

Network Time Protocol

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).

- Overview, on page 1
- Guidelines and Limitations, on page 3
- Enable or Disable NTP, on page 6
- Configure Device as an Authoritative NTP Server, on page 9
- Configure Server and Peer, on page 9
- Configure Authentication, on page 11
- Configure Access Restrictions, on page 13
- Configure Source IP Address, on page 15
- Configure Source Interface, on page 15
- Configure Logging, on page 16
- Additional References, on page 17

Overview

A Network Time Protocol (NTP) server is a device that receives its time from an authoritative time source and distributes this time across the network to synchronize devices.

- It receives time from authoritative sources such as radio clocks, atomic clocks, or GPS time sources.
- It distributes synchronized time to network devices with high efficiency (as little as one packet per minute for millisecond accuracy).
- It uses a stratum system to describe the distance between a device and the authoritative time source.

Stratum and Synchronization Behavior

NTP uses a stratum system to indicate how far a device is from an authoritative time source, and compares time from multiple devices before synchronizing.

- 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 server.

- 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.

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



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.

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 as 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.

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 9000 Series NX-OS Fundamentals Configuration Guide.

Virtualization Support

NTP recognizes virtual routing and forwarding (VRF) instances. NTP uses the default VRF if you do not configure a specific VRF for the NTP server and NTP peer. See the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for more information about VRFs.

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 9000 Series NX-OS High Availability and Redundancy Guide.

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

Default Settings

The following table lists the default settings for NTP parameters.

Parameters	Default
NTP	Enabled
NTP authentication	Disabled
NTP access	Enabled
NTP logging	Disabled

Guidelines and Limitations

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

Configuration Guidelines

1. Before configuring a name based NTP server (FQDN) in a non-default VRF, you must configure a DNS server under that specific VRF. If you configure the DNS server from the global configuration mode using **use-vrf** option, then that name based NTP server configuration will not be added to the running configuration. If you attempted to configure NTP server using this method, you must remove the NTP configuration using the **no** version of the command, add the DNS server under that VRF, and then add name based NTP server to the VRF. The configured DNS server must be reachable and must return the correct IP for the FQDN of the NTP server when queried.
2. Configure **clock protocol ntp** to synchronize the system clock from an NTP server, or to act as an NTP server providing time to other devices.
3. We recommend that you configure 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).
4. A peer that is 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.
5. If you have only one server, we recommend that you configure all the devices as clients to that server.
6. You can configure up to 64 NTP entities (servers and peers).
7. If you configure NTP in a VRF, ensure that the NTP server and peers can reach each other through the configured VRFs.

General Guidelines

- NTP server functionality is supported.
- Manually distribute NTP authentication keys on the NTP server and Cisco NX-OS devices across the network.
- If you are using the switch as an edge device and want to use NTP, we recommend using the **ntp access-group** command and filtering NTP only to the required edge devices.
- If the system has been configured with the **ntp passive** , **ntp broadcast client** , or **ntp multicast client** commands, when NTP receives an incoming symmetric active, broadcast, or multicast packet, it can set up an ephemeral peer association in order to synchronize with the sender.

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

- If you specify the **ntp authenticate** command, when a symmetric active, broadcast, or multicast packet is received, the system does not synchronize to the peer unless the packet carries one of the authentication keys that are specified in the **ntp trusted-key** global configuration command.
- To prevent synchronization with unauthorized network hosts, the **ntp authenticate** command should be specified any time the **ntp passive** , **ntp broadcast client** , or **ntp multicast client** command has been specified unless other measures, such as the **ntp access-group** command, have been taken to prevent unauthorized hosts from communicating with the NTP service on the device.
- While configuring NTP authentication password, use printable ASCII characters without #. If the password contains # authentication will not work for that key.

