Configuring NTP

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

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

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 Associations

An NTP association can be one of the following:

- A peer association—The device can either synchronize to another device or allow another device to synchronize to it.
- A server association—The device synchronizes to a server.

You need to configure only one end of an association. The other device can automatically establish the association.

NTP Broadcast Associations

In a broadcast-based NTP association, an NTP server sends NTP broadcast packets throughout a network. Broadcast clients listen for the NTP broadcast packets sent by the server and do not engage in any polling.

NTP broadcast servers allow you to synchronize a large number of clients without creating a lot of NTP traffic because unsolicited messages are sent to a designated IPv4 local broadcast address, and ordinarily no request is expected from the clients.

NTP Multicast Associations

When the device operates as an NTP multicast server, it sends NTP multicast messages to a designated IPv4 or IPv6 multicast group IP address.

When the device operates as an NTP multicast client, it listens for NTP multicast packets that are sent by an NTP multicast server to a designated IPv4 or IPv6 multicast group IP address.

NTP multicast servers allow you to synchronize a large number of clients without creating a lot of NTP traffic because unsolicited messages are sent to a designated multicast group address, and ordinarily no request is expected from the clients.

NTP as a Time Server

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.

Clock Manager

Clocks are resources that need to be shared across different processes. Multiple time synchronization protocols, such as NTP, might be running in the system.

The clock manager allows you to specify the protocol to control the various clocks in the system. Once you specify the protocol, the system clock starts updating. For information on configuring the clock manager, see the *Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*.

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

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* for more information about VRFs.

For more information about VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration 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 appropriate license. See the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* for configuration information and the *Cisco NX-OS Licensing Guide* for licensing information.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- The Cisco NX-OS software supports NTP version 4 (NTPv4).
- 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.
- We recommend that you do not configure (just) two NTP servers. Instead, you should configure one, three, or four or more NTP servers.

  All NTP servers return the time together with an estimate of the current error. When using multiple time servers, NTP also wants these servers to agree on some time, meaning there must be one error interval where the correct time must be. When there are just two NTP servers, there might be an issue if both sources do not fall into the small common range because the NTP client will be unable to determine which source is more correct.
- You can configure up to 64 NTP entities (servers and peers).
- 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 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.
- 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.

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

- The NTP source-interface and source configuration has a limitation of getting applied only when configured on the client. If the configuration is done on the server (the switch with the NTP master), source address of the outgoing packet will still be that of the received destination address.

Default Settings for NTP

The following table lists the default settings for NTP parameters.

Parameters	Default
NTP	Enabled in all VDCs and for all interfaces. By default, NTP is enabled as server and client.
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
NTP multicast client	Disabled
NTP logging	Disabled

Configuring NTP

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 in a VDC

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature ntp** **Example:** `switch(config)# feature ntp`	Enables or disables NTP.

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

Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Enabling or Disabling NTP on an Interface

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

Procedure

	Command or Action	Purpose

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

Step 2	**interface***type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

	Command or Action	Purpose

Step 3	(Optional) [**no**]**ntp disable**{**ip** | **ipv6**}
	Example:
	`switch(config-if)# ntp disable ip`
		Disables NTP IPv4 or IPv6 on the specified interface. Use the no form of this command to reenable NTP on the interface.

Step 4	(Optional) **copy running-config startup-config** **Example:** `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 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	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp master** [*stratum*] **Example:** `switch(config)# ntp master`	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) **show running-config ntp** **Example:** `switch(config)# show running-config ntp`	Displays the NTP configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring an NTP Server and Peer

You can configure an NTP server and peer.

Before you begin

Make sure you know the IP address or Domain Name System (DNS) names of your NTP server and its peers.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters 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*] **Example:** `switch(config)# ntp server 192.0.2.10`	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 *key-id* 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 *max-poll* and *min-poll* arguments is from 4 to 16 seconds, and the default values are 6 and 4, respectively. Use the **prefer** keyword to make this server the preferred NTP server for the device. 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. **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.
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*] **Example:** `switch(config)# ntp peer 2001:0db8::4101`	Forms an association with a peer. You can specify multiple peer associations. 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. 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. Use the **prefer** keyword to make this peer the preferred NTP peer for the device.

	Command or Action	Purpose
		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	(Optional) **show ntp peers** **Example:** `switch(config)# show ntp peers`	Displays the configured server and peers. **Note** A domain name is resolved only when you have a DNS server configured.
Step 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies 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. 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:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp authentication-key** *number* **md5** *md5-string* **Example:** `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. The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters.

	Command or Action	Purpose
		Beginning with Cisco NX-OS Release 7.3(0)D1(1), you can enter up to 32 alphanumeric characters for the MD5 string.
Step 3	(Optional) **show ntp authentication-keys** **Example:** `switch(config)# show ntp authentication-keys`	Displays the configured NTP authentication keys.

Step 4	[**no**] **ntp trusted-key** *number*
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)# ntp authentication-key 42 md5 aNiceKey`
	`switch(config)# ntp server 10.1.1.1 key 42`
	`switch(config)# ntp trusted-key 42`
	`switch(config)# ntp authenticate`
	`switch(config)# copy running-config startup-config`
	`[########################################] 100%`
	`switch(config)#`
		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.
		This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

Step 5	(Optional) **show ntp trusted-keys** **Example:** `switch(config)# show ntp trusted-keys`	Displays the configured NTP trusted keys.
Step 6	[**no**] **ntp authenticate** **Example:** `switch(config)# ntp authenticate`	Enables or disables the NTP authentication feature. NTP authentication is disabled by default.
Step 7	(Optional) **show ntp authentication-status** **Example:** `switch(config)# show ntp authentication-status`	Displays the status of NTP authentication.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp access-group** {**peer** | **serve** | **serve-only** | **query-only**} *access-list-name* **Example:** `switch(config)# ntp access-group peer accesslist1`	Creates or removes an access group to control NTP access and applies a basic IP access list. ACL processing stops and does not continue to the next access group option if NTP matches a deny ACL rule in a configured peer. • 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.
Step 3	(Optional) **show ntp access-groups** **Example:** `switch(config)# show ntp access-groups`	Displays the NTP access group configuration.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **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.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the NTP Source Interface

You can configure NTP to use a specific interface.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp source-interface** *interface* **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.
Step 3	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

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.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC.

