

Network Time Protocol

- Network Time Protocol, on page 1
- Obtain NTP time information, on page 3
- Configure NTP access groups , on page 6
- Configure NTP authentication , on page 7
- Configure the source IP address for NTP packets , on page 8
- Configure the system as an authoritative NTP server , on page 9
- Update the hardware clock, on page 9
- Verify the status of external reference clock , on page 10
- Disable NTP services on a specific interface , on page 11
- FQDN for NTP server , on page 11
- NTP-PTP interworking, on page 14

Network Time Protocol

A network time protocol is a time synchronization standard that

- synchronizes timekeeping among distributed devices by exchanging timestamped messages,
- uses a hierarchical stratum structure to ensure accurate and robust time propagation, and
- enables reliable event correlation and time-sensitive functions across networked system

A stratum is the level of a device in the NTP hierarchy, reflecting its distance from an authoritative time source such as an atomic or GPS clock.

NTP uses User Datagram Protocol (UDP) and operates in Coordinated Universal Time (UTC). It promotes efficiency by requiring minimal traffic (typically one packet per minute) to achieve synchronization within milliseconds. NTP enforces accuracy by refusing to synchronize with unsynchronized or significantly divergent devices, regardless of their stratum.

- Routers and switches in a data center use NTP to align their logs for troubleshooting and security audits.
- Computers on a corporate network synchronize with an NTP server to maintain consistent system clocks.

Using manual time settings on network devices, rather than NTP, can lead to clock drift and inconsistent logs.

Best practices: NTP configuration and WNRO issues mitigation

Best practices for configuring NTP

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.

Mitigate GPS Week Number Rollover (WNRO) issues

To minimize the risk and impact of GPS Week Number Rollover (WNRO) issues in your network, apply these best practices:

- If your NTP source or server chain does not include any GPS sources, you do not need to take action—WNRO will not affect your network.
- GPS WNRO affects only the system clock; it does not disrupt user traffic.
- Contact your GPS hardware manufacturer for guidance and corrective actions if you suspect your GPS source may be susceptible to WNRO-related issues.
- If your GPS source is identified as a potential disruption point for WNRO (for example, on 2019-04-06 or later), configure the NTP master on the Cisco device connected to this source. Set the clock on the Stratum 1 device to isolate the affected source. With this setup, the device presents its own clock for synchronization to downstream NTP clients.
- Configure multiple NTP servers (ideally more than 3, preferably four servers) at the Stratum 2 level of your network. This enables NTP clients at Stratum 2 to synchronize with multiple Stratum 1 servers, which, if affected by WNRO, will be automatically marked as false ticker or outlier sources to prevent incorrect clock distribution.

Note The NTP master command is a temporary workaround. Use it only until the GPS source issue is resolved, to prevent incorrect time values from being propagated throughout your network

Obtain NTP time information

Procedure

Step 1 Configure poll-based associations.

Step 2 Configure broadcast based NTP association.

Configure poll-based associations

Establish a peer-to-peer NTP association between your router and one or more other devices to enable mutually redundant time synchronization.

Use this task when you need routers (or servers) to keep each other's time in sync, typically to improve redundancy and reliability for time sources in your network. You can configure NTP associations in either client mode or symmetric active mode, depending on the accuracy and reliability requirements.

The client and the symmetric active modes should be used when NTP is required to provide a high level of time accuracy and reliability.

When a networking device is operating in the client mode, it polls its assigned time serving hosts for the current time. The networking device then picks a host from all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host doesn't capture or use any time information sent by the local client device. This mode is most suited for file-server and workstation clients that aren't required to provide any form of time synchronization to other local clients. Use the **server** command to individually specify the time-serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode.

When a networking device is operating in the symmetric active mode, it polls its assigned time-serving hosts for the current time and it responds to polls by its hosts. Because this is a peer-to-peer relationship, the host also retains time-related information about the local networking device that it's communicating with. This mode should be used when there are several mutually redundant servers that are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet today adopt this form of network setup. Use the **peer** command to individually specify the time-serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the symmetric active mode.

When the router polls several other devices for the time, the router selects one device with which to synchronize.

Note To configure a peer-to-peer association between the router and another device, you must also configure the router as a peer on the other device.

You can configure multiple peers and servers, but you can't configure a single IP address as both a peer and a server at the same time.

