Number of Buffers used by packets generated by system:  511
Number of Buffers used by incoming packets:               0
Statistics for the FS Header pool
Caller pc    : 0x608F68FC count:        9
Resource User:       Init count:       12
Caller pc    : 0x61A21D3C count:        1
Caller pc    : 0x60643FF8 count:        1
Caller pc    : 0x61C526C4 count:        1
Number of Buffers used by packets generated by system:   28
Number of Buffers used by incoming packets:               0
```

The following is sample output from the **show buffers usage pool**command for the pool named small:

```
Router# show buffers usage pool small
Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0
```

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
show buffers leak	Displays details of the buffers that have leaked.

show calendar

To display the current time and date setting for the hardware clock, use the **show calendar** command in EXEC mode:

show 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 (calendar) which is separate from the software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

You can compare the time and date shown with this command with the time and date listed via the **show clock** EXEC command to verify that the hardware clock and software clock are synchronized with each other. The time displayed is relative to the configured time zone.

Examples

In the following sample display, the hardware clock indicates the time stamp of 12:13:44 p.m. on Friday, July 19, 1996:

```
Router> show calendar
12:13:44 PST Fri Jul 19 1996
```

Related Commands

Command	Description
show clock	Displays the time and date from the system software clock.

show clock

To display the time and date from the system software clock, use the **show clock** command in user EXEC or privileged EXEC mode.

show clock [detail]

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).

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.
12.4(20)T	Support for IPv6 was added.
15.2(1)S	This command is supported in the Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The software clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the “authoritative” flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:

Symbol	Description	Example
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.

Note In general, NTP synchronization takes approximately 15 to 20 minutes.

Examples

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail
15:29:03.158 PST Tue Feb 25 2003
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock
.16:42:35.597 UTC Tue Feb 25 2003
```

Related Commands

Command	Description
clock set	Manually sets the software clock.
show calendar	Displays the current time and date setting of the system hardware clock.

show ntp associations

To display the status of Network Time Protocol (NTP) associations, use the **show ntp associations** command in user EXEC or privileged EXEC mode.

show ntp associations [detail]

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.

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.
12.4(20)T	The command was integrated into Cisco IOS Release 12.4(20)T. Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.7S	This command was modified. The command output was modified to display assoc ID and assoc name fields when the **detail** keyword is used.

Examples

were
Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Device> show ntp associations

      address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
```

```
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

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

Table 3: show ntp associations Field Descriptions

Field	Description
address	Address of the peer.
ref clock	Address of the reference clock of the peer.
st	Stratum of the peer.
when	Time since the last NTP packet was received from the peer (in seconds).
poll	Polling interval (in seconds).
reach	Peer reachability (bit string, in octal).
delay	Round-trip delay to the peer (in milliseconds).
offset	Relative time of the peer clock to the local clock (in milliseconds).
disp	Dispersion.
*	Synchronized to this peer.
#	Almost synchronized to this peer.
+	Peer selected for possible synchronization.
-	Peer is a candidate for selection.
~	Peer is statically configured.

