CHAPTER 5

# Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on Cisco NX-OS devices.

This chapter includes the following sections:

- Information About NTP, page 5-63
- Licensing Requirements for NTP, page 5-65
- Prerequisites for NTP, page 5-65
- Guidelines and Limitations, page 5-65
- Default Settings, page 5-66
- Configuring NTP, page 5-66
- Verifying the NTP Configuration, page 5-79
- Configuration Examples for NTP, page 5-80
- Additional References, page 5-81
- Feature History for NTP, page 5-82

## Information About NTP

This section includes the following topics:

- NTP Overview, page 5-63
- NTP as Time Server, page 5-64
- Distributing NTP Using CFS, page 5-64
- Clock Manager, page 5-64
- High Availability, page 5-65
- Virtualization Support, page 5-65

### NTP Overview

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

Beginning with Cisco NX-OS Release 5.2, the Cisco NX-OS device can use NTP to distribute time. 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.

For more information about CFS, see the "Configuring CFS" section on page 1-1.

## Clock Manager

Clocks are resources that need to be shared across different processes and across different VDCs. Multiple time synchronization protocols, such as NTP and Precision Time Protocol (PTP), might be running in the system, and multiple instances of the same protocol might be running in different VDCs.

Beginning with Cisco NX-OS Release 5.2, the clock manager allows you to specify the protocol and a VDC running that protocol to control the various clocks in the system. Once you specify the protocol and VDC, the system clock starts updating. For information on configuring the clock manager, see the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*.

## High Availability

Stateless restarts are supported for NTP. After a reboot or a supervisor switchover, the running configuration is applied. For more information on high availability, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x.*

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

## Virtualization Support

If you are running a Cisco NX-OS Release prior to 5.2, up to one instance of NTP is supported on the entire platform. You must configure NTP in the default virtual device context (VDC), and you are automatically placed in the default VDC unless you specify otherwise.

If you are running Cisco NX-OS Release 5.2 or later, multiple instances of NTP are supported, one instance per VDC. By default, Cisco NX-OS places you in the default VDC unless you specifically configure another VDC.

Only one VDC (the default VDC by default) synchronizes the system clock at any given time. The NTP daemon in all other VDCs acts only as an NTP server for the other devices. To change which VDC synchronizes the system clock, use the **clock protocol ntp vdc** *vdc-id* command.

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. See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x* for more information about VRFs.

For more information about VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x.*

# Licensing Requirements for NTP

| Product | License Requirement |
|---|---|
| Cisco NX-OS | NTP requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*. |

# Prerequisites for NTP

NTP has the following prerequisites:

- To configure NTP, you must have connectivity to at least one server that is running NTP.
- To configure VDCs, you must install the Advanced Services license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x.*

# Guidelines and Limitations

NTP has the following configuration guidelines and limitations:

- NTP server functionality is supported starting in Cisco NX-OS Release 5.2.
- 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, then 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.

# Default Settings

Table 5-1 lists the default settings for NTP parameters.

*Table 5-1 Default NTP Parameters*

| Parameters | Default |
|---|---|
| NTP | Enabled in all VDCs |
| NTP authentication | Disabled |
| NTP access | Enabled |
| NTP logging | Disabled |

# Configuring NTP

This section includes the following topics:

- Enabling or Disabling NTP, page 5-67
- Configuring the Device as an Authoritative NTP Server, page 5-68
- Configuring an NTP Server and Peer, page 5-69
- Configuring NTP Authentication, page 5-72
- Configuring NTP Access Restrictions, page 5-73

- Configuring the NTP Source IP Address, page 5-75
- Configuring the NTP Source Interface, page 5-75
- Configuring NTP on a Secondary (Non-Default) VDC, page 5-75
- Configuring NTP Logging, page 5-76
- Enabling CFS Distribution for NTP, page 5-77
- Committing NTP Configuration Changes, page 5-78
- Discarding NTP Configuration Changes, page 5-79
- Releasing the CFS Session Lock, page 5-79