To change the configuration of a specific IP address from peer to server or from server to peer, use the **no** form of the **peer** or **server** command to remove the current configuration before you perform the new configuration. If you don't remove the old configuration before performing the new configuration, the new configuration doesn't overwrite the old configuration.

Before you begin

- Access the router's CLI with configuration privileges.
- Identify the IP addresses of peer devices.
- Ensure you have configuration access to the other device(s) for mutual setup.

Procedure

Step 1 Form a server association with another system.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# server 172.19.69.1 minpoll 8 maxpoll 12
```

This step can be repeated as necessary to form associations with multiple devices.

Step 2 Form a peer association with another system.

Example:

```
Router(config-ntp)# peer 192.168.22.33 minpoll 8 maxpoll 12
source hundredGigE 0/0/0/1
Router(config-ntp)# end
```

This step can be repeated as necessary to form associations with multiple systems.

Note To complete the configuration of a peer-to-peer association between the router and the remote device, the router must also be configured as a peer on the remote device.

Step 3 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 server 172.19.69.1 minpoll 8 maxpoll 12
```

```
 peer 192.168.22.33 minpoll 8 maxpoll 12 source HundredGigE0/0/0/1
!
```

The router is associated with other devices in mutually redundant NTP associations, enhancing time synchronization resilience across your network.

Set-up broadcast-based NTP associations

Set up your device to use NTP broadcast packets for time synchronization in a localized network with many clients.

Use broadcast-based NTP associations if your network is localized, has more than 20 clients, and requires moderate time accuracy and reliability. Consider this method for networks with limited bandwidth, system memory, or CPU resources.

Note NTP is enabled when you issue the first NTP configuration command; there is no dedicated command to enable NTP.

Before you begin

- Ensure the NTP server and clients are on the same subnet.
- Determine which interfaces will send and receive broadcast packets.

Procedure

Step 1 Enable NTP on your device by entering any NTP configuration command.

Step 2 On the NTP server, configure the interface to send NTP broadcast packets.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# broadcastdelay 2
Router(config-ntp)# interface HundredGigE 0/2/0/0
Router(config-ntp-int)# broadcast client
```

Step 3 On each client device, configure the interface to receive broadcast NTP.

Example:

```
Router(config-ntp-int)# broadcast destination 10.50.32.149
Router(config-ntp-int)# end
```

Step 4 (Optional) Set broadcast delay if needed.

Example:

```
Router(config-ntp-int)# broadcastdelay 2
```

Step 5 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 interface HundredGigE0/2/0/0
  broadcast client
  broadcast destination 10.50.32.149
 !
 broadcastdelay 2
!
```

Configure NTP access groups

Restrict or permit Network Time Protocol (NTP) access to your device by defining access groups based on access lists.

Access groups allow you to control which network devices, subnets, or hosts can synchronize with or query the device via NTP using basic IPv4 or IPv6 access lists.

NTP access group options are scanned in this order, from least to most restrictive.

- `peer` — Allows time requests and NTP control queries and allows the system to synchronize time with peers whose addresses match the access list.
- `serve` — Allows time requests and NTP control queries but does not permit the system to synchronize itself to peers.
- `serve-only` — Allows only time requests.
- `query-only` — Allows only NTP control queries.

If any access groups are specified, only those access types are granted. For details on NTP control queries, refer to RFC 1305 (NTP version 3).

For details on NTP control queries, see RFC 1305 (NTP version 3).

Procedure

Step 1 Create an access group and apply a basic IPv4 or IPv6 access list to it.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# access-group peer peer-acl
Router(config-ntp)# end
```

Step 2 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 access-group ipv4 peer peer-acl
```

```
 broadcastdelay 2
!
```

Only the devices, subnets, or hosts specified in the access lists are allowed the configured NTP access type. All other access types are denied unless explicitly permitted by an access group.

Configure NTP authentication

Ensure your device authenticates and synchronizes time only with trusted peers using encrypted NTP authentication.

Use encrypted NTP authentication to ensure your device accepts time synchronization only from designated, trusted peers. This method leverages authentication keys and a message authentication code (MAC) to provide access control and data integrity, instead of relying on IP address-based restrictions.

Before you begin

- Confirm you have access to the device CLI.
- Gather the required MD5 authentication keys.

