

Network Time Protocol

Network Time Protocol (NTP) synchronizes time in a network and provides:

- synchronization of time across a network of machines, and
- UDP over IP.

NTP version 3 is defined in RFC 1305. By default, NTP services are disabled on all interfaces.

- NTP time synchronization, on page 1
- Configure NTP, on page 7
- Additional references for NTP, on page 12
- Release information for NTP, on page 13

NTP time synchronization

When multiple time sources are available, such as Virtual Integrated Network System (VINES), hardware clock, or manual configuration, NTP is considered the most authoritative and overrides time set by other methods.

An NTP network receives time from sources like a radio or atomic clock and distributes it to machines in the network.

NTP efficiently synchronizes two machines within a millisecond using just one packet per minute.

NTP time accuracy mechanisms

NTP avoids syncing with machines whose time is inaccurate in two ways.

- It ignores machines that are not synchronized.
- It compares the time that it received from multiple machines and skips any machine whose time significantly differs from others, even if it has a lower stratum. This method creats a self-organizing tree of NTP servers.

NTP stratum levels

To maintain hierarchical accuracy, NTP uses stratum levels to define the distance of a device from an authoritative time source, ensuring precise synchronization across the network. For example:

- A stratum 1 server has a direct source like a radio, atomic clock, or Global Positioning System (GPS).

- A stratum 2 server gets time from a stratum 1 server.

NTP software

Some manufacturers provide NTP software for host systems and a public version for UNIX. This software lets UNIX-based servers get time from an atomic clock and share it with our routers.

NTP features

The router does not support stratum 1 connections, such as radio or atomic clock. However, it supports GPS time sources. For network time, we recommend using public NTP servers on the internet.

If the network is isolated from the internet, the router allows a machine to act as synchronized via NTP, even if its time is set using other methods. Other machines in the network can then synchronize with it via NTP.

NTP associations

NTP communications, known as associations, are statically configured using the IP addresses of peers. Accurate timekeeping is achieved through the exchange of NTP messages between associated machines.

In a LAN, NTP can use IP broadcast messages to reduce configuration complexity. Machines send or receive broadcasts, but timekeeping is less accurate due to one-way communication.

NTP security

We recommend you to use NTP security features to prevent incorrect time settings. Two options are available to secure NTP.

- Access list restrictions.
- Encrypted authentication.

NTP access group

NTP access groups define and restrict access to NTP services using access control lists (ACLs). They:

- control which systems can communicate with the NTP server or peer by specifying access types and associating them with ACLs,
- grant or deny access to an entire network, a subnet, or a specific host within a subnet, and
- are configured using the `ntp access-group` command in global configuration mode.

Access group options and behavior

The access group options are processed from least restrictive to most restrictive:

1. ipv4—configures IPv4 access lists.
2. ipv6—configures IPv6 access lists.
3. peer—allows:
    - time requests,
    - NTP control queries, and

- the system to synchronize itself to a system whose address passes the access list criteria.

4. serve—It:
   - allows time requests and NTP control queries.
   - does not allow the system to synchronize itself to a system whose address passes the access list criteria.
5. serve-only—allows only time requests from a system whose address passes the access list criteria.
6. query-only—allows only NTP control queries from a system whose address passes the access list criteria.

If a source IP matches multiple access lists, access is granted based on the first match.

If access groups are not configured, all access types are allowed.

If access groups are configured, only specified types are allowed.

For details on NTP control queries, refer to RFC 1305 (NTP Version 3).

Encrypted NTP authentication

You can use NTP authentication for access control by verifying trusted NTP packets with authentication keys, instead of relying on IP-based access lists. The authentication process:

- Create an NTP packet with an embedded MD5-generated cryptographic checksum key and send it to the receving client.
- The client verifies the checksum against trusted keys.
- The system accepts packets that have a matching authentication key and valid timestamp information, ignoring all others.

In large networks, the Range of Trusted Key Configuration feature simplifies the configuration of multiple trusted keys.

Source IP address for NTP packets

The sending interface determines the source IP of an NTP packet. Use the **ntp source interface** command in the global configuration mode to specify the source interface.