**Note** Be aware that the Cisco NX-OS commands for this feature may differ from those commands used in Cisco IOS.

## Enabling or Disabling NTP

You can enable or disable NTP in a particular VDC. NTP is enabled in all VDCs by default.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

### SUMMARY STEPS

1. **config t**
2. **[no] feature ntp**
3. (Optional) **show ntp status**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **`config t`**<br>**Example:**<br>`switch# config t`<br>`Enter configuration commands, one per line.  End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | `[no]` **`feature ntp`**<br>**Example:**<br>`switch(config)# feature ntp` | Enables or disables NTP in a particular VDC. NTP is enabled by default.<br>**Note** If you are running a Cisco NX-OS Release prior to 5.2, NTP is enabled or disabled using the [**no**] **ntp enable** command. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | **show ntp status**<br><br>**Example:**<br>switch(config)# show ntp status<br>Distribution: Enabled<br>Last operational state: Fabric Locked | (Optional) Displays the status of the NTP application. |
| **Step 4** | **copy running-config startup-config**<br><br>**Example:**<br>switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to disable NTP:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no feature ntp
```

# 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.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

### SUMMARY STEPS

1. **config t**
2. **[no] ntp master** [*stratum*]
3. (Optional) **show running-config ntp**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>switch# config t<br>Enter configuration commands, one per line.  End with CNTL/Z.<br>switch(config)# | Places you in global configuration mode. |
| **Step 2** | [no] **ntp master** [*stratum*]<br><br>**Example:**<br>switch(config)# ntp master | Configures the device as an authoritative NTP server.<br>You can specify a different stratum level from which NTP clients get their time synchronized. The range is from 1 to 15. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | **show running-config ntp**<br>**Example:**<br>`switch(config)# show running-config ntp` | (Optional) Displays the NTP configuration. |
| **Step 4** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

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

```
switch# config t
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 are in the correct VDC. To change the VDC, use the **switchto vdc** command.

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

If you plan to use CFS to distribute your NTP configuration to other devices, then you should have already completed the following:

- Enabled CFS distribution using the "Configuring CFS Distribution" section on page 1-6.
- Enabled CFS for NTP using the "Enabling CFS Distribution for NTP" section on page 5-77.

### SUMMARY STEPS

1. **config t**
2. [**no**] **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
3. [**no**] **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]
4. (Optional) **show ntp peers**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **`config t`**<br><br>**`Example:`**<br>`switch# config t`<br>`Enter configuration commands, one per line.`<br>`End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | [**no**] **ntp server** {*ip-address* \| *ipv6-address* \| *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]<br><br>**`Example:`**<br>`switch(config)# ntp server 192.0.2.10` | Forms an association with a server.<br>Use the **key** keyword to configure a key to be used while communicating with the NTP server. The range for the *key-id* argument is from 1 to 65535.<br>Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a peer. The range for the *max-poll* and *min-poll* arguments is from 4 to 16 seconds, and the default values are 6 and 4, respectively.<br>Use the **prefer** keyword to make this the preferred NTP server for the device.<br>Use the **use-vrf** keyword to configure the NTP server to communicate over the specified VRF. The *vrf-name* argument can be **default**, **management**, or any case-sensitive alphanumeric string up to 32 characters.<br>**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. For more information on trusted keys, see the "Configuring NTP Authentication" section on page 5-72. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | [**no**] **ntp peer** {*ip-address* \| *ipv6-address* \| *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**] [**use-vrf** *vrf-name*]<br>**Example:**<br>switch(config)# ntp peer 2001:0db8::4101 | Forms an association with a peer. You can specify multiple peer associations.<br>Use the **key** keyword to configure a key to be used while communicating with the NTP peer. The range for the *key-id* argument is from 1 to 65535.<br>Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a peer. The range for the *max-poll* and *min-poll* arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively.<br>Use the **prefer** keyword to make this the preferred NTP peer for the device.<br>Use the **use-vrf** keyword to configure the NTP peer to communicate over the specified VRF. The *vrf-name* argument can be **default**, **management**, or any case-sensitive alphanumeric string up to 32 characters. |
| **Step 4** | **show ntp peers**<br>**Example:**<br>switch(config)# show ntp peers | (Optional) Displays the configured server and peers.<br>**Note** A domain name is resolved only when you have a DNS server configured. |
| **Step 5** | **copy running-config startup-config**<br>**Example:**<br>switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to configure an NTP server and peer:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 192.0.2.10 key 10 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 prefer use-vrf Red
switch(config)# show ntp peers
--------------------------------------------------
  Peer IP Address               Serv/Peer
--------------------------------------------------
  2001:0db8::4101                Peer (configured)
  192.0.2.10                   Server (configured)
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