  To configure NTP authentication passwords with length greater than 20 characters, use hex characters (0-9,A-F) only.
- The **ntp authenticate** command does not authenticate peer associations that are configured via the **ntp server** and **ntp peer** configuration commands. To authenticate the **ntp server** and **ntp peer** associations, specify the **key** keyword.
- A maximum of four IP ACLs can be configured for a single NTP access group. IPv4 and IPv6 ACLs are supported.
- If packet flooding occurs on the inband ports, it can increase the CPU usage by NTPD to more than 90%. To overcome this high CPU usage by NTPD, use the custom CoPP policy to rate limit the incoming traffic to NTP. For more information about creating a custom CoPP policy, refer to the Configuring Control Plane Policing chapter in the relevant version of the Cisco Nexus 9000 Series NX-OS Security Configuration Guide on cisco.com .

Note The recommended rate limit is 1000 kbps for the policy **CIR** field and 64,000 bytes for the **BC** field.

Release Specific Guidelines

Beginning with Cisco NX-OS Release 9.3(9)

- NTP version 4 (NTPv4) is supported on Nexus standalone switches.

Beginning with Cisco NX-OS Release 10.1(1)

- Cisco Nexus 9000 switches do not sync with stratum 14 and 15.
- NTP version 4 (NTPv4) is supported on Nexus standalone switches.

Beginning with Cisco NX-OS Release 10.3(3)F

- In line with the RFC 8573 standards, NTP security is enhanced with the AES128CMAC authentication mechanism along with Type-6 encryption support for authentication keys.
- This feature provides an option to set the password as Type-0, Type-7, or Type-6.
- The maximum number of unique keys which can be configured is 1024, and the range is 1 to 65535.
- For Type-6 authentication to work, configure the same primary (master) key on the device, which was used to generate the new Type-6 key being configured, along with **feature password encryption aes** .
- If you enforce re-encryption using the **encryption re-encrypt obfuscated** command, all the NTP non-Type-6 passwords will be re-encrypted to Type-6.

  The **encryption delete type6** command deletes all the Type-6 passwords configured on NTP.

  The **encryption decrypt type6** command decrypts the existing configured Type-6 passwords.
- To perform ISSD from AES128CMAC/Type-6 supported version to a non-AES128CMAC/Type-6 supported version, unconfigure the Type-6 keys and then perform the ISSD.
- It is recommended to specify the encryptType and keyString when programmatically (restconf/Netconf and so on) configuring a key chain. If not specified, then the key chain infra uses the already available (or default) value of the missing property to configure the keyString.
- If you need to configure with a property missing, then you need to follow the same sequence of steps in both the peer routers.

Beginning with Cisco NX-OS Release 10.4(4)M

-

Best Practices for NTP configuration

Follow these best practices when configuring NTP:

- Configure multiple redundant NTP time sources to avoid reliance on a single server and improve reliability.
- Use a loopback interface as the NTP source for consistency across device reboots and interface changes.
- Enable NTP authentication to secure communications and prevent malicious time alterations.
- Monitor NTP status and logs regularly; implement detection and alerting mechanisms using commands like **show ntp status** and **show ntp associations**.

- Use the **ntp panic-threshold-apply** command to check the configuration sanity checks, which reject large clock changes and prevent network instability.
- Address failure modes related to time-based authentication keychains by configuring overlapping key lifetimes to avoid routing disruptions.
- Regularly monitor and validate NTP synchronization status with monitoring tools and SNMP traps.
- Ensure operational practices include multiple NTP sources and configuration checks to prevent routing disruptions caused by time inaccuracies.

These practices help maintain accurate time synchronization, improve NTP security, and minimize the risk of network instability caused by incorrect time settings.

Enable or Disable NTP

NTP is enabled by default.