This interface serves as the source address for all packets. Use the **source** keyword within the **ntp peer** or **ntp server** command for a specific association.

Poll-based NTP associations

Network devices with NTP operate in different association modes to synchronize time with reference sources, either by polling host servers or listening to NTP broadcasts. Poll-based association modes provide high time accuracy and reliability through regular polling of time sources.

Poll-based association modes

The poll-based association uses modes to provide a high level of time accuracy and reliability. It supports two modes.

- client, and
- symmetric active

The choice of mode depends on:

- The role of the device as a timekeeping server or client.
- The proximity of the device to a Stratum 1 timekeeping server.

The table compares NTP client mode and symmetric active mode.

Table 1: Comparison of NTP client and symmetric active modes

Feature	Client mode	Symmetric active mode
Function	The device polls its assigned time-serving hosts for the current time and synchronizes with one of them.	The device polls its assigned time-serving hosts and also responds to polls from those hosts.
Type of relationship	Client-host relationship: The host does not capture or use time information from the client.	Peer-to-peer relationship: The peers retain time-related information from the client.
Use case	Best suited for file servers and workstation clients that do not provide time synchronization to other clients.	Recommended for setups with mutually redundant servers interconnected via diverse network paths.
Typical deployment	Used by devices that require time synchronization but do not provide time services to others.	Commonly used by stratum 1 and stratum 2 servers on the internet.
Command to configure	Use the **ntp server** command to specify the time server and set the device to operate in client mode.	Use the **ntp peer** command to specify the time-serving hosts and set the device to operate in symmetric active mode.

Polling considerations

Devices engage in polling when operating as a:

- client or a host in client mode, or
- peer in symmetric active mode.

Usually, polling has minimal impact on memory, CPU, and bandwidth resources. However, excessive simultaneous polling can degrade system or network performance.

To avoid performance issues:

- limit the number of direct peer-to-peer or client-to-server associations, and
- use NTP broadcasts to propagate time information within a localized network.

Broadcast-based NTP association

Broadcast-based NTP association lets you passively receive time updates from NTP servers. This is efficient for localized networks and it is:

- suitable for networks with modest time-accuracy and reliability requirements,
- preferable with more than 20 clients in a network, and
- recommended for networks with limited bandwidth, system memory, or CPU resources.

Broadcast-based NTP functionality

In broadcast client mode:

- A device listens for NTP broadcast packets sent by broadcast time servers and does not poll servers.
- Time accuracy may be slightly reduced, as time information flows only one way.

Broadcast-based NTP configuration

Broadcast-based NTP requires these considerations:

- Use the **ntp broadcast client** command to configure a router to listen for NTP broadcast packets.
- For broadcast client mode to work:
  - The broadcast server and its clients must be on the same subnet.
  - Enable the time server to transmit NTP broadcast packets on the device interface using the **ntp broadcast** command.

NTP services on a specific interface

By default, the NTP services are disabled on all interfaces and enabled globally when any NTP command is entered.

Use the **ntp disable** command in interface configuration mode to prevent NTP packets on specific interfaces.

System as an authoritative NTP server

Use the **ntp** command in global configuration mode to configure authoritative NTP server, even without synchronization to an external time source.



Note Use the **ntp primary** command with caution, as it can easily override valid time sources, especially when configured with a low stratum number. Configuring multiple machines with the **ntp primary** command in the same network may cause timekeeping instability if they do not agree on the time.

Recommendations for NTP

NTP configuration guidelines and restrictions ensure secure, accurate, and reliable implementation in your network, providing consistency and preventing vulnerabilities.

Configuration guidelines

These guidelines explain how to configure the feature for proper operation and security.

- Use the **ntp allow mode private** command to process NTP mode 7 packets, which are disabled by default.
- Use the **show running-config | include ntp** command to check if a device is configured with NTP or not. If the output contains any of these commands, then that device is vulnerable:
  - **ntp broadcast client**
  - **ntp primary**
  - **ntp multicast client**
  - **ntp peer**
  - **ntp server**

Usage guidelines

These guidelines provide recommendations for using the feature effectively in different scenarios.