The following is sample output from the **show ntp associations detail** command:

```
Device> show ntp associations detail

172.31.32.2 configured, insane, invalid, stratum 5
ref ID 172.31.32.1, time AFE252C1.6DBDDFF2 (00:12:01.428 PDT Mon Jul 5 1993)
our mode active, peer mode active, our poll intvl 1024, peer poll intvl 64
root delay 137.77 msec, root disp 142.75, reach 376, sync dist 215.363
delay 4.23 msec, offset -8.587 msec, dispersion 1.62
precision 2**19, version 4
assoc ID 1, assoc name 192.168.1.55,
assoc in packets 60, assoc out packets 60, assoc error packets 0
org time AFE252E2.3AC0E887 (00:12:34.229 PDT Tue Oct 4 2011)
rcv time AFE252E2.3D7E464D (00:12:34.240 PDT Mon Jan 1 1900)
xmt time AFE25301.6F83E753 (00:13:05.435 PDT Tue Oct 4 2011)
filtdelay =     4.23    4.14    2.41    5.95    2.37    2.33    4.26    4.33
filtoffset =   -8.59   -8.82   -9.91   -8.42  -10.51  -10.77  -10.13  -10.11
```

```
filterror =     0.50    1.48    2.46    3.43    4.41    5.39    6.36    7.34
192.168.13.33 configured, selected, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE24F0E.14283000 (23:56:14.078 PDT Sun Jul 4 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 83.72 msec, root disp 217.77, reach 377, sync dist 264.633
delay 4.07 msec, offset 3.483 msec, dispersion 2.33
precision 2**6, version 3
assoc ID 2, assoc name myserver
assoc in packets 0, assoc out packets 0, assoc error packets 0
org time AFE252B9.713E9000 (00:11:53.442 PDT Tue Oct 4 2011)
rcv time AFE252B9.7124E14A (00:11:53.441 PDT Mon Jan 1 1900)
xmt time AFE252B9.6F625195 (00:11:53.435 PDT Mon Jan 1 1900)
filtdelay =     6.47    4.07    3.94    3.86    7.31    7.20    9.52    8.71
filtoffset =    3.63    3.48    3.06    2.82    4.51    4.57    4.28    4.59
filterror =     0.00    1.95    3.91    4.88    5.84    6.82    7.80    8.77
192.168.13.57 configured, our_master, sane, valid, stratum 3
ref ID 192.168.1.111, time AFE252DC.1F2B3000 (00:12:28.121 PDT Mon Jul 5 1993)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 125.50 msec, root disp 115.80, reach 377, sync dist 186.157
delay 7.86 msec, offset 11.176 msec, dispersion 3.62
precision 2**6, version 2
assoc ID 2, assoc name myserver
assoc in packets 0, assoc out packets 0, assoc error packets 0
org time AFE252DE.77C29000 (00:12:30.467 PDT Tue Oct 4 2011)
rcv time AFE252DE.7B2AE40B (00:12:30.481 PDT Mon Jan 1 1900)
xmt time AFE252DE.6E6D12E4 (00:12:30.431 PDT Mon Jan 1 1900)
filtdelay =    49.21    7.86    8.18    8.80    4.30    4.24    7.58    6.42
filtoffset =   11.30   11.18   11.13   11.28    8.91    9.09    9.27    9.57
filterror =     0.00    1.95    3.91    4.88    5.78    6.76    7.74    8.71
```

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

Table 4: show ntp associations detail Field Descriptions

Field	Descriptions
configured	Peer was statically configured.
insane	Peer fails basic checks.
invalid	Peer time is believed to be invalid.
ref ID	Address of the machine the peer is synchronized to.
time	Last time stamp the peer received from its master.
our mode	Mode of the source relative to the peer (active/passive/client/server/bdcast/bdcast client).
peer mode	Peer's mode relative to the source.
our poll intvl	Source poll interval to the peer.
peer poll intvl	Peer's poll interval to the source.
root delay	Delay (in milliseconds) along the path to the root (ultimate stratum 1 time source).
root disp	Dispersion of the path to the root.
reach	Peer reachability (bit string in octal).

Field	Descriptions
sync dist	Peer synchronization distance.
delay	Round-trip delay to the peer (in milliseconds).
offset	Offset of the peer clock relative to the system clock.
dispersion	Dispersion of the peer clock.
precision	Precision of the peer clock in Hertz.
assoc ID	Association ID of the peer.
assoc name	Association name of the peer.
version	NTP version number that the peer is using.
org time	Originate time stamp.
rcv time	Receive time stamp.
xmt time	Transmit time stamp.
filtdelay	Round-trip delay (in milliseconds) of each sample.
filtoffset	Clock offset (in milliseconds) of each sample.
filterror	Approximate error of each sample.
sane	Peer passes basic checks.
selected	Peer is selected for possible synchronization.
valid	Peer time is believed to be valid.
our_master	Local machine is synchronized to this peer.

Related Commands

Command	Description
show ntp status	Displays the status of the NTP.

show ntp info

To display static information about Network Time Protocol (NTP) entities, use the **show ntp info** command in user EXEC or privileged EXEC mode.

show ntp info

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **show ntp info** command to display static information about the NTP implementation running on the host.

Examples

The following is sample output from the **show ntp info** command:

```
Device> show ntp info

Ntp Software Name: Example_NTP
Ntp Software Version: ntp-1.1
Ntp Software Vendor: vendor1
Ntp System Type: Example_System
```

Related Commands

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

Table 5: show ntp info Field Descriptions

Field	Description
Ntp Software Name	Product name of the running NTP version.
Ntp Software Version	Version number of the installed NTP implementation.