# 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

Make sure that you configured the NTP server with the authentication keys that you plan to specify in this procedure. See the "Configuring an NTP Server and Peer" section on page 5-69 for information.

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

## SUMMARY STEPS

1. **config t**
2. [**no**] **ntp authentication-key** *number* **md5** *md5-string*
3. (Optional) **show ntp authentication-keys**
4. [**no**] **ntp trusted-key** *number*
5. (Optional) **show ntp trusted-keys**
6. [**no**] **ntp authenticate**
7. (Optional) **show ntp authentication-status**
8. (Optional) **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | `config t`<br>**Example:**<br>`switch# config t`<br>`Enter configuration commands, one per line.`<br>`End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | [**no**] **ntp authentication-key** *number* **md5** *md5-string*<br>`switch(config)# ntp authentication-key 42 md5 aNiceKey` | 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.<br>The range for authentication keys is from 1 to 65535. Cisco NX-OS Release 5.2(3) and later 5.x releases support up to 15 alphanumeric characters for the MD5 string. Earlier releases support up to 8 alphanumeric characters. |

| | Command | Purpose |
|---|---|---|
| **Step 3** | **show ntp authentication-keys**<br>**Example:**<br>`switch(config)# show ntp authentication-keys` | (Optional) Displays the configured NTP authentication keys. |
| **Step 4** | [no] **ntp trusted-key** *number*<br>**Example:**<br>`switch(config)# ntp trusted-key 42` | Specifies one or more keys (defined in Step 2) that a 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.<br>This command provides protection against accidentally synchronizing the device to a time source that is not trusted. |
| **Step 5** | **show ntp trusted-keys**<br>**Example:**<br>`switch(config)# show ntp trusted-keys` | (Optional) Displays the configured NTP trusted keys. |
| **Step 6** | [no] **ntp authenticate**<br>**Example:**<br>`switch(config)# ntp authenticate` | Enables or disables the NTP authentication feature. NTP authentication is disabled by default. |
| **Step 7** | **show ntp authentication-status**<br>**Example:**<br>`switch(config)# show ntp authentication-status` | (Optional) Displays the status of NTP authentication. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to configure the device to synchronize only to time sources that provide authentication key 42 in their NTP packets:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

# 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.

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

## SUMMARY STEPS

1. **config t**
2. [**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name*
3. (Optional) **show ntp access-groups**
4. (Optional) **copy running-config startup-config**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **`config t`**<br><br>**`Example:`**<br>`switch# config t`<br>`Enter configuration commands, one per line.`<br>`End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | `[no]` **`ntp access-group`** `{`**`peer`** `\|` **`serve`** `\|`<br>**`serve-only`** `\|` **`query-only`**`}` *`access-list-name`*<br><br>**`Example:`**<br>`switch(config)# ntp access-group peer`<br>`accesslist1` | Creates or removes an access group to control NTP access and applies a basic IP access list.<br><br>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.<br><br>• 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.<br><br>• 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.<br><br>• The **serve-only** keyword enables the device to receive only time requests from servers specified in the access list.<br><br>• The **query-only** keyword enables the device to receive only NTP control queries from the servers specified in the access list. |
| **Step 3** | **`show ntp access-groups`**<br><br>**`Example:`**<br>`switch(config)# show ntp access-groups` | (Optional) Displays the NTP access group configuration. |
| **Step 4** | **`copy running-config startup-config`**<br><br>**`Example:`**<br>`switch(config)# copy running-config`<br>`startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

