Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on Cisco MDS 9000 Series switches.

Information About NTP

This section describes information about NTP.

NTP

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization occurs when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

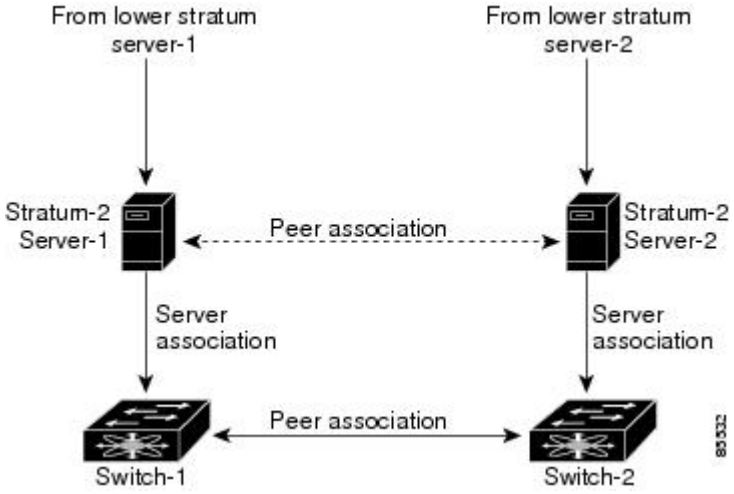
By configuring an IP address as a peer, the Cisco NX-OS device will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both of these instances point to different time servers, your NTP service is more reliable. Even if the active server link is lost, you can still maintain the correct time due to the presence of the peer.

If an active server fails, a configured peer helps in providing the NTP time. To ensure backup support if the active server fails, provide a direct NTP server association and configure a peer.

If you only configure a peer, the most accurate peer takes on the role of the NTP server and the other peer acts as a peer. Both devices end at the correct time if they have the correct time source or if they point to the correct NTP source.

Figure 1: NTP Peer and Server Association

Not even a server down time will affect well-configured switches in the network. This figure displays a network with two NTP stratum 2 servers and two switches.



In this configuration, the switches were configured as follows:

- Stratum-2 Server-1
  - IPv4 address-10.10.10.10
- Stratum-2 Server-2
  - IPv4 address-10.10.10.9
- Switch-1 IPv4 address-10.10.10.1
- Switch-1 NTP configuration
  - NTP server 10.10.10.10
  - NTP peer 10.10.10.2
- Switch-2 IPv4 address-10.10.10.2
- Switch-2 NTP configuration
  - NTP server 10.10.10.9
  - NTP peer 10.10.10.1

Prerequisites for NTP

NTP has the following prerequisite:

- The switch should have IP connectivity to other NTP-enabled devices.

Guidelines and Limitations for NTP

NTP has the following configuration guidelines and limitations:

- You should allow a peer association with another device only when you are sure that the switch's clock is reliable (either it has a high quality local clock or the switch is itself 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).

Configuring NTP

This section describes how to configure NTP.

Enabling NTP

To enable NTP on a switch:

Note NTP is enabled by default.

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP:

switch(config)# **feature ntp**

Disabling NTP

To disable NTP on a switch:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP:

switch(config)# **no feature ntp**

Configuring Authentication Keys

The **ntp trusted-key** command provides protection against accidentally synchronizing the device to a time source that is not trusted. To synchronize a server device time zone with a client device time zone, the NTP authentication feature can be enabled only on the server device. To synchronize a client device time zone with a server device time zone, the NTP authentication feature must be enabled on both devices and the keys specified on the client device must be one of the keys specified on the server device. If the keys specified on the server device and the client device are different, then only the server device time zone can be synchronized with the client device time zone.

To configure the keys to be used to authenticate NTP associations, perform these steps:

Before you begin

Make sure that you configured the NTP server with the authentication keys that you plan to specify in this procedure.

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Define an authentication key:

switch(config)# **ntp authentication-key** *id* **md5** *key* [**0** | **7**]

The range for key *id* is from 1 to 65535. For the *key*, you can enter up to eight alphanumeric characters.

Step 3 Specify one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it:

switch(config)# **ntp trusted-key** *id*

The range for key *id* is from 1 to 65535.

What to do next

Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations, on page 4.

Enabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations

Temporary, symmetric, broadcast, or multicast updates (as opposed to server or peer updates) should be authenticated to prevent untrusted sources from injecting updates to devices.

To enable authentication of these types of NTP associations, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP authentication of packets from new temporary, symmetric, broadcast, or multicast associations with remote network hosts (this does not authenticate peer associations that are created using the **ntp server** or **ntp peer** commands.):

switch# **ntp authenticate**

Disabling Authentication of Temporary, Symmetric, Broadcast, or Multicast NTP Associations

To disable authentication of these types of NTP associations, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP authentication of packets from new temporary, symmetric, broadcast, or multicast associations with remote network hosts (this does not authenticate peer associations that are created using the **ntp server** or **ntp peer** commands.):

switch(config)# **no ntp authenticate**

NTP authentication is disabled by default.

