



Configuring NTP

This chapter contains the following sections:

- [Information About NTP, on page 1](#)
- [NTP as Time Server, on page 2](#)
- [Distributing NTP Using CFS, on page 2](#)
- [Clock Manager, on page 2](#)
- [High Availability, on page 2](#)
- [Virtualization Support, on page 2](#)
- [Prerequisites for NTP, on page 3](#)
- [Guidelines and Limitations for NTP, on page 3](#)
- [Default Settings, on page 4](#)
- [Configuring NTP, on page 5](#)
- [Verifying the NTP Configuration, on page 17](#)
- [Configuration Examples for NTP, on page 18](#)

Information About NTP

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server, and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 time server.

Before synchronizing, NTP compares the time reported by several network devices and does not synchronize with one that is significantly different, even if it is a stratum 1. Because Cisco NX-OS cannot connect to a radio or atomic clock and act as a stratum 1 server, we recommend that you use the public NTP servers

available on the Internet. If the network is isolated from the Internet, Cisco NX-OS allows you to configure the time as though it were synchronized through NTP, even though it was not.



Note You can create NTP peer relationships to designate the time-serving hosts that you want your network device to consider synchronizing with and to keep accurate time if a server failure occurs.

The time kept on a device is a critical resource, so we strongly recommend that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

NTP as Time Server

Other devices can configure it as a time server. You can also configure the device to act as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an outside time source.

Distributing NTP Using CFS

Cisco Fabric Services (CFS) distributes the local NTP configuration to all Cisco devices in the network.

After enabling CFS on your device, a network-wide lock is applied to NTP whenever an NTP configuration is started. After making the NTP configuration changes, you can discard or commit them.

In either case, the CFS lock is then released from the NTP application.

Clock Manager

Clocks are resources that need to be shared across different processes.

Multiple time synchronization protocols, such as NTP and Precision Time Protocol (PTP), might be running in the system.

High Availability

Stateless restarts are supported for NTP. After a reboot or a supervisor switchover, the running configuration is applied.

You can configure NTP peers to provide redundancy in case an NTP server fails.

Virtualization Support

NTP recognizes virtual routing and forwarding (VRF) instances. NTP uses the default VRF if you do not configure a specific VRF for the NTP server and NTP peer.

Prerequisites for NTP

NTP has the following prerequisites:

- To configure NTP, you must have connectivity to at least one server that is running NTP.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- The **show ntp session status** CLI command does not show the last action time stamp, the last action, the last action result, and the last action failure reason.
- NTP server functionality is supported.
- You should have a peer association with another device only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as a backup. If you have two servers, you can configure several devices to point to one server and the remaining devices to point to the other server. You can then configure a peer association between these two servers to create a more reliable NTP configuration.
- If you have only one server, you should configure all the devices as clients to that server.
- You can configure up to 64 NTP entities (servers and peers).
- If CFS is disabled for NTP, NTP does not distribute any configuration and does not accept a distribution from other devices in the network.
- After CFS distribution is enabled for NTP, the entry of an NTP configuration command locks the network for NTP configuration until a **commit** command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the network except the device that initiated the lock.
- If you use CFS to distribute NTP, all devices in the network should have the same VRFs configured as you use for NTP.
- If you configure NTP in a VRF, ensure that the NTP server and peers can reach each other through the configured VRFs.
- You must manually distribute NTP authentication keys on the NTP server and Cisco NX-OS devices across the network.
- If you are using the switch as an edge device and want to use NTP, Cisco recommends using the **ntp access-group** command and filtering NTP only to the required edge devices.
- If the system has been configured with the **ntp passive**, **ntp broadcast client**, or **ntp multicast client** commands, when NTP receives an incoming symmetric active, broadcast, or multicast packet, it can set up an ephemeral peer association in order to synchronize with the sender.



Note Make sure that you specify **ntp authenticate** before enabling any of the above commands. Failure to do so will allow your device to synchronize with any device that sends one of the above packet types, including malicious attacker-controlled devices.