Procedure

Step 1 Define the authentication keys.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# authenticate
Router(config-ntp)# authentication-key 3 md5 clear key1
```

Each key has a key number, a type, a value, and, optionally, a name. Currently the only key type supported is md5.

Step 2 Define trusted authentication keys.

Example:

```
Router(config-ntp)# trusted-key 3
Router(config-ntp)# commit
```

If a key is trusted, this router only synchronizes to a system that uses this key in its NTP packets.

Step 3 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 authentication-key 3 md5 encrypted 020D01425A
 authenticate
 trusted-key 3
 !
```

The device synchronizes time only with designated, trusted peers by validating NTP packets using authentication keys and an embedded MAC.

Configure the source IP address for NTP packets

Set a specific interface's IP address as the source for all NTP packets sent by the router, instead of the default interface-based source IP.

By default, a router uses the outgoing interface IP address as the source IP in NTP packets. In networks with multiple interfaces, you may need to control which interface's IP address is used as the NTP source for security, routing, or reachability purposes.

Before you begin

- Identify the interface you want to use as the NTP source.
- Confirm that NTP is enabled on your router.

Procedure

Step 1 Configure an interface from which the IP source address.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# source HundredGigE 0/0/0/1
Router(config-ntp)# end
```

Note This interface will be used as the source IP address for all NTP packets. If you need to set a source address for a specific association, use the source keyword with the peer or server command instead. For more details, see Configuring Poll-Based Associations.

Step 2 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 authentication-key 3 md5 encrypted 020D01425A
 authenticate
 trusted-key 3
 source HundredGigE0/0/0/1
!
```

Configure the system as an authoritative NTP server

Enable your router to function as an authoritative NTP server within your network, providing time synchronization to other devices even if the system is not synchronized to an external time source.

Use this task when no reliable external NTP source is available, or when you want your router to act as the main time reference for other network devices. Setting the router as an authoritative NTP server helps maintain time consistency across the network.

Before you begin

- Understand that configuring multiple authoritative NTP servers with low stratum numbers on the same network may cause time inconsistencies.

Procedure

Step 1 Make the router an authoritative NTP server.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# master 9
Router(config-ntp)# end
```



Note Use the **master** command with caution. It's easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **master** command can cause instability in time keeping if the machines don't agree on the time.

Step 2 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 master 9
```

Update the hardware clock

Ensure the hardware clock (system calendar) on your device synchronizes periodically with the more accurate software clock, especially when using NTP.

Devices with hardware clocks may experience slight time drift over periods. Synchronizing the hardware clock to the NTP-synchronized software clock maintains time accuracy, which is important for logging, authentication, and other timed operations.

Before you begin

- Confirm that Network Time Protocol (NTP) is correctly configured on your device.
- Verify that your device supports a hardware clock and the update-calendar feature.

Procedure

Step 1 Configure the router to update its system calendar from the software clock at periodic intervals.

Example:

```
Router# configure
Router(config)# ntp
Router(config-ntp)# update-calendar
Router(config-ntp)# end
```

Step 2 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 update-calendar
```

Verify the status of external reference clock

Ensure NTP is synchronized and external reference clocks are operating properly.

Procedure

Step 1 Display the status of NTP associations.

Example:

```
Router# show ntp associations
address         ref clock     st  when  poll reach  delay  offset    disp
 ~172.19.69.1      .AUTH.           16     -  1024    0    0.00   0.000   15937
 ~192.168.22.33    .AUTH.           16     -  1024    0    0.00   0.000   15937
*~127.127.1.1      .LOCL.            9    51    64   37    0.00   0.000  438.28
 * sys_peer, # selected, + candidate, - outlayer, x falseticker, ~ configured
```

Step 2 Display the status of NTP.

Example:

```
Router# show ntp status
Clock is synchronized, stratum 10, reference is 127.127.1.1
nominal freq is 1000000000.0000 Hz, actual freq is 1000000000.0000 Hz, precision is 2**24
reference time is E8CE945C.8E2A8B07 (15:01:48.555 UTC Mon Oct  9)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 63.52 msec, peer dispersion is 63.40 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.0000000000 s/s
system poll interval is 64, last update was 9 sec ago
```