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

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
 switch(config)#
```

Step 2 Enable or disable NTP using the command [**no**] **feature ntp**

Example:

```
switch(config)# feature ntp
```

Step 3 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

This example for md5 shows how to configure the device to synchronize only to time sources that provide authentication key 42 in their NTP packets:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 aNiceKey
switch(config)# ntp server 192.0.2.105 key 42
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

This example for aes128cmac shows how to configure the device to synchronize only to time sources that provide authentication key 12 in their NTP packets:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ntp authentication-key 12 aes128cmac password 0/6/7
switch(config)# ntp server 192.0.2.105 key 12
switch(config)# ntp trusted-key 12
switch(config)# ntp authenticate
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
```

Note When only a single ACL group is applied, then all the packets relevant for other ACL categories are denied and only packets relevant for the configured ACL group is processed, as mentioned in below scenarios:

- If serve ACL is configured, then only client, control, and private packets are processed and all the other packets are denied.
- If serve-only ACL is configured, then only client packets are processed and all the other packets are denied.

If more than a single ACL is configured, it follows the order of processing as mentioned in below scenario:

- If serve and serve-only both are configured for the same IP address without match-all configured, where the IP is permitted in serve-acl and denied in serve-only, the client, control, private packets are permitted for that IP.

What to do next

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 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.

Configure 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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
 switch(config)#
```

Step 2 Configure the device as an authoritative NTP server using the command [**no**] **ntp master** [*stratum*]

Example:

```
switch(config)# ntp master
```

You can specify a different stratum level from which NTP clients get their time synchronized. The range is from 1 to 15.

Step 3 Display the NTP configuration using the command **show running-config ntp**

Example:

```
switch(config)# show running-config ntp
```

This is an optional step.

Step 4 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure Server and Peer

Configure an NTP server and peer to synchronize the device clock with a reliable time source.

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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
  switch(config)#
```

Step 2 Form an association with a server using the command [**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
```

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 (configured as powers of 2, so effectively 16 to 65536 seconds), and the default values are 6 and 4, respectively (*maxpoll* default = 64 seconds, *minpoll* default = 16 seconds).

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 Form an association with a peer using the command [**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
```

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 server. The range for the *max-poll* and *min-poll* arguments is from 4 to 17 (configured as powers of 2, so effectively 16 to 131072 seconds), and the default values are 6 and 4, respectively (*maxpoll* default = 64 seconds, *minpoll* default = 16 seconds).

Use the **prefer** keyword to make this peer the preferred NTP peer for the device.

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 Display the configured server and peers using the command **show ntp peers**

Example:

```
switch(config)# show ntp peers
```

This is an optional step.



Note A domain name is resolved only when you have a DNS server configured.

When DNS/Name Server resolves both IPv4 and IPv6, IPv6 Address is preferred by NX-OS.

Step 5 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure Authentication

Use this task to configure NTP authentication on your device, ensuring that the device synchronizes only with trusted time sources.

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.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
  switch(config)#
```

Step 2 Define the authentication keys using the command [**no**] **ntp authentication-key** *number* { **md5** | **aes128cmac** } *password string encryption-type*

Example:

```
switch(config)# ntp authentication-key 42 md5 aNiceKey


switch(config)# ntp authentication-key 21 md5
 JDYk3pp/Fuv0zWyVSRhS6EDERSSsp1uA7s57dvdsx
 g74ndf02lEI9dF6WX6Z78/5R8qPmSRRrDUDtCcUlZ
 XDUrf0ErodS3ikPQA= 6

switch(config)# ntp authentication-key
 12 aes128cmac
 JDYkzj4NojJdSkQPvBhFvAO9xCSVwj2iRGvShNSg
 ER4JwMBMtUEibfqkscgZ4+/iTdDmeCRW9SGWLxKb
 3Xk5g8pz4bR7Iu1a7QA= 6
```

You can choose either md5 or aes128cmac authentication scheme.

If the user is using the Type-6 key generated from the same primary (**master**) key, then the device does not synchronize to a time source until the user enables **feature password encryption aes** .

For Type-0 and Type-7 encryption types, the maximum length is 32 characters. Until Release 10.3(3)F, it was 15 (alphanumeric) characters. For the Type-6 encryption type, the maximum limit is 128 characters.

Step 3 Form an association with a server using the command **ntp server** *ip-address* **key** *key-id*

Example:

```
switch(config)# ntp server 192.0.2.1 key 1001
```

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.

To require authentication, the **key** keyword must be used. Any **ntp server** or **ntp peer** commands that do not specify the **key** keyword will continue to operate without authentication.

Step 4 Display the configured NTP authentication keys using the command **show ntp authentication-keys**

Example:

```
switch(config)# show ntp authentication-keys
```

This is an optional step.

Step 5 Specify one or more keys using the command [**no**] **ntp trusted-key** *number*

Example:

```
switch(config)# ntp trusted-key 42
```

This command specifies one or more keys (defined in Step 2) that an unconfigured remote symmetric, broadcast, and multicast time source must provide in its NTP packets in order for the device to synchronize to it. The range for trusted keys is from 1 to 65535.

This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

Step 6 Display the configured NTP trusted keys using the command **show ntp trusted-keys**

Example:

```
switch(config)# show ntp trusted-keys
```

This is an optional step.

Step 7 Enable or disable authentication for ntp passive, ntp broadcast client, and ntp multicast using the command **[no] ntp authenticate**

Example:

```
switch(config)# ntp authenticate
```

NTP authentication is disabled by default.

Step 8 Display the status of NTP authentication using the command **show ntp authentication-status**

Example:

```
switch(config)# show ntp authentication-status
```

This is an optional step.

Step 9 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure 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.

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

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

The access groups are evaluated in the following order:

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

ACL processing of serve-only or query-only depends on the NTP packet type.

Procedure

Step 1 Enter global configuration mode uisng the command **configure terminal**

Example:

```
switch# configure terminal
 switch(config)#
```

Step 2 Create or remove an access group to control NTP access and applies a basic IP access list using the command [**no**] **ntp access-group match-all** | {{ **peer** | **serve** | **serve-only** | **query-only** } *access-list-name* }

Example:

```
switch(config)# ntp access-group match-all
 switch(config)# ntp access-group peer peer-acl
 switch(config)# ntp access-group serve serve-acl
```

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.
- The **match-all** keyword enables the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. If the incoming packet does not match the ACL in the peer access group, it goes to the serve access group to be processed. If the packet does not match the ACL in the serve access group, it goes to the serve-only access group, and so on.



Note The **match-all** keyword is available beginning with Cisco NX-OS Release 7.0(3)I6(1) and is supported on Cisco Nexus 9000 Series switches and the Cisco Nexus 3164Q, 31128PQ, 3232C, and 3264Q switches.

- The *access-list-name* variable is the name of the NTP access group. The name can be an alphanumeric string up to 64 characters, including special characters.

Step 3 Display the NTP access group configuration using the command **show ntp access-groups**

Example:

```
switch(config)# show ntp access-groups
```

This is an optional step.

Step 4 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure 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

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
  switch(config)#
```

Step 2 Configure the source IP address for all NTP packets using the command [**no**] **ntp source** *ip-address*

Example:

```
switch(config)# ntp source 192.0.2.1
```

The *ip-address* can be in IPv4 or IPv6 format.

Step 3 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure Source Interface

You can configure NTP to use a specific interface.

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
 switch(config)#
```

Step 2 Configure the source interface for all NTP packets using the command [**no**] **ntp source-interface** *interface*

Example:

```
switch(config)# ntp source-interface ethernet 2/1
```

Use the **?** keyword to display a list of supported interfaces.

Step 3 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Configure Logging

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

Procedure

Step 1 Enter global configuration mode using the command **configure terminal**

Example:

```
switch# configure terminal
  switch(config)#
```

Step 2 Enable or disable system logs to be generated with significant NTP events using the command [**no**] **ntp logging**

Example:

```
switch(config)# ntp logging
```

NTP logging is disabled by default.

Step 3 Display the NTP logging configuration status using the command **show ntp logging-status**

Example:

```
switch(config)# show ntp logging-status
```

This is an optional step.

Step 4 Copy the running configuration to the startup configuration using the command **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
```

This is an optional step.

Additional References

Related Documents

- Clock manager : Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide
- MIBs related to NTP : To locate and download supported MIBs, go to the following URL: https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html