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

```
switch# config t
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.

To configure the NTP source IP address, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `[no] ntp source ip-address`<br>**Example:**<br>`switch(config)# ntp source 192.0.2.1` | Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format. |

# Configuring the NTP Source Interface

You can configure NTP to use a specific interface.

To configure the NTP source interface, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| `[no] ntp source-interface interface`<br>**Example:**<br>`switch(config)# ntp source-interface ethernet 2/1` | Configures the source interface for all NTP packets. Use the **?** keyword to display a list of supported interfaces. |

# Configuring NTP on a Secondary (Non-Default) VDC

You can configure a non-default VDC to get a timing update from the default VDC and its clients in order to synchronize with it.

## BEFORE YOU BEGIN

Use the **switchto vdc** command to switch to the desired non-default VDC.

### SUMMARY STEPS

1. **config t**
2. **feature ntp**
3. **ntp master**
4. (Optional) **ntp source-interface** *interface*
5. (Optional) **ntp source** *ip-address*
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **`config t`**<br>**`Example:`**<br>`switch# config t`<br>`Enter configuration commands, one per line.`<br>`End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | **`feature ntp`**<br>**`Example:`**<br>`switch(config)# feature ntp` | Enables NTP in the non-default VDC. |
| **Step 3** | **`ntp master`**<br>**`Example:`**<br>`switch(config)# ntp master` | Configures the device as an authoritative NTP server. |
| **Step 4** | **`ntp source-interface`** *`interface`*<br>**`Example`**`:`<br>`switch(config)# ntp source-interface ethernet 2/1` | (Optional) Configures the source interface for all NTP packets. Use the **?** keyword to display a list of supported interfaces. |
| **Step 5** | **`ntp source`** *`ip-address`*<br>**`Example`**`:`<br>`switch(config)# ntp source 192.0.2.1` | (Optional) Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format. |
| **Step 6** | **`copy running-config startup-config`**<br>**`Example:`**<br>`switch(config)# copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

# Configuring NTP Logging

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

### BEFORE YOU BEGIN

Make sure that you are in the correct VDC. To change the VDC, use the **switchto vdc** command.

### SUMMARY STEPS

1. **config t**
2. [**no**] **ntp logging**
3. (Optional) **show ntp logging-status**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **config t**<br><br>**Example:**<br>switch# config t<br>Enter configuration commands, one per line.<br>End with CNTL/Z.<br>switch(config)# | Places you in global configuration mode. |
| **Step 2** | [no] **ntp logging**<br><br>**Example:**<br>switch(config)# ntp logging | Enables or disables system logs to be generated with significant NTP events. NTP logging is disabled by default. |
| **Step 3** | **show ntp logging-status**<br><br>**Example:**<br>switch(config)# show ntp logging-status | (Optional) Displays the NTP logging configuration status. |
| **Step 4** | **copy running-config startup-config**<br><br>**Example:**<br>switch(config)# copy running-config<br>startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

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

```
switch# config t
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 using the "Configuring CFS Distribution" section on page 1-6.

### SUMMARY STEPS

1. **config t**
2. [no] **ntp distribute**
3. (Optional) **show ntp status**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **`config t`**<br><br>**Example:**<br>`switch# config t`<br>`Enter configuration commands, one per line.  End with CNTL/Z.`<br>`switch(config)#` | Places you in global configuration mode. |
| **Step 2** | `[no]` **`ntp distribute`**<br><br>**Example:**<br>`switch(config)# ntp distribute` | Enables or disables the device to receive NTP configuration updates that are distributed through CFS. |
| **Step 3** | **`show ntp status`**<br><br>**Example:**<br>`switch(config)# show ntp status` | (Optional) Displays the NTP CFS distribution status. |
| **Step 4** | **`copy running-config startup-config`**<br><br>**Example:**<br>`switch(config)# copy running-config startup-config` | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

# 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.

To commit the NTP configuration changes, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| **`ntp commit`**<br><br>**Example:**<br>`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.