```
authenticate is enabled, panic handling is disabled,
hostname resolution retry interval is 1440 minutes.
```

Disable NTP services on a specific interface

Prevent NTP packets from being received on a designated network interface.

By default, NTP services are disabled on all interfaces. However, when any NTP command is configured, NTP becomes active globally. You may need to selectively disable NTP on specific interfaces to enhance security or control synchronization sources.

Procedure

Step 1 Disable NTP services on the specified interface using one of these commands:

- interface

```
Router# configure
Router(config)# ntp
Router(config-ntp)# interface HundredGigE 0/0/0/1 disable
Router(config-ntp)# end
```

- no interface

```
Router# configure
Router(config)# ntp
Router(config-ntp)# no interface HundredGigE 0/0/0/1
Router(config-ntp)# end
```

Step 2 Verify the configured NTP profile details.

Example:

```
Router# show running-config ntp
ntp
 interface HundredGigE0/0/0/1
  disable
 !
```

FQDN for NTP server

A fully qualified domain name (FQDN) is a network identifier that

- uniquely specifies the complete path to a system within the Domain Name System (DNS) hierarchy,
- enables devices and applications to resolve hostnames dynamically to IPv4 or IPv6 addresses using DNS, and
- allows network services, such as NTP, to refer to servers without embedding static IP addresses, which simplifies service migration and management.

Starting Cisco IOS XR Software Release 7.9.1 you can configure FQDN in nondefault VRF also.

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
FQDN for NTP Server on Nondefault VRF	Release 7.9.1	You can now specify a Fully Qualified Domain Name (FQDN) as the hostname for NTP server configuration over nondefault VRFs. FQDNs are easy to remember compared to numeric IP addresses. Service migration from one host to another can cause a change in IP address leading to outages. Prior releases allowed FQDN handling in only default VRFs.

Configure FQDN on NTP server on default VRF

Configure an NTP server on your router using a fully qualified domain name (FQDN) within the default VRF to synchronize system time.

Use this procedure when you want your router to synchronize time with an external NTP server identified by its FQDN, and you do not need to specify a custom VRF. This supports environments where only the default VRF is in use and DNS resolution is available.

Before you begin

- Ensure DNS resolution is configured and operational on the router.
- Confirm network connectivity to the intended NTP server.

Procedure

Step 1 Specify the NTP server using the FQDN

Example:

```
Router# configure
Router(config)# ntp server time.cisco.com
Router(config)# commit
```

You do not need to enter a VRF name; the default VRF is used automatically.

Step 2 Verify the NTP configuration.

Example:

```
Router# show running-config ntp
ntp
 server 192.0.2.1
!
```

Step 3 Verify the NTP association status.

Example:

```
Router# show ntp associations

      address       ref clock     st  when  poll reach  delay  offset    disp
 ~192.0.2.1       173.38.201.67    2    42   128    3  196.06  -14.25  3949.4
 * sys_peer, # selected, + candidate, - outlayer, x falseticker, ~ configured
```

Your router is now configured to use the specified NTP server via its FQDN in the default VRF, and NTP associations are established as verified in the output.

Configure FQDN on NTP server on nondefault VRF

Enable NTP synchronization using an FQDN in a nondefault VRF context.

Use this task when your NTP server is identified by FQDN and resides in a nondefault VRF, requiring DNS resolution on that VRF.

Before you begin

- Ensure DNS resolution is configured for the target VRF.
- Ensure the NTP server FQDN is reachable from the device.

Procedure

Step 1 Verify reachability of the FQDN using the **ping** command.

Example:

```
Router# ping time.cisco.com vrf vrf_1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.1 timeout is 2 seconds:
```

Step 2 Configure the FQDN as the NTP server or peer for the specific VRF.

Example:

```
Router# configure
Router(config)# ntp server vrf vrf_1 time.cisco.com minpoll 4 maxpoll 4 iburst
Router(config)# commit
```

Note If the FQDN you're trying to configure isn't reachable, the CLI treats it as invalid input.

Step 3 Verify the NTP configuration.

Example:

```
Router# show running-config ntp
 ntp
  server vrf vrf_1 192.0.2.1 minpoll 4 maxpoll 4 iburst
 !
```

Step 4 Verify that an NTP association is established.

Example:

```
Router# show ntp associations
 address         ref clock     st  when  poll reach  delay  offset    disp
~192.0.2.1 vrf vrf_1
                173.38.201.115  2    14    16   37  179.10  13.492  16.680
* sys_peer, # selected, + candidate, - outlayer, x falseticker, ~ configured
```

NTP-PTP interworking

NTP-PTP interworking is a time synchronization technique that

- enables the Network Time Protocol (NTP) to use Precision Time Protocol (PTP) and other high-precision time sources,
- improves system clock accuracy from milliseconds to nanosecond-level to support applications needing higher precision, and
- allows for robust synchronization, even during network delays, system bootup, switchovers, or hardware failures.

Starting with Cisco IOS XR Software Release 7.11.1, NTP-PTP interworking provides the ability to use PTP and other valid time-of-day sources, such as Data over Cable Service Interface Specification (DOCSIS) Timing Interface (DTI) and Global Positioning System (GPS), as reference clocks for the operating system. PTP delivers nanosecond-level accuracy, whereas NTP is typically accurate to within the millisecond range. By enabling NTP to reference PTP, overall synchronization precision increases, meeting the needs of demanding network and application environments.

NTP-PTP interworking also facilitates communication of status changes between NTP and PTP processes, supporting unambiguous control of the operating system time and backplane time—even in the event of bootup, switchover, or component failure. PTP's resilience against network delays ensures reliable synchronization, making NTP less likely to lose sync under adverse network conditions.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
NTP-PTP Interworking	Release 25.4.1	Introduced in this release on: Fixed Systems (8010 (ASIC: A100])(select variants only*) *This feature is now supported on: • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D

Feature Name	Release Information	Feature Description
NTP-PTP Interworking	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 (ASIC: A100])(select variants only*) *This feature is now supported on: • 8712-MOD-M • 8011-4G24Y4H-I
NTP-PTP Interworking	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 88-LC1-12TH24FH-E • 88-LC1-36EH+A8:B12 • 88-LC1-52Y8H-EM
NTP-PTP Interworking	Release 7.11.1	We have improved NTP synchronization and reliability to achieve nanosecond-level accuracy for applications that require high-precision timing. This is achieved by enabling NTP-PTP interworking which allows the use of PTP as the reference clock. As in previous releases, the NTP client continues to support polling NTP protocol-based external time servers to synchronize the local system clock and achieve accuracy within the millisecond range.

Configure NTP-PTP interworking

Enable synchronization between NTP and PTP systems for accurate timekeeping in your network.

NTP-PTP interworking allows devices using NTP to obtain time, directly or indirectly, from a PTP-enabled Grandmaster. This ensures network-wide time accuracy, especially when NTP and PTP domains coexist.

Before you begin

- Ensure that PTP is enabled on the device before configuring NTP-PTP interworking.
- For PTP, verify the Grandmaster (GM) receives its timing reference from a GPS/GNSS clock.
  - If you are configuring on a GM node, ensure the GM is locked to the GPS/GNSS clock.
  - On a Boundary Clock (BC) node, verify the BC is clocked by a GM (that is locked to GPS/GNSS).
  - On a Transparent Clock (TC) node, ensure the GM and BC are properly referenced in the chain; then configure the TC accordingly.
- If the GM doesn't have a GPS/GNSS reference, be aware the default PTP clock will be set to Jan 1, 1970.

Procedure

Step 1 Enable NTP and set the master primary reference clock to PTP.

Example:

```
Router(config)# ntp
   Router(config-ntp)# master primary-reference-clock
   Router(config-ntp)# commit
```

OR configure an NTP server that synchronizes to a nearby PTP interface (option 2)

```
Router(config)# ntp server 198.51.100.1
   Router(config-ntp)# commit
```

Replace `198.51.100.1` with the actual IP address of the PTP-synchronized NTP server or interface in your topology.

Step 2 Verify the NTP status.

Example:

```
Router# show ntp status
```

The output should indicate 'Clock is synchronized' with the correct reference.

Step 3 Verify NTP associations.

Example:

```
Router# show ntp associations
```

The output should show an association to the configured NTP server with reference type PTP, if PTP is the underlying source.

NTP is now synchronized using a PTP reference, ensuring precise timekeeping across your network. Devices in the NTP domain can accurately obtain the time from a PTP-based Grandmaster or server.