Enabling NTP Servers and Peers

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

NTP implements authentication through keys. Use NTP keys to filter exchanges to only trusted devices. This avoids trusting NTP updates from misconfigured or malicious sources.

To enable NTP server and peers, perform these steps:

Before you begin

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

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Form an association with a server:

switch(config)# **ntp server** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

You can specify multiple server associations.

Use the **key** keyword to enable authentication with the named server using the specified key. The range for the *id* argument is from 1 to 65535.

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

Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a server. The range for the *interval* is from 4 to 16 seconds, and the default values are 6 for maxpoll and 4 for minpoll.

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:

switch(config)# **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*} [**key** *id*] [**prefer**] [**maxpoll** *interval*] [**minpoll** *interval*]

You can specify multiple peer associations.

Use the **key** keyword to enable authentication with the named server using the specified key. The range for the *id* argument is from 1 to 65535.

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

Use the **maxpoll** and **minpoll** keywords to configure the maximum and minimum intervals in which to poll a peer. The range for the interval is from 4 to 17 seconds, and the default values are 6 for maxpoll and 4 for minpoll.

Note If you configure a key to be used while communicating with the NTP peer, make sure that the key exists as a trusted key on the device.

Disabling NTP Servers and Peers

To disable NTP server and peers, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable an NTP server:

switch(config)# **no ntp server** {*ip-address* | *ipv6-address* | *dns-name*}

Step 3 Disable an NTP peer:

switch(config)# **no ntp peer** {*ip-address* | *ipv6-address* | *dns-name*}

Enabling NTP Modes

To enable processing of NTP control mode and private mode packets, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable the processing of control mode and private mode packets:

switch(config)# **ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

The default time duration is 3 seconds, which means that a control mode packet is processed or responded every 3 seconds. Range is from 1 to 65535.

Disabling NTP Modes

To disable processing of NTP control mode and private mode packets, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable the processing of control mode and private mode packets:

switch(config)# **no ntp allow** {**private** | **control** [**rate-limit** *seconds*]}

Enabling NTP Source Interface

To override the default source address of NTP packets sent from the switch, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Override the default source address of NTP packets sent from the switch:

switch(config)# **ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

Only a single **ntp source-interface** command can be specified. All NTP packets sent through all interfaces will use the address specified by this command as the source address.

Disabling NTP Source Interface

To restore the default source address of NTP packets, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Restore the default source address of NTP packets:

switch(config)# **no ntp source-interface** {**ethernet** *slot/port.sub-interface* | **mgmt** *number* | **port-channel** *number*}

Enabling NTP Logging

To enable logging of NTP message to syslog, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP logging:

switch(config)# **ntp logging**

Disabling NTP Logging

To disable logging of NTP message to syslog, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP logging:

switch(config)# **no ntp logging**

Configuring NTP Syslog Logging Level

To configure the severity threshold of NTP syslog messages, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Configure the severity threshold of NTP syslog messages:

switch(config)# **logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

The following keywords specify the severity levels:

- **0**—Specifies to log emergency messages.

- **1**—Specifies to log alert messages.
- **2**—Specifies to log critical messages.
- **3**—Specifies to log error messages.
- **4**—Specifies to log warning messages.
- **5**—Specifies to log notification messages.
- **6**—Specifies to log informational messages.
- **7**—Specifies to log debugging messages.

Setting the Default NTP Syslog Severity Logging Level

To return to the default NTP syslog severity logging level, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Return to the default NTP syslog severity logging level:

switch(config)# **no logging level ntp** {**0** | **1** | **2** | **3** | **4** | **5** | **6** | **7**}

Displaying and Clearing NTP Statistics

NTP generates statistics that you can display and clear as needed.

To display and clear NTP statistics, perform these steps:

Step 1 Display NTP statistics:

switch# **show ntp statistics** {**peers** | **io** | **local** | **memory**}

You can display the following NTP statistics:

- **peer**—NTP statistics per peer.
- **io**—Statistics of NTP packet handling.
- **local**—Statistics of NTP packet types.
- **memory**—Statistics of memory usage by NTP.

Step 2 Clear NTP statistics:

switch# **clear ntp statistics** {**peer** | **io** | **local** | **memory**}

Resynchronizing NTP

If the NTP client on a switch has lost synchronization with servers or peers, you may need to restart the NTP client. This will restart the synchronization process with all NTP servers and peers configured on the local switch. To check the status of NTP servers and clients, see the Troubleshooting NTP.