- If the **ntp authenticate** command is specified, when a symmetric active, broadcast, or multicast packet is received, the system does not synchronize to the peer unless the packet carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.
- To prevent synchronization with unauthorized network hosts, the **ntp authenticate** command should be specified any time the **ntp passive**, **ntp broadcast client**, or **ntp multicast client** command has been specified unless other measures, such as the **ntp access-group** command, have been taken to prevent unauthorized hosts from communicating with the NTP service on the device.
- The **ntp authenticate** command does not authenticate peer associations configured via the **ntp server** and **ntp peer** configuration commands. To authenticate the **ntp server** and **ntp peer** associations, specify the **key** keyword.
- Use NTP broadcast or multicast associations when time accuracy and reliability requirements are modest, your network is localized, and the network has more than 20 clients. We recommend that you use NTP broadcast or multicast associations in networks that have limited bandwidth, system memory, or CPU resources.
- A maximum of four ACLs can be configured for a single NTP access group.



Note Time accuracy is marginally reduced in NTP broadcast associations because information flows only one way.

Default Settings

The following are the default settings for NTP parameters.

Parameters	Default
NTP	Enabled for all interfaces
NTP passive (enabling NTP to form associations)	Enabled
NTP authentication	Disabled
NTP access	Enabled
NTP access group match all	Disabled
NTP broadcast server	Disabled
NTP multicast server	Disabled

Parameters	Default
NTP multicast client	Disabled
NTP logging	Disabled

Configuring NTP

Enabling or Disabling NTP on an Interface

You can enable or disable NTP on a particular interface. NTP is enabled on all interfaces by default.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Enters interface configuration mode.
Step 3	switch(config-if)# [no] ntp disable {ip ipv6}	Disables NTP IPv4 or IPv6 on the specified interface. Use the no form of this command to reenabling NTP on the interface.
Step 4	(Optional) switch(config-if)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

The following example shows how to enable or disable NTP on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp disable ip
switch(config-if)# copy running-config startup-config
```

Configuring the Device as an Authoritative NTP Server

You can configure the device to act as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an existing time server.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 2	<code>[no] ntp master [stratum]</code>	Configures the device as an authoritative NTP server. You can specify a different stratum level from which NTP clients get their time synchronized. The range is from 1 to 15.
Step 3	(Optional) <code>show running-config ntp</code>	Displays the NTP configuration.
Step 4	(Optional) <code>switch(config)# copy running-config startup-config</code>	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure the Cisco NX-OS device as an authoritative NTP server with a different stratum level:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp master 5
```

Configuring an NTP Server and Peer

You can configure an NTP server and peer.

Before you begin

Make sure that you know the IP address or DNS names of your NTP server and its peers.

Procedure

	Command or Action	Purpose
Step 1	<code>switch# configure terminal</code>	Enters global configuration mode.
Step 2	<code>switch(config)# [no] ntp server {ip-address ipv6-address dns-name} [key key-id] [maxpoll max-poll] [minpoll min-poll] [prefer] [use-vrf vrf-name]</code>	Forms an association with a server. Use the key keyword to configure a key to be used while communicating with the NTP server. The range for the <i>key-id</i> argument is from 1 to 65535. Use the maxpoll and minpoll keywords to configure the maximum and minimum intervals in which to poll a server. The range for the <i>max-poll</i> and <i>min-poll</i> arguments is from 4 to 16 (configured as powers of 2, so effectively 16 to 65536 seconds), and the default values