- For more information on understanding Cisco software releases, see the White Paper: Cisco IOS and NX-OS Software Reference Guide.
- The **ntp refclock gps** command is supported only in the Primary Reference Time Clock (PRTC) mode.
- To mitigate the vulnerability, disable NTP as a workaround. Only configured IP packets can exploit the vulnerability. Transit traffic is not affected.

Restrictions

NTP authentication comes with certain considerations for efficient usage. These are the performance and synchronization considerations.

- Encryption and decryption in NTP authentication are CPU-intensive and may reduce time accuracy.
- Use access lists for less resource-intensive access control, if your network allows it.
- Once NTP authentication is configured, the router synchronizes and provides time only to trusted sources.

To reduce security risks and ensure reliable operation, by default:

- NTP services are disabled on all interfaces.
- The `Line Aux 0` option is disabled.

To reduce security vulnerabilities and minimize risks:

- Cisco software supporting NTPv4 is unaffected; earlier versions are vulnerable.

- NTP versions 4.2.4p7 and earlier are vulnerable to unauthenticated remote attacks that may cause a Denial of Service (DoS) condition.
- NTP peer authentication is not a workaround and remains a vulnerable configuration.
- When NTP debugging is enabled, the message "`NTP: Receive: dropping message: Received NTP private mode 7 packet`" may appear, indicating the issue.

Configure NTP

NTP configuration includes:

- Configure poll-based NTP associations
- Configure broadcast-based NTP associations
- Configure an external reference clock
- Configure NTP authentication

Configure poll-based NTP associations

Use this procedure to configure poll-based NTP associations.

Procedure

Step 1 Use the **enable** command to enable the privileged EXEC mode.

Example:

```
Router> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 Use the **ntp peer** command to form a peer association with another system.

Example:

```
Router(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer
```

The syntax of the command is: **ntp peer***ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**]

Table 2: syntax description

ntp peer	Creates a symmetric NTP association with a peer.
ip-address	IPv4 or IPv6 address of the NTP peer.

normal-sync	Uses standard NTP sync behavior (no fast or accelerated sync modes).
version *number*	NTP protocol version (1–4). Default value is 4.
key *key-id*	Authentication key ID to use (must be preconfigured).
prefer	Marks this peer as preferred during clock selection.

Step 4 Use the **ntp server** command to form a server association with another system.

Example:

```
Router(config)# ntp server 192.168.10.1 version 2 prefer
```

The syntax of the command is: **ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**]

Table 3: Syntax description

Keyword	description
ntp server	Adds an NTP server for time synchronization.
ip-address	IPv4 or IPv6 address of the NTP server.
version *number*	NTP protocol version to use (1–4). Default value is 4.
key *key-id*	Uses the specified authentication key ID (must be preconfigured).
prefer	Marks this server as the preferred source during clock selection.

Step 5 Use the **end** command to exit global configuration mode and returns to privileged EXEC mode.

Example:

```
Router(config)# end
```

Configure broadcast-based NTP associations

Use this procedure to configure broadcast-based NTP associations.

Procedure

Step 1 Use the **enable** command to enable privileged EXEC mode.

Example:

```
Router> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 Use the **interface** command to configure an interface and enter interface configuration mode.

Example:

```
Router(config)# interface GigabitEthernet 0/0/0
```

Step 4 Use the **ntp broadcast version** command to configure the specified interface to send NTP broadcast packets.

Example:

```
Router(config-if)# ntp broadcast version 2
```

Step 5 Use the **ntp broadcast client** command to configure the specified interface to receive NTP broadcast packets.

Example:

```
Router(config-if)# ntp broadcast client
```

Step 6 Use the **ntp broadcastdelay** command to adjust the estimated round-trip delay for NTP broadcasts.

Example:

```
Router(config-if)# ntp broadcastdelay 100
```

Step 7 Use the **end** command to exit the interface configuration mode and return to privileged EXEC mode.

Example:

```
Router(config)# end
```

Configure an external reference clock

Use this procedure to configure an external reference clock for synchronization.