To restart the NTP client on the switch, perform the following steps:

Retry synchronization:

switch# **ntp sync-retry**

Distributing the NTP Configuration Using CFS

You can distribute local NTP configuration to other switches in the fabric using CFS.

Note Only NTP server and peer configuration is distributed through CFS.

Enabling NTP Configuration Distribution

To enable CFS distribution of NTP configuration, perform these steps:

Before you begin

- Ensure that CFS is enabled. For more information, see the "Verifying CFS Distribution Status" section in the "Cisco MDS 9000 Series System Management Configuration Guide."
- Ensure that NTP is enabled. For more information, see "Verifying NTP, on page 12."

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable NTP configuration distribution to all switches in a fabric:

switch(config)# **ntp distribute**

This command acquires a fabric lock and stores all future configuration changes in the pending database.

Disabling NTP Configuration Distribution

To disable CFS distribution of NTP configuration, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Disable NTP configuration distribution:

switch(config)# **no ntp distribute**

Committing NTP Configuration Changes

When you commit the NTP configuration changes, the Cisco NX-OS software applies the pending changes to the running configuration on the local Cisco MDS switch and to all the Cisco MDS switches in a fabric that can receive NTP configuration distributions.

To apply pending NTP configuration to an NTP CFS enabled peers in a fabric, perform these steps:

Before you begin

Enable NTP configuration distribution on other Cisco MDS switches in a fabric.

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Distribute the pending NTP configuration to an NTP CFS enabled peers in the fabric:

switch(config)# **ntp commit**

Discarding NTP Configuration Changes

In NTP distribution mode, configuration changes are buffered until committed by the user. You can discard the changes before they are committed with the **abort** command.

To terminate and unlock the existing NTP CFS distribution session on a switch, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Terminate and unlock the existing NTP CFS distribution session on a switch:

switch(config)# **ntp abort**

Forcing Termination of a Lost NTP Configuration Session

When a user starts making NTP configuration changes in distribute mode, a session is created and CFS creates a fabric wide session lock. The session lock is to prevent other users from simultaneously creating sessions and making NTP configuration changes. If the user does not commit or cancel the changes, further NTP configuration sessions will be prevented until the lock is cleared. In this case, the session lock can be released by another user and this action causes all pending NTP configuration changes in the session to be discarded and the lock to be released. Releasing the session lock can be performed from any switch in the fabric. If the administrator performs this task, pending configuration changes are discarded and the fabric lock is released.

To use administrative privileges and release the locked NTP session, perform this step:

Release the locked NTP session:

switch# **clear ntp session**

Verifying NTP

Use the following commands to verify NTP:

This example shows how to verify if NTP is enabled:

```
switch(config)# show running-config all | include "feature ntp"
feature ntp
```

This example shows how to display the current NTP configuration:

```
switch# show running-config ntp

!Command: show running-config ntp
!Time: Fri Jan 1 1:23:45 2018

version 8.2(1)
logging level ntp 6
ntp peer 192.168.12.34
ntp server 192.168.86.42
ntp authentication-key 1 md5 fewhg12345 7
ntp logging
```

This example shows the uncommitted (pending) NTP configuration for the current session:

```
switch# configure terminal
switch(config)# ntp distribute
switch(config)# ntp peer 192.168.12.34
switch(config)# show ntp pending peers

ntp peer 192.168.12.34

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

This example shows the difference between the pending CFS database and the current NTP configuration:

```
switch# show ntp pending-diff
```

This example shows if the time stamp check is enabled using the **time-stamp** command:

```
switch# show ntp timestamp status
Linecard 3 does not support Timestamp check.
```

Troubleshooting NTP

Use the following information for troubleshooting NTP:

This example shows the NTP CFS status:

```
switch# show ntp status
Distribution : Disabled
Last operational state: No session
```

This example shows how to verify to which switches NTP configuration changes will be distributed to:

```
switch1# show cfs peers name ntp

Scope : Physical-fc-ip
--------------------------------------------------------------------------
Switch                  WWN IP Address
--------------------------------------------------------------------------
20:00:8c:60:4f:0d:2b:b0 192.168.12.34 [Local]
                        [switch1]
20:00:8c:60:4f:0d:32:d0 192.168.56.78 [Merged]
                        [switch2.mydomain.com]

Total number of entries = 2
```

This example shows the NTP session information:

```
switch# show ntp session status
Last Action Time Stamp     : None
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : none
```

This example shows all the NTP peers:

```
switch# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  10.105.194.169                Server (configured)
```

This example shows the difference between **show ntp pending peers** and **show ntp pending-diff** commands. The outputs are similar when adding NTP servers or peers.