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp broadcast** [**destination** *ip-address*] [**key** *key-id*] [**version** *number*] **Example:** `switch(config-if)# ntp broadcast destination 192.0.2.10`	Enables an NTP IPv4 broadcast server on the specified interface. • destination *ip-address*—Configures the broadcast destination IP address. • key *key-id*—Configures the broadcast authentication key number. The range is from 1 to 65535. • version *number*—Configures the NTP version. The range is from 2 to 4.

Step 4	Required: **exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits interface configuration mode.

Step 5	(Optional) [**no**] **ntp broadcastdelay** *delay* **Example:** `switch(config)# ntp broadcastdelay 100`	(Optional) Configures the estimated broadcast round-trip delay in microseconds. The range is from 1 to 999999.
Step 6	(Optional) **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.

Example

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

```
switch# configure terminal
switch(config)# interface ethernet6/1
switch(config-if)# ntp broadcast 192.0.2.10
```

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.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC.

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp multicast** [*ipv4-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*] **Example:** `switch(config-if)# ntp multicast FF02:1::FF0E:8C6C`	Enables an NTP IPv6 broadcast server on the specified interface. • destination *ip-address*—Configures the broadcast destination IP address. • key *key-id*—Configures the broadcast authentication key number. The range is from 1 to 65535. • ttl *value*—The time-to-live value of the multicast packets. The range is from 1 to 255. • version *number*—Configures the NTP version. **Note** For an IPv4 multicast server, the range is from 2 to 4.

	Command or Action	Purpose
Step 4	(Optional) **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.

Example

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

```
switch# configure terminal
switch(config)# interface ethernet2/2
switch(config-if)# ntp multicast FF02::1:FF0E:8C6C
```

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.

Before you begin

Use the **switchto vdc** command to switch to the desired nondefault VDC

Procedure

	Command or Action	Purpose

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

Step 2	**interface** *type slot/port*
	Example:
	`switch(config)# interface ethernet 6/1`
	`switch(config-if)#`
		Enters interface configuration mode.

Step 3	Required: [**no**] **ntp multicast client** [*ipv4-address* | *ipv6-address*] **Example:** `switch(config-if)# ntp multicast FF02:1::FF0E:8C6C`	Enables an NTP IPv6 broadcast server on the specified interface.
Step 4	(Optional) **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.

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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature ntp**	Enables NTP in the non-default VDC.
Step 3	switch(config)# **ntp master**	Configures the device as an authoritative NTP server.
Step 4	(Optional) switch(config)# **ntp source-interface** *interface*	Configures the source interface for all NTP packets. The following list contains the valid values for *interface*. • ethernet • loopback • mgmt • port-channel • vlan
Step 5	(Optional) [**no**] **ntp source** *ip-address*	Configures the source IP address for all NTP packets. The *ip-address* can be in IPv4 or IPv6 format.
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 examples show how to configure NTP on a secondary (non-default) VDC.

```
switch# configure terminal
switch(config)# feature ntp
switch(config)# ntp master
switch(config)# ntp source-interface ethernet
switch(config)# ntp source 192.0.2.2
switch(config)# 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	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **ntp logging** **Example:** `switch(config)# ntp logging`	Enables or disables system logs to be generated with significant NTP events. NTP logging is disabled by default.
Step 3	(Optional) **show ntp logging-status** **Example:** `switch(config)# show ntp logging-status`	Displays the NTP logging configuration status.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies 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

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

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 rts-update	Displays the RTS update status.
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 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# 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 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# 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
```

Additional References

Related Documents

Related Topic	Document Title
Clock manager	*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*
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*

MIBs

MIBs	MIBs Link
MIBs related to NTP	To locate and download supported MIBs, go to the follow http://www.cisco.com/public/sw-center/netmgmt/cmtk/m

Feature History for NTP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

Table 1: Feature History for NTP

Feature Name	Releases	Feature Information
NTP	7.3(0)D1(1)	Increased the length of NTP authentication keys from 15 to 32 alphanumeric characters.
NTP	6.2(2)	Introduced the **ntp access-group match-all** command to cause the access group options to be scanned in order, from least restrictive to most restrictive.
NTP	6.2(2)	Introduced the **no ntp passive** command to prevent NTP from forming associations.

NTP	6.2(2)	Added the ability to configure NTP broadcast and multicast servers and multicast clients on an interface.
NTP	6.2(2)	Added the ability to enable or disable NTP on an interface.
NTP	6.1(1)	NTP access group options are now scanned in order from least restrictive to most restrictive.
NTP	6.1(1)	Increased the length of NTP authentication keys from 8 to 15 alphanumeric characters.
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.
NTP	5.2(1)	Changed the command to enable or disable NTP from [**no**] **ntp enable** to [**no**] feature ntp.
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.
NTP access groups	5.2(1)	Added the **serve, serve-only**, and **query-only** access group options to control access to additional NTP services.
NTP access groups	5.0(2)	Added the ability to control access to NTP services by using access groups.
NTP authentication	5.0(2)	Added the ability to enable or disable NTP authentication.
NTP logging	5.0(2)	Added the ability to enable or disable NTP logging.
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.
CFS support	4.2(1)	Added the ability to distribute NTP configuration using CFS.

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.