

# Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 is documented in RFC 1305.

NTP services are disabled on all interfaces by default.

Networking devices running NTP can be configured to operate in a variety of association modes when synchronizing time with reference time sources.

Line Aux 0 option is disabled by default.

When you configure both IP address and FQDN of the same NTP server in Cisco IOS XE, only the FQDN configuration is displayed in the **show running-config** command output after FQDN resolves to the same IP address.

This module describes how to configure Network Time Protocol on Cisco devices.


- Restrictions for Network Time Protocol, on page 1
- Information About Network Time Protocol, on page 2
- How to Configure Network Time Protocol, on page 7
- Configuration Examples for Network Time Protocol, on page 15
- Additional References for Network Time Protocol, on page 16
- Feature Information for Network Time Protocol, on page 17


# Restrictions for Network Time Protocol

The Network Time Protocol (NTP) package contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. NTP versions 4.2.4p7 and earlier are vulnerable.

The vulnerability is due to an error in handling of certain malformed messages. An unauthenticated, remote attacker could send a malicious NTP packet with a spoofed source IP address to a vulnerable host. The host that processes the packet sends a response packet back to the transmitter. This action could start a loop of messages between the two hosts that could cause both the hosts to consume excessive CPU resources, use up the disk space by writing messages to log files, and consume the network bandwidth. All of these could cause a DoS condition on the affected hosts.

For more information, see theNetwork Time Protocol Package Remote Message Loop Denial of Service Vulnerability web page.

Cisco software releases that support NTPv4 are not affected. All other versions of Cisco software are affected.

To display whether a device is configured with NTP, use the **show running-config | include ntp** command. If the output returns any of the following commands, then that device is vulnerable to the attack:

- **ntp broadcast client**
- **ntp primary**
- **ntp multicast client**
- **ntp peer**
- **ntp server**

There are no workarounds for this vulnerability other than disabling NTP on the device. Only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Depending on your release, your feature will process NTP mode 7 packets and will display the message "NTP: Receive: dropping message: Received NTP private mode 7 packet " if debugs for NTP are enabled. Configure the **ntp allow mode private** command to process NTP mode 7 packets. This command is disabled by default.

**Note** NTP peer authentication is not a workaround and is a vulnerable configuration.

# Information About Network Time Protocol

## Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to the accuracy of within a millisecond of one another.

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

NTP has two ways to avoid synchronizing to a machine whose time may not be accurate. NTP will never synchronize to a machine that is not in turn synchronized. NTP will compare the time reported by several machines, and will not synchronize to a machine whose time is significantly different from others, even if its stratum is lower. This strategy effectively builds a self-organizing tree of NTP servers.

The Cisco implementation of NTP does not support stratum 1 service; that is, you cannot connect to a radio or atomic clock (for some specific platforms, however, you can connect to a GPS time-source device). Cisco recommends that the time service for your network be derived from the public NTP servers available in the IP Internet.

If the network is isolated from the Internet, the Cisco implementation of NTP allows a machine to be configured so that it acts as though it is synchronized via NTP, when in fact it has determined the time using other means. Other machines can then synchronize to that machine via NTP.

A number of manufacturers include NTP software for their host systems and a publicly available version for systems running UNIX. This software also allows UNIX-derivative servers to acquire the time directly from an atomic clock, which would subsequently propagate time information along to Cisco routers.

The communications between machines running NTP (known as associations) are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is made possible through exchange of NTP messages between each pair of machines with an association.

However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each machine can be configured to send or receive broadcast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

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

When multiple sources of time (Virtual Integrated Network System (VINES), hardware clock, manual configuration) are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

NTP services are disabled on all interfaces by default. See How to Configure Network Time Protocol to enable NTP services.

## NTP Support for IPv6 Networks

***Table 1: Feature History***

| Feature Name | Release Information | Feature Description |
|---|---|---|
| NTP Support for IPv6 Networks | Cisco IOS XE Release 17.11.1 | Network Time Protocol (NTP) synchronizes device clocks across networks to maintain system accuracy. In this release, NTP supports IPv6 multicast networks. The NTP server sends clock updates as multicast messages to the clients across IPv6 networks. As NTP packets are sent only to the intended clients, it reduces timing traffic in the network. |

NTP version 4 supports IPv6 networks. It provides the following capabilities:

- Synchronizes time over IPv6 networks.
- Provides a security framework based on public key cryptography and standard X509 certificates.
- Uses specific multicast groups and automatically calculates its time-distribution hierarchy through an entire network. NTP automatically configures the hierarchy of the servers in order to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

# NTP Association Modes

There are different modes in which a NTP-enabled router gathers information about its peer with which it is associated. Using one of the modes listed below, NTP collects peer details:

- Poll
- Broadcast
- Multicast

## Poll-Based NTP Associations

Networking devices running NTP can be configured to operate in variety of association modes when synchronizing time with reference time sources. A networking device can obtain time information on a network in two ways—by polling host servers and by listening to NTP broadcasts. This section focuses on the poll-based association modes. Broadcast-based NTP associations are discussed in the *Broadcast-Based NTP Associations* section.

The following are the two most commonly used poll-based association modes:

- Client mode
- Symmetric active mode

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 will then pick a host from among all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host will not capture or use any time information sent by the local client device. This mode is most suited for file-server and workstation clients that are not required to provide any form of time synchronization to other local clients. Use the **ntp server** command to individually specify the time server 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 will also retain time-related information of the local networking device that it is communicating with. This mode should be used when a number of mutually redundant servers are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet adopt this form of network setup. Use the **ntp 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.

The specific mode that you should set for each of your networking devices depends primarily on the role that you want them to assume as a timekeeping device (server or client) and the device's proximity to a stratum 1 timekeeping server.

A networking device engages in polling when it is operating as a client or a host in the client mode or when it is acting as a peer in the symmetric active mode. Although polling does not usually place a burden on memory and CPU resources such as bandwidth, an exceedingly large number of ongoing and simultaneous polls on a system can seriously impact the performance of a system or slow the performance of a given network. To avoid having an excessive number of ongoing polls on a network, you should limit the number of direct, peer-to-peer or client-to-server associations. Instead, you should consider using NTP broadcasts to propagate time information within a localized network.

### Broadcast-Based NTP Associations

Broadcast-based NTP associations should be used when time accuracy and reliability requirements are modest and if your network is localized and has more than 20 clients. Broadcast-based NTP associations are also recommended for use on networks that have limited bandwidth, system memory, or CPU resources.

A networking device operating in the broadcast client mode does not engage in any polling. Instead, it listens for NTP broadcast packets that are transmitted by broadcast time servers. Consequently, time accuracy can be marginally reduced because time information flows only one way.

The NTP server and client can communicate using IPv4 broadcast messages.

Use the **ntp broadcast client** command to set your networking device to listen for NTP broadcast packets propagated through a network. For broadcast client mode to work, the broadcast server and its clients must be located on the same subnet. You must enable the time server that transmits NTP broadcast packets on the interface of the given device by using the **ntp broadcast** command.

### Multicast-Based NTP Associations

Multicast mode is used when you intend having a time source that sends out time to multiple clients—One source and many clients. You must configure multicast capabilities and all related commands on the server and the client. NTP version 4 uses IPv6 multicast messages to send and receive clock updates.

The multicast server periodically sends clock synchronization messages to the multicast address that you have configured. Clients listen to these messages and synchronize to the server. In the multicast mode, the synchronization is only one-way—A multicast client to a multicast server. A multicast server can provide time synchronization for clients in the same subnet or in different subnets.

A multicast client is enabled by using the **ntp multicast client** command and specifying the multicast group address.

## NTP Access Group

The access list-based restriction scheme allows you to grant or deny certain access privileges to an entire network, a subnet within a network, or a host within a subnet. To define an NTP access group, use the **ntp access-group** command in global configuration mode.

The access group options are scanned in the following order, from least restrictive to the most restrictive:

1. **ipv4**—Configures IPv4 access lists.
2. **ipv6**—Configures IPv6 access lists.
3. **peer**—Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
4. **serve**—Allows time requests and NTP control queries, but 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 the source IP address matches the access lists for more than one access type, the first type is granted access. If no access groups are specified, all access types are granted access to all systems. If any access groups are specified, only the specified access types will be granted access.

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

The encrypted NTP authentication scheme should be used when a reliable form of access control is required. Unlike the access list-based restriction scheme that is based on IP addresses, the encrypted authentication scheme uses authentication keys and an authentication process to determine if NTP synchronization packets sent by designated peers or servers on a local network are deemed as trusted before the time information that they carry along with them is accepted.

The authentication process begins from the moment an NTP packet