Procedure

Step 1 Use the **enable** command to enable the privileged EXEC mode.

Example:

```
Router> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 Use the **line aux** command to enter line configuration mode for the auxiliary port 0.

Example:

```
Router(config)# line aux 0
```

Step 4 Use the **end** command to exit line configuration mode and returns to privileged EXEC mode.

Example:

```
Router(config-line)# end
```

Step 5 (Optional) Use the **show ntp associations** command to view the status of NTP associations, including the status of the GPS reference clock.

Example:

```
Router# show ntp associations
```

Step 6 (Optional) Use the **show ntp status** command to view the status of NTP.

Example:

```
Router# show ntp status
```

Step 7 (Optional) Use the **debug ntp refclock** command to check the reference clock activities.

Example:

```
Router# debug ntp refclock
```

Configure NTP authentication

Use this procedure to configure NTP authentication.

Procedure

Step 1 Use the **enable** command to enable privileged EXEC mode.

Example:

```
Router> enable
```

Enter your password if prompted.

Step 2 Use the **configure terminal** command to enter global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 Use the **ntp authenticate** command to enable the NTP authentication.

Example:

```
Router(config)# ntp authenticate
```

Step 4 Use the **ntp authentication-key** command to define authentication keys.

Example:

```
Router(config)# ntp authentication-key 1 md5 key1
```

Each key is defined by a key number, a type, and a value.

Step 5 Use the **ntp trusted-key** command to define trusted authentication keys.]

Example:

```
Router(config)# ntp trusted-key 1 - 3
```

If a key is trusted, this device can synchronize with a system that uses this key in its NTP packets.

Step 6 Use the **ntp server** command to synchronize the software clock with an NTP time server.

Example:

```
Router(config)# ntp server 172.16.22.44 key 2
```

Step 7 Use the **end** command to exit global configuration mode and returns to privileged EXEC mode.

Example:

```
Router(config)# end
```

Additional references for NTP

This table lists the NTP reference documents.

Table 4: NTP reference documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases Guide
Basic System Management commands	Basic System Management Command Reference
NTPv4 in IPv6	*Cisco IOS Basic System Management Guide*
IP extended access lists	*Cisco IOS IP Addressing Configuration Guide*
IPX extended access lists	*Novell IPX Configuration Guide*
NTP package vulnerability	*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability (DoS)*
Cisco IOS and NX-OS software releases	*'White Paper: Cisco IOS and NX-OS Software Reference Guide*

Standards and RFCs

Standard/RFCs	Title
RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*

Technical assistance

Description	Link
The Cisco technical documentation website provides online resources for downloading documentation, software, and tools. Use these resources to install and configure the software. Troubleshoot and resolve technical issues with Cisco products and technologies using these resources. Access to most tools on the Cisco technical documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Additional references for NTP

This table lists the NTP reference documents.

Table 5: NTP reference documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases Guide
Basic System Management commands	Basic System Management Command Reference
NTPv4 in IPv6	*Cisco IOS Basic System Management Guide*
IP extended access lists	*Cisco IOS IP Addressing Configuration Guide*
IPX extended access lists	*Novell IPX Configuration Guide*
NTP package vulnerability	*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability (DoS)*
Cisco IOS and NX-OS software releases	*'White Paper: Cisco IOS and NX-OS Software Reference Guide*

Standards and RFCs

Standard/RFCs	Title
RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*

Technical assistance

Description	Link
The Cisco technical documentation website provides online resources for downloading documentation, software, and tools. Use these resources to install and configure the software. Troubleshoot and resolve technical issues with Cisco products and technologies using these resources. Access to most tools on the Cisco technical documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Release information for NTP

This table shows the software release that introduced each feature and lists later releases in the same train supporting the feature unless stated otherwise.

Table 6: Feature information

Feature Name	Feature Information
Network Time Protocol	NTP is a protocol designed to time-synchronize a network of machines. NTP runs on UDP, which in turn runs on IP. NTP is documented in RFC 1305.

You can use Cisco Feature Navigator to find platform and software image support information at www.cisco.com/go/cfn. A Cisco.com account is not required.