	Command or Action	Purpose
		<p>are 6 and 4, respectively (<i>maxpoll</i> default = 64 seconds, <i>minpoll</i> default = 16 seconds).</p> <p>Use the prefer keyword to make this the preferred NTP server for the device.</p> <p>Use the use-vrf keyword to configure the NTP server to communicate over the specified VRF.</p> <p>The <i>vrf-name</i> argument can be default, management, or any case-sensitive alphanumeric string up to 32 characters.</p> <p>Note If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.</p>
Step 3	<pre>switch(config)# [no] ntp peer {ip-address ipv6-address dns-name} [key key-id] [maxpoll max-poll] [minpoll min-poll] [prefer] [use-vrf vrf-name]</pre>	<p>Forms an association with a peer. You can specify multiple peer associations.</p> <p>Use the key keyword to configure a key to be used while communicating with the NTP peer. The range for the <i>key-id</i> argument is from 1 to 65535.</p> <p>Use the maxpoll and minpoll keywords to configure the maximum and minimum intervals in which to poll a server. The range for the <i>max-poll</i> and <i>min-poll</i> arguments is from 4 to 17 (configured as powers of 2, so effectively 16 to 131072 seconds), and the default values are 6 and 4, respectively (<i>maxpoll</i> default = 64 seconds, <i>minpoll</i> default = 16 seconds).</p> <p>Use the prefer keyword to make this the preferred NTP peer for the device.</p> <p>Use the use-vrf keyword to configure the NTP peer to communicate over the specified VRF. The <i>vrf-name</i> argument can be default, management, or any case-sensitive alphanumeric string up to 32 characters.</p>
Step 4	(Optional) switch(config)# show ntp peers	<p>Displays the configured server and peers.</p> <p>Note A domain name is resolved only when you have a DNS server configured.</p>
Step 5	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring NTP Authentication

You can configure the device to authenticate the time sources to which the local clock is synchronized. When you enable NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the **ntp trusted-key** command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.

Before you begin

Authentication for NTP servers and NTP peers is configured on a per-association basis using the **key** keyword on each **ntp server** and **ntp peer** command. Make sure that you configured all NTP server and peer associations with the authentication keys that you plan to specify in this procedure. Any **ntp server** or **ntp peer** commands that do not specify the **key** keyword will continue to operate without authentication.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	[no] ntp authentication-key number md5 md5-string Example: <pre>switch(config)# ntp authentication-key 42 md5 aNiceKey</pre>	Defines the authentication keys. The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the ntp trusted-key number command. The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters.
Step 3	ntp server ip-address key key-id Example: <pre>switch(config)# ntp server 192.0.2.1 key 1001</pre>	Enables authentication for the specified NTP server, forming an association with a server. Use the key keyword to configure a key to be used while communicating with the NTP server. The range for the <i>key-id</i> argument is from 1 to 65535. To require authentication, the key keyword must be used. Any ntp server or ntp peer commands that do not specify the key keyword will continue to operate without authentication.
Step 4	(Optional) show ntp authentication-keys Example: <pre>switch(config)# show ntp authentication-keys</pre>	Displays the configured NTP authentication keys.

	Command or Action	Purpose
Step 5	<code>[no] ntp trusted-key number</code> Example: <code>switch(config)# ntp trusted-key 42</code>	Specifies one or more keys (defined in Step 2) that an unconfigured remote symmetric, broadcast, and multicast time source must provide in its NTP packets in order for the device to synchronize to it. The range for trusted keys is from 1 to 65535. This command provides protection against accidentally synchronizing the device to a time source that is not trusted.
Step 6	(Optional) <code>show ntp trusted-keys</code> Example: <code>switch(config)# show ntp trusted-keys</code>	Displays the configured NTP trusted keys.
Step 7	<code>[no] ntp authenticate</code> Example: <code>switch(config)# ntp authenticate</code>	Enables or disables authentication for ntp passive, ntp broadcast client, and ntp multicast. NTP authentication is disabled by default.
Step 8	(Optional) <code>show ntp authentication-status</code> Example: <code>switch(config)# show ntp authentication-status</code>	Displays the status of NTP authentication.
Step 9	(Optional) <code>copy running-config startup-config</code> Example: <code>switch(config)# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Configuring NTP Access Restrictions

You can control access to NTP services by using access groups. Specifically, you can specify the types of requests that the device allows and the servers from which it accepts responses.

