CHAPTER 3

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 3-1
- Licensing Requirements for NTP, page 3-3
- Prerequisites for NTP, page 3-3
- Guidelines and Limitations, page 3-3
- Configuring NTP, page 3-3
- Verifying NTP Configuration, page 3-10
- NTP Example Configuration, page 3-11
- Default Settings, page 3-11
- Additional References, page 3-11
- Feature History for NTP, page 3-12

Information About NTP

This section includes the following topics:

- NTP Overview, page 3-1
- Distributing NTP Using CFS, page 3-2
- High Availability, page 3-2
- Virtualization Support, page 3-2

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. With the User Datagram Protocol (UDP) as its transport protocol, NTP uses standard Universal Time Coordinated (UTC).

An NTP server usually receives its time from a 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 an atomic clock).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 NTP 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 networking device to consider synchronizing with and to keep accurate time if a server failure occurs.

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 2-1.

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*.

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

Virtualization Support

Up to one instance of NTP is supported on the entire platform. You must configure NTP in the default VDC. You are automatically placed in the default VDC unless you specify otherwise. For more information about VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*.

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 4.x* for more information about VRFs.

Licensing Requirements for NTP

Product	License Requirement
NX-OS	NTP requires no license and is bundled with the Cisco NX-OS system images at no extra charge to you. For a complete explanation of the 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.
- NTP must be configured in the default VDC. It cannot be configured in any other VDC except the default VDC.
- To configure VDCs, you must install the Advanced Services license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*.

Guidelines and Limitations

NTP has the following configuration guidelines and limitations:

- NTP server functionality is not supported in Cisco NX-OS Release 4.2.
- 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 only have 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, then 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 the NTP server and peers can reach each other through the configured VRFs.

Configuring NTP

This section includes the following topics:

- Enabling or Disabling the NTP Protocol, page 3-4
- Configuring an NTP Server and Peer, page 3-5
- Configuring the NTP Source IP Address, page 3-7
- Configuring the NTP Source Interface, page 3-7
- Configuring NTP on a Secondary (Non-Default) VDC, page 3-7
- Enabling CFS Distribution for NTP, page 3-8
- Committing NTP Configuration Changes, page 3-9
- Discarding NTP Configuration Changes, page 3-9
- Releasing CFS Session Lock, page 3-10

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

Enabling or Disabling the NTP Protocol

You can enable or disable NTP. NTP is enabled by default. You can disable NTP and then reenable it.

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 enable**
3. **show ntp status**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Places you in global configuration mode.

Step 2	**[no] ntp enable** **Example:** `switch(config)# ntp enable`	Enables or disables the NTP protocol on the entire device. NTP is enabled by default.

	Command	Purpose

Step 3	**show ntp status**
	
	Example:
	`switch(config)# show ntp status`
	`Distribution : Enabled`
	`Last operational state: Fabric Locked`
		(Optional) Displays the status of the NTP application.

Step 4	**copy running-config startup-config** **Example:** `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 ntp enable
```

Configuring an NTP Server and Peer

You can configure an NTP server and peer. You need to know the IP address or DNS names of your NTP server and its peers.

BEFORE YOU BEGIN

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

- If you plan to use CFS to distribute your NTP configuration to other devices, then you should have already completed the following:
  - Enable CFS distribution using the "Configuring CFS Distribution" section on page 2-5.
  - Enable CFS for NTP using the "Enabling CFS Distribution for NTP" section on page 3-8.

SUMMARY STEPS

1. **config t**
2. **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**prefer**] [**use-vrf** *vrf-name*]
3. **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**prefer**] [**use-vrf** *vrf-name*]
4. **show ntp peers**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	Places you in global configuration mode.
Step 2	**ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**prefer**] [**use-vrf** *vrf-name*] **Example:** switch(config)# ntp server 192.0.2.10	Forms an association with a server. Optionally configures the NTP server to communicate over the specified VRF. The *vrf-name* can be any case-sensitive alphanumeric string up to 64 characters. Optionally use the **pefer** keyword to make this the preferred NTP server for the device.
Step 3	**ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**prefer**] [**use-vrf** *vrf-name*] switch(config)# ntp peer 2001:0db8::4101	Forms an association with a peer. You can specify multiple peer associations. Optionally configures the NTP peer to communicate over the specified VRF. Optionally use the **pefer** keyword to make this the preferred NTP peer for the device. The *vrf-name* can be any case-sensitive alphanumeric string up to 64 characters.
Step 4	**show ntp peers** **Example:** switch(config)# show ntp peers	(Optional) Displays the configured server and peers. **Note** A domain name is resolved only when you have a DNS server configured.
Step 5	**copy running-config startup-config** **Example:** 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 192.0.2.105 use-vrf Red
switch(config)# ntp peer 2001:0db8::4101 use-vrf Red
switch(config)# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  2001:db8::4101                Peer (configured)
  192.0.2.105                   Server (configured)
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 packet 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
ntp source *ip-address* **Example**: `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
ntp source-interface *interf* **Example**: `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** **Example:** switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	Places you in global configuration mode.
Step 2	**feature ntp** **Example:** switch(config)# feature ntp	Enables NTP in the non-default VDC.
Step 3	**ntp master** **Example:** switch(config)# ntp master	Configures the device as an authoritative NTP server.
Step 4	**ntp source-interface** *interface* **Example:** 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* **Example:** 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** **Example:** 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.

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

- You have already enabled CFS distribution for the device using the "Configuring CFS Distribution" section on page 2-5.

SUMMARY STEPS

1. **configure terminal**
2. **ntp distribute**
3. **show ntp status**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal** **Example:** switch# configure terminal switch(config)#	Places you into CLI Global Configuration mode.
Step 2	switch(config)# **ntp distribute** **Example:** switch(config)# ntp distribute	Enables the device to receive NTP configuration updates that are distributed through CFS.
Step 3	**show ntp status** **Example:** switch(config)# show ntp status	(Optional) Displays the NTP CFS distribution status.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy run start [####################################] 100% switch(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 **Example**: switch(config)# ntp commit switch(config)#	Distributes the NTP configuration changes to all switches in the network and releases the CFS lock. 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 **Example:** `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 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 will also discard 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 **Example:** `switch(config)# clear ntp session`	Discards the NTP configuration changes in the pending database and releases the CFS lock..

Verifying NTP Configuration

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

Command	Purpose
show ntp peer-status	Displays the status for all NTP servers and peers.
show ntp peers	Displays all the NTP peers.
show ntp pending peers	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 session status	Displays the NTP CFS distribution session information
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

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

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

NTP Example Configuration

This example shows how to configure an NTP server and peer 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
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)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Default Settings

Table 3-1 lists the default settings for NTP parameters.

Table 3-1 Default NTP Parameters

Parameters	Default
NTP	Enabled

Additional References

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

- Related Documents, page 3-11
- MIBs, page 3-12

Related Documents

Related Topic	Document Title
NTP CLI commands	*Cisco Nexus 7000 Series NX-OS System Management Command Reference*
VDCs and VRFs	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.x*

MIBs

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

Feature History for NTP

Table 3-2 lists the release history for this feature.

Table 3-2 Feature History for NTP

Feature Name	Releases	Feature Information
CFS support	4.2(1)	Added ability to distribute NTP configuration using CFS. See the "Enabling CFS Distribution for NTP" section on page 3-8.
NTP source IP address or interface	4.1(3)	Added ability set the source IP address or source interface that NTP includes in all NTP packets sent to peers.
NTP protocol	4.0(3)	Added ability to disable the NTP protocol. See the "Enabling or Disabling the NTP Protocol" section on page 3-4.