To discard NTP configuration changes, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| **ntp abort**<br>**Example:**<br>`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.

To release the session lock from any device and discard any pending database changes, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| **clear ntp session**<br>**Example:**<br>`switch(config)# clear ntp session` | Discards the NTP configuration changes in the pending database and releases the CFS lock. |

# Verifying the NTP Configuration

To display the NTP configuration, perform one of the following tasks:

| 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 internal** | Displays internal NTP information. |
| **show ntp logging-status** | Displays the NTP logging status. |
| **show ntp peer-status** | Displays the status for all NTP servers and peers. |
| **show ntp peers** | 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. |

| Command | Purpose |
|---|---|
| **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* \| *ipv6-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. |

Use the **clear ntp session** command to clear the NTP sessions.

Use the **clear ntp statistics** command to clear the NTP statistics.

# 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 configuration in startup so that it is saved across reboots and restarts:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp peer 2001:0db8::4101
switch(config)# show ntp peers
--------------------------------------------------
  Peer IP Address               Serv/Peer
--------------------------------------------------
  2001:db8::4101                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# config t
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
```

# Additional References

For additional information related to implementing NTP, see the following sections:

- Related Documents, page 5-82
- MIBs, page 5-82

## Related Documents

| Related Topic | Document Title |
|---|---|
| NTP CLI commands | *Cisco Nexus 7000 Series NX-OS System Management Command Reference* |
| Clock manager | *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x* |
| VDCs and VRFs | *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x* |

## MIBs

| MIBs | MIBs Link |
|---|---|
| • CISCO-NTP-MIB | To locate and download MIBs, go to the following URL:<br>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

# Feature History for NTP

Table 5-2 lists the release history for this feature.

*Table 5-2 Feature History for NTP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| NTP | 5.2(3) | Increased the length of NTP authentication keys from 8 to 15 alphanumeric characters. |
| NTP | 5.2(1) | Added NTP support for all VDCs, enabling them to act as time servers. See the "Virtualization Support" section on page 5-65. |
| NTP | 5.2(1) | Changed the command to enable or disable NTP from [**no**] **ntp enable** to [**no**] **feature ntp**. See the "Enabling or Disabling NTP" section on page 5-67. |
| NTP | 5.2(1) | Added the ability to configure the device as an authoritative NTP server, enabling it to distribute time even when it is not synchronized to an existing time server. See the "Configuring the Device as an Authoritative NTP Server" section on page 5-68. |
| NTP access groups | 5.2(1) | Added the **serve**, **serve-only**, and **query-only** access group options to control access to additional NTP services. See the "Configuring NTP Access Restrictions" section on page 5-73. |
| NTP | 5.1(1) | No change from Release 5.0. |
| NTP access groups | 5.0(2) | Added the ability to control access to NTP services by using access groups. See the "Configuring NTP Access Restrictions" section on page 5-73. |

*Table 5-2 Feature History for NTP (continued)*

| Feature Name | Releases | Feature Information |
|---|---|---|
| NTP authentication | 5.0(2) | Added the ability to enable or disable NTP authentication. See the "Configuring NTP Authentication" section on page 5-72. |
| NTP logging | 5.0(2) | Added the ability to enable or disable NTP logging. See the "Configuring NTP Logging" section on page 5-76. |
| NTP server configuration | 5.0(2) | Added the optional **key** keyword to the **ntp server** command to configure a key to be used while communicating with the NTP server. See the "Configuring an NTP Server and Peer" section on page 5-69. |
| CFS support | 4.2(1) | Added the ability to distribute NTP configuration using CFS. See the "Enabling CFS Distribution for NTP" section on page 5-77. |
| NTP source IP address or interface | 4.1(3) | Added the ability set the source IP address or source interface that NTP includes in all NTP packets sent to peers. |
| NTP | 4.0(3) | Added the ability to disable NTP.<br>See the "Enabling or Disabling NTP" section on page 5-67. |