If you do not configure any access groups, NTP access is granted to all devices. If you configure any access groups, NTP access is granted only to the remote device whose source IP address passes the access list criteria.

Beginning with Cisco NX-OS Release 7.0(3)I7(3), access groups are evaluated in the following method:

- Without the **match-all** keyword, the packet gets evaluated against the access groups (in the order mentioned below) until it finds a permit. If a permit is not found, the packet is dropped.
- With **match-all** keyword, the packet gets evaluated against all the access groups (in the order mentioned below) and the action is taken based on the last successful evaluation (the last access group where an ACL is configured).

The mapping of the access group to the type of packet is as follows:

- peer—process client, symmetric active, symmetric passive, serve, control, and private packets(all types)

- **serve**—process client, control, and private packets
- **serve-only**—process client packets only
- **query-only**—process control and private packets only

The access groups are evaluated in the following descending order:

1. **peer** (all packet types)
2. **serve** (client, control, and private packets)
3. **query only** (client packets) or **query-only** (control and private packets)

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] ntp access-group match-all {peer serve serve-only query-only} access-list-name	<p>Creates or removes an access group to control NTP access and applies a basic IP access list.</p> <p>The access group options are scanned in the following order, from least restrictive to most restrictive. However, if NTP matches a deny ACL rule in a configured peer, ACL processing stops and does not continue to the next access group option.</p> <ul style="list-style-type: none"> • The peer keyword enables the device to receive time requests and NTP control queries and to synchronize itself to the servers specified in the access list. • The serve keyword enables the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers. • The serve-only keyword enables the device to receive only time requests from servers specified in the access list. • The query-only keyword enables the device to receive only NTP control queries from the servers specified in the access list. • The match-all keyword enables the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. If the incoming packet does not match the ACL in the peer access

	Command or Action	Purpose
		group, it goes to the serve access group to be processed. If the packet does not match the ACL in the serve access group, it goes to the serve-only access group, and so on. Note The match-all keyword is available beginning with Cisco NX-OS Release 7.0(3)I6(1).
Step 3	switch(config)# show ntp access-groups	(Optional) Displays the NTP access group configuration.
Step 4	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure the device to allow it to synchronize to a peer from access group "accesslist1":

```
switch# configure terminal
switch(config)# ntp access-group peer accesslist1
switch(config)# show ntp access-groups
Access List Type
-----
accesslist1 Peer
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

Configuring the NTP Source IP Address

NTP sets the source IP address for all NTP packets based on the address of the interface through which the NTP packets are sent. You can configure NTP to use a specific source IP address.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	[no] ntp source ip-address	Configures the source IP address for all NTP packets. The <i>ip-address</i> can be in IPv4 or IPv6 format.

Example

This example shows how to configure an NTP source IP address of 192.0.2.2.

```
switch# configure terminal
switch(config)# ntp source 192.0.2.2
```

Configuring the NTP Source Interface

You can configure NTP to use a specific interface.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	[no] ntp source-interface <i>interface</i>	Configures the source interface for all NTP packets. The following list contains the valid values for <i>interface</i> . <ul style="list-style-type: none"> • ethernet • loopback • mgmt • port-channel • vlan

Example

This example shows how to configure the NTP source interface:

```
switch# configure terminal
switch(config)# ntp source-interface ethernet
```

Configuring an NTP Broadcast Server

You can configure an NTP IPv4 broadcast server on an interface. The device then sends broadcast packets through that interface periodically. The client is not required to send a response.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Enters interface configuration mode.
Step 3	switch(config-if)# [no] ntp broadcast [destination <i>ip-address</i>] [key <i>key-id</i>] [<i>version number</i>]	Enables an NTP IPv4 broadcast server on the specified interface. <ul style="list-style-type: none"> • destination <i>ip-address</i>—Configures the broadcast destination IP address.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • key <i>key-id</i>—Configures the broadcast authentication key number. The range is from 1 to 65535. • <i>version number</i>—Configures the NTP version. The range is from 2 to 4.
Step 4	switch(config-if)# exit	Exits interface configuration mode.
Step 5	(Optional) switch(config)# [no] ntp broadcastdelay <i>delay</i>	Configures the estimated broadcast round-trip delay in microseconds. The range is from 1 to 999999.
Step 6	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure an NTP broadcast server:

```
switch# configure terminal
switch(config)# interface ethernet 6/1
switch(config-if)# ntp broadcast destination 192.0.2.10
switch(config-if)# exit
switch(config)# ntp broadcastdelay 100
switch(config)# copy running-config startup-config
```

Configuring an NTP Multicast Server

You can configure an NTP IPv4 or IPv6 multicast server on an interface. The device then sends multicast packets through that interface periodically.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Enters interface configuration mode.
Step 3	switch(config-if)# [no] ntp multicast <i>[ipv4-address ipv6-address] [key key-id] [ttl value] [version number]</i>	<p>Enables an NTP IPv4 or IPv6 multicast server on the specified interface.</p> <ul style="list-style-type: none"> • <i>ipv4-address</i> or <i>ipv6-address</i>— Multicast IPv4 or IPv6 address. • key <i>key-id</i>—Configures the broadcast authentication key number. The range is from 1 to 65535. • <i>ttl value</i>—Time-to-live value of the multicast packets. The range is from 1 to 255.

	Command or Action	Purpose
		<ul style="list-style-type: none"> <i>version number</i>—NTP version. The range is from 2 to 4.
Step 4	(Optional) switch(config-if)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure an Ethernet interface to send NTP multicast packets:

```
switch# configure terminal
switch(config)# interface ethernet 2/2
switch(config-if)# ntp multicast FF02::1:FF0E:8C6C
switch(config-if)# copy running-config startup-config
```

Configuring an NTP Multicast Client

You can configure an NTP multicast client on an interface. The device then listens to NTP multicast messages and discards any messages that come from an interface for which multicast is not configured.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface <i>type slot/port</i>	Enters interface configuration mode.
Step 3	switch(config-if)# [no] ntp multicast client [<i>ipv4-address</i> <i>ipv6-address</i>]	Enables the specified interface to receive NTP multicast packets.
Step 4	(Optional) switch(config-if)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure an Ethernet interface to receive NTP multicast packets:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ntp multicast client FF02::1:FF0E:8C6C
switch(config-if)# copy running-config startup-config
```

Configuring NTP Logging

You can configure NTP logging in order to generate system logs with significant NTP events. NTP logging is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] ntp logging	Enables or disables system logs to be generated with significant NTP events. NTP logging is disabled by default.
Step 3	(Optional) switch(config)# show ntp logging-status	Displays the NTP logging configuration status.
Step 4	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

The following example shows how to enable NTP logging in order to generate system logs with significant NTP events:

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

Enabling CFS Distribution for NTP

You can enable CFS distribution for NTP in order to distribute the NTP configuration to other CFS-enabled devices.

Before you begin

Make sure that you have enabled CFS distribution for the device.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] ntp distribute	Enables or disables the device to receive NTP configuration updates that are distributed through CFS.
Step 3	(Optional) switch(config)# show ntp status	Displays the NTP CFS distribution status.
Step 4	(Optional) switch(config)# copy running-config startup-config	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to enable the device to receive NTP configuration updates through CFS:

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# copy running-config startup-config
```

Committing NTP Configuration Changes

When you commit the NTP configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the devices in the network receive the same configuration.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# ntp commit	Distributes the NTP configuration changes to all Cisco NX-OS devices in the network and releases the CFS lock. This command overwrites the effective database with the changes made to the pending database.

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes instead of committing them. If you discard the changes, Cisco NX-OS removes the pending database changes and releases the CFS lock.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# ntp abort	Discards the NTP configuration changes in the pending database and releases the CFS lock. Use this command on the device where you started the NTP configuration.

Releasing the CFS Session Lock

If you have performed an NTP configuration and have forgotten to release the lock by either committing or discarding the changes, you or another administrator can release the lock from any device in the network. This action also discards pending database changes.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# clear ntp session	Discards the NTP configuration changes in the pending database and releases the CFS lock.

Verifying the NTP Configuration

Command	Purpose
show ntp access-groups	Displays the NTP access group configuration.
show ntp authentication-keys	Displays the configured NTP authentication keys.
show ntp authentication-status	Displays the status of NTP authentication.
show ntp logging-status	Displays the NTP logging status.
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peer	Displays all the NTP peers.
show ntp pending	Displays the temporary CFS database for NTP.
show ntp pending-diff	Displays the difference between the pending CFS database and the current NTP configuration.
show ntp rts-update	Displays the RTS update status.
show ntp session status	Displays the NTP CFS distribution session information.
show ntp source	Displays the configured NTP source IP address.
show ntp source-interface	Displays the configured NTP source interface.
show ntp statistics {io local memory peer {ipaddr {ipv4-addr} name peer-name}}	Displays the NTP statistics.
show ntp status	Displays the NTP CFS distribution status.
show ntp trusted-keys	Displays the configured NTP trusted keys.
show running-config ntp	Displays NTP information.

Configuration Examples for NTP

Configuration Examples for NTP

This example shows how to configure an NTP server and peer, enable NTP authentication, enable NTP logging, and then save the startup configuration so that it is saved across reboots and restarts:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 192.0.2.105
switch(config)# show ntp peers
-----
Peer IP Address Serv/Peer
-----
192.0.2.100 Peer (configured)
192.0.2.105 Server (configured)
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# show ntp authentication-keys
-----
Auth key MD5 String
-----
42 aNicekey
switch(config)# ntp trusted-key 42
switch(config)# show ntp trusted-keys
Trusted Keys:
42
switch(config)# ntp authenticate
switch(config)# show ntp authentication-status
Authentication enabled.
switch(config)# ntp logging
switch(config)# show ntp logging
NTP logging enabled.
switch(config)# copy running-config startup-config
[#####] 100%
switch(config)#
```

This example shows an NTP access group configuration with the following restrictions:

- Peer restrictions are applied to IP addresses that pass the criteria of the access list named “peer-acl.”
- Serve restrictions are applied to IP addresses that pass the criteria of the access list named “serve-acl.”
- Serve-only restrictions are applied to IP addresses that pass the criteria of the access list named “serve-only-acl.”
- Query-only restrictions are applied to IP addresses that pass the criteria of the access list named “query-only-acl.”

```
switch# configure terminal
switch(config)# ntp peer 10.1.1.1
switch(config)# ntp peer 10.2.2.2
switch(config)# ntp peer 10.3.3.3
switch(config)# ntp peer 10.4.4.4
switch(config)# ntp peer 10.5.5.5
switch(config)# ntp peer 10.6.6.6
switch(config)# ntp peer 10.7.7.7
switch(config)# ntp peer 10.8.8.8
```

```
switch(config)# ntp access-group peer peer-acl
switch(config)# ntp access-group serve serve-acl
switch(config)# ntp access-group serve-only serve-only-acl
switch(config)# ntp access-group query-only query-only-acl
switch(config)# ip access-list peer-acl
switch(config-acl)# 10 permit ip host 10.1.1.1 any
switch(config-acl)# 20 permit ip host 10.8.8.8 any
switch(config)# ip access-list serve-acl
switch(config-acl)# 10 permit ip host 10.4.4.4 any
switch(config-acl)# 20 permit ip host 10.5.5.5 any
switch(config)# ip access-list serve-only-acl
switch(config-acl)# 10 permit ip host 10.6.6.6 any
switch(config-acl)# 20 permit ip host 10.7.7.7 any
switch(config)# ip access-list query-only-acl
switch(config-acl)# 10 permit ip host 10.2.2.2 any
switch(config-acl)# 20 permit ip host 10.3.3.3 any
```