Field	Description
Ntp Software Vendor	Name of the vendor or author of the installed NTP version.
Ntp System Type	Information about the platform.

Related Commands

Command	Description
show ntp status	Displays the status of NTP.

show ntp packets

To display information about Network Time Protocol (NTP) packets, use the **show ntp packets** command in user EXEC or privileged EXEC mode.

show ntp packets [**mode** {**active**| **client**| **passive**| **server**| **xcast-client**| **xcast-server**}]

Syntax Description

mode	Specifies the association mode.
active	Displays symmetric-active statistics.
client	Displays client statistics.
passive	Displays symmetric-passive statistics.
server	Displays server statistics.
xcast-client	Displays broadcast-client statistics.
xcast-server	Displays broadcast-server statistics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following is sample output from the **show ntp packets** command:

```
Device# show ntp packets

Ntp In packets: 100
Ntp Out packets: 110
Ntp bad version packets: 4
Ntp protocol error packets: 0
```

The following is sample output from the **show ntp packets mode active** command:

```
Device# show ntp packets mode active

Ntp In packets symmetric-active: 40
Ntp Out packets symmetric-active: 50
```

The following is sample output from the **show ntp packets mode client** command:

```
Device# show ntp packets mode client

Ntp In packets client: 40
Ntp Out packets client: 50
```

The following is sample output from the **show ntp packets mode passive** command:

```
Device# show ntp packets mode passive

Ntp In packets symmetric-passive: 40
Ntp Out packets symmetric-passive: 50
```

The following is sample output from the **show ntp packets mode server** command:

```
Device# show ntp packets mode server

Ntp In packets server: 0
Ntp Out packets server: 0
```

The following is sample output from the **show ntp packets mode xcast-client** command:

```
Device# show ntp packets mode xcast-client

Ntp In packets xcast-client: 0
Ntp Out packets xcast-client: 0
```

The following is sample output from the **show ntp packets mode xcast-server** command:

```
Device# show ntp packets mode xcast-server

Ntp In packets xcast-server: 0
Ntp Out packets xcast-server: 0
```

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

Table 6: show ntp packets Field Descriptions

Field	Description
Ntp In packets	Number of packets entering the NTP entity.
Ntp Out packets	Number of packets exiting the NTP entity.
Ntp bad version packets	Number of packets with incorrect version numbers that entered the NTP entity.
Ntp protocol error packets	Number of packets with incorrect protocol that entered the NTP entity.
Ntp In packets symmetric-active	Number of packets entering the host that is operating in symmetric-active mode.
Ntp Out packets symmetric-active	Number of packets exiting the host that is operating in symmetric-active mode.
Ntp In packets client	Number of packets entering the host that is operating in client mode.
Ntp Out packets client	Number of packets exiting the host that is operating in client mode.
Ntp In packets symmetric-passive	Number of packets entering the host that is operating in symmetric-passive mode.

Field	Description
Ntp Out packets symmetric-passive	Number of packets exiting the host that is operating in symmetric-passive mode.
Ntp In packets server	Number of packets entering the NTP server.
Ntp Out packets server	Number of packets exiting the NTP server.
Ntp In packets xcast-client	Number of packets entering the host that is operating in xcast-client.
Ntp Out packets xcast-client	Number of packets exiting the host that is operating in xcast-client.
Ntp In packets xcast-server	Number of packets entering the host that is operating in xcast-server.
Ntp Out packets xcast-server	Number of packets exiting the host that is operating in xcast-server.

Related Commands

Command	Description
show ntp status	Displays the status of NTP.

show ntp status

To display the status of the Network Time Protocol (NTP), use the **show ntp status** command in user EXEC or privileged EXEC mode.

show ntp status

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.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.
Cisco IOS XE Release 3.7S	This command was modified. The output of the command was enhanced to include reference assoc ID, time resolution, ntp uptime, system time, leap time, and leap direction fields.