```
switch1# configure terminal
switch1(config)# ntp authenticate
switch1(config)# ntp authentication-key 1 md5 aNiceKey
switch1(config)# ntp server 192.168.12.34 key 1
switch1(config)# ntp authentication-key 2 md5 goodTime
switch1(config)# ntp peer 192.168.56.78 key 2
switch1(config)# show ntp pending peers

ntp server 192.168.12.34


ntp peer 192.168.56.78

switch1(config)# show ntp pending-diff
+ntp peer 192.168.56.78
+ntp server 192.168.12.34
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
```

Caution Only the server and peer commands are distributed to the NTP peer switches. Other parameters such as enabling authentication and configuring authentication keys must be configured on each switch.

Continuing the example on switch1, the outputs differ when deleting servers or peers:

```
switch1(config)# no ntp peer 192.168.56.78
switch1(config)# show ntp pending peers

ntp server 192.168.12.34

switch1(config)# show ntp pending-diff
-ntp peer 192.168.56.78
switch1(config)# ntp commit
switch1(config)# show ntp pending peers
switch1(config)# show ntp pending-diff
switch1(config)# end
```

This example shows the status of a peer. Information about each peer is displayed in the table, one peer per line. The first character of each line is a status flag. A legend above the table shows the meaning of this flag. NTP servers and peers that are in synchronization and used for local time updates have an equal (=) flag. There must be at least one device with this flag for the time on the local switch to be updated. Passive peers are peers that are currently unsynchronized. This means the local switch will not use time updates from these peers. The *remote* column shows the source IP address of the peer. The accuracy of the peer's source clock, or stratum, is shown in the *st* column. The higher the stratum value, the lower the accuracy of the peer's clock source, 16 being the lowest accuracy. The polling interval, in seconds, is shown in the *poll* column. The reachability field in the *reach* column is a circular bit map of the last 8 transactions with that peer, '1' indicating success and '0' indicating failure, the most recent transaction in the lowest significant bit. This peer has not lost any of the last 6 poll messages. The round trip time between the local switch and peer, in seconds, is shown in the *delay* column.

```
switch# show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
```

```
    remote           local    st   poll   reach delay
------------------------------------------------------------------
*10.105.194.169     0.0.0.0    4     16      77   0.00099
```

This example shows the detailed NTP information for a single server or peer.

The *time last received* parameter will return to zero each time frame is received from that server or peer. Consequently, this parameter will steadily increment if the peer is unreachable or not sending to the local switch NTP client.

```
switch# show ntp statistics  peer ipaddr 10.105.194.169
remote host:          10.105.194.169
local interface:      Unresolved
time last received:   9s
time until next send: 54s
reachability change:  54705s
packets sent:         3251
packets received:     3247
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      6
```

This example shows the counters maintained by the local NTP client on the switch:

```
switch# show ntp statistics local
system uptime:          24286
time since reset:       24286
old version packets:    13
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      13
bad authentication:     0
```

Example: Configuring NTP

This example displays how to enable the NTP protocol:

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

This example displays how to disable the NTP protocol:

```
switch# configure terminal
switch(config)# no feature ntp
```

This example displays how to configure an NTP server:

```
switch# configure terminal
```

```
switch(config)# ntp server 192.0.2.10
```

This example displays how to configure an NTP peer:

```
switch# configure terminal
switch(config)# ntp peer 2001:0db8::4101
```

This example displays how to configure NTP authentication:

```
switch# configure terminal
switch(config)# ntp authentication-key 42 md5 key1_12
switch(config)# ntp trusted-key 42
switch(config)# ntp authenticate
```

This example displays how to enable the processing of private mode packets:

```
switch# configure terminal
switch(config)# ntp allow private
```

This example displays how to enable the processing of control mode packets with a rate-limit of 10 seconds:

```
switch# configure terminal
switch(config)# ntp allow control rate-limit 10
```

This example displays how to configure an NTP source interface:

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

This example enables logging of NTP messages to syslog and changes the syslog logging threshold to 'information':

```
switch# configure terminal
switch(config)# ntp logging
switch(config)# logging logfile messages 6
switch(config)# end
switch# show logging | include "logfile:" next 1
Logging logfile: enabled
Name - messages: Severity - information Size - 4194304
switch# show logging logfile | include %NTP
2017 Jan 1 1:02:03 switch %NTP-6-NTP_SYSLOG_LOGGING: : Peer 192.168.12.34 is reachable
2017 Jan 1 2:34:56 switch %NTP-6-NTP_SYSLOG_LOGGING: : System clock has been updated,
offset= sec
```

This example displays how to disable NTP logging:

```
switch# configure terminal
switch(config)# no ntp logging
```

Default Settings for NTP

This table lists the default settings for NTP parameters.

Table 1: Default NTP Settings

NTP	Disabled
NTP Modes	Disabled
NTP Source Interface	mgmt0
NTP Logging	Disabled
NTP Distribution	Disabled