Examples

The following is sample output from the **show ntp status** command:

```
Device> show ntp status

Clock is synchronized, stratum 2, reference assoc id 1, reference is 192.0.2.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**7
reference time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec, time resolution 1000 (1 msec),
root dispersion is 15.91 msec, peer dispersion is 8.01 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 6 sec ago.
ntp uptime (00:00:00.000) UTC,
system time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
leap time is D2352258.243DDF14 (24:00:00.000 IST Tue Dec 31 2011)
leap direction is 1
```

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

Table 7: show ntp status Field Descriptions

Field	Description
synchronized	System is synchronized with an NTP peer.
reference assoc id	Reference association identity.
stratum	NTP stratum of this system.
reference	Address of the peer that the system is synchronized with.
nominal freq	Nominal frequency of the system hardware clock (in Hertz).
actual freq	Measured frequency of the system hardware clock (in Hertz).
precision	Precision of the clock of this system (in Hertz).
reference time	Reference time stamp.
clock offset	Offset of the system clock to the synchronized peer (in milliseconds).
root delay	Total delay along the path to the root clock (in milliseconds).
time resolution	Time resolution of the underlying operating system (in milliseconds).
root dispersion	Dispersion of the root path.
peer dispersion	Dispersion of the synchronized peer.
ntp uptime	Uptime of the NTP entity.
system time	Current date and time of the system.
leap time	Date on which the next known leap second will occur.
leap direction	Direction of next known leap second.

Related Commands

Command	Description
show ntp status	Displays the status of NTP.

show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp**command in EXEC mode on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

show sntp

Syntax Description

This command has no arguments or keywords.

Command Modes

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.
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 is sample output from the **show sntp** command:

```
Router> show sntp
SNTP server     Stratum   Version    Last Receive
171.69.118.9       5         3        00:01:02
172.21.28.34       4         3        00:00:36    Synced  Bcast
Broadcast client mode is enabled.
```

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

Table 8: show sntp Field Descriptions

Field	Description
SNTP server	Address of the configured or broadcast NTP server.
Stratum	NTP stratum of the server. The stratum indicates how far away from an authoritative time source the server is.
Version	NTP version of the server.
Last Receive	Time since the last NTP packet was received from the server.
Synced	Indicates the server chosen for synchronization.

Field	Description
Bcast	Indicates a broadcast server.

Related Commands

Command	Description
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

show time-range

To display information about configured time ranges, use the **show time-range** command in user EXEC or privileged EXEC mode.

show time-range

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior.

Command Modes

User EXEC and Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.33(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 this command to display configured time ranges.

Examples

The following is sample output for the **show time-range** command. The word (active) indicates that the time range is in effect at that moment; otherwise, the output will indicate (inactive).

```
Router# show time-range
time-range entry: test (active)
    absolute start 00:00 01 January 2006 end 23:59 31 December 2006
    periodic weekdays 8:00 to 20:00
```

Related Commands

Command	Description
time-range	Specifies a time range by name and allows you configure a range during which an access list, for example, is active.

sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client**command in global configuration mode to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. To prevent the router from accepting broadcast traffic, use the **no** form of this command.

sntp broadcast client

no sntp broadcast client

Syntax Description

This command has no arguments or keywords.

Command Default

The router does not accept SNTP traffic from broadcast servers.

Command Modes

Global configuration

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.
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

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

You must configure the router with either this command or the **sntp server** global configuration command to enable SNTP.

Examples

The following example enables the router to accept broadcast NTP packets and shows sample **show sntp** command output:

```
Router(config)# sntp broadcast client
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp
SNTP server     Stratum   Version    Last Receive
```

```
172.21.28.34       4         3        00:00:36    Synced  Bcast
Broadcast client mode is enabled.
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

sntp logging

To enable Simple Network Time Protocol (SNTP) message logging, use the **sntp logging** command in global configuration mode. To disable SNTP logging, use the **no** form of this command.

sntp logging

no sntp logging

Syntax Description

This command has no arguments or keywords.

Command Default

SNTP message logging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **sntp logging** command to control the display of SNTP logging messages.

SNTP is a compact, client-only version of Network Time Protocol (NTP). SNTP can be used only to receive the time from NTP servers; SNTP cannot be used to provide time services to other systems. You should consider carefully the use of SNTP rather than NTP in primary servers.

Examples

The following example shows how to enable SNTP message logging, configure the IP address of the SNTP server as 10.107.166.3, and verify that SNTP logging is enabled:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# sntp logging
Router(config)# sntp server 10.107.166.3
Router(config)# end
Router#
04:02:54: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# show running-config | include ntp
sntp logging
sntp server 10.107.166.3
```

The “sntp logging” entry in the configuration file verifies that SNTP message logging is enabled.

The following example shows how to disable SNTP message logging and verify that it is disabled:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no
 sntp logging
Router(config)# end
```

```
Router#
04:04:34: %SYS-5-CONFIG_I: Configured from console by console
Router# show running-config | include ntp
sntp server 10.107.166.3
```

The “sntp logging” entry no longer appears in the configuration file, which verifies that SNTP message logging is disabled.

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.
sntp server	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to request and accept NTP traffic from a time server.

sntp server

To configure a Cisco 800, Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** command in global configuration mode. To remove a server from the list of NTP servers, use the **no** form of this command.

sntp server {*address*| *hostname*} [**version** *number*]

no sntp server {*address*| *hostname*}

Syntax Description

address	IP address of the time server.
hostname	Host name of the time server.
version *number*	(Optional) Version of NTP to use. The default is 1.

Command Default

The router does not accept SNTP traffic from a time server.

Command Modes

Global configuration

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.
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

SNTP is a compact, client-only version of the NTP. SNMP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server.

You must configure the router with either this command or the **sntp broadcast client** global configuration command in order to enable SNTP.

SNTP time servers should operate only at the root (stratum 1) of the subnet, and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. A stratum 2 server cannot be used as an SNTP time server. The use of SNTP rather than NTP in primary servers should be carefully considered.

Examples

The following example enables the router to request and accept NTP packets from the server at 172.21.118.9 and displays sample **show sntp** command output:

```
Router(config)# sntp server 172.21.118.9
Router(config)# end
Router#
%SYS-5-CONFIG: Configured from console by console
Router# show sntp
SNTP server     Stratum   Version    Last Receive
172.21.118.9       5         3        00:01:02    Synced
```

Related Commands

Command	Description
show sntp	Displays information about SNTP on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.
sntp broadcast client	Configures a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router to use SNTP to accept NTP traffic from any broadcast server.

sntp source-interface

To use a particular source address in Simple Network Time Protocol (SNTP) packets, use the **sntp source-interface** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

sntp source-interface *type number*

no sntp source-interface

Syntax Description

type	Type of interface.
number	Number of the interface.

Command Default

The source address is determined by the outgoing interface.

Command Modes

Global configuration

Command History

Release	Modification
12.4(10)	This command was introduced.

Usage Guidelines

Use this command to specify a particular source IP address for all SNTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. The **no** form of the command only replaces the default; that is, the source address of the SNTP request sent is determined by the outgoing interface.

If this command is the last one issued and you then remove it, the SNTP process stops.

Examples

The following example shows how to configure a router to use the IP address of interface Ethernet 0 as the source address for all outgoing SNTP packets:

```
Router(config)#
sntp source-interface ethernet 0
```

The following example shows how to remove a configured SNTP option:

```
Router(config)#
no sntp source-interface
```

time-period

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

time-period *minutes*

no time-period *minutes*

Syntax Description

minutes	Specifies how often, in minutes, to automatically save an archive file of the current running configuration in the Cisco configuration archive.

Command Default

No time increment is set.

Command Modes

Archive configuration (config-archive)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 10000 series.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

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

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

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

Examples

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

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

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.
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	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-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the time-range command in global configuration or webvpn context configuration mode. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Desired name for the time range. The name cannot contain either a space or quotation mark, and it must begin with a letter.

Command Default

None

Command Modes

Global configuration Webvpn context configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(17a)SX	Support for this command was implemented on the Cisco 7600 series routers.
12.2(17d)SXB.	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was available in webvpn context configuration mode.
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 **time-range** entries are identified by a name, which is referred to by one or more otherconfiguration commands. Multiple time ranges can occur in a single access list or other feature.

Note In Cisco IOS 12.2SX releases, IP and IPX-extended access lists are the only types of access lists that can use time ranges.

After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

Tip To avoid confusion, use different names for time ranges and named access lists.

Examples

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 24:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface ethernet 0
 ip access-group strict in
```

Related Commands

Command	Description
absolute	Specifies an absolute start and end time for a time range.
ip access-list	Defines an IP access list by name.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit (IP)	Sets conditions under which a packet passes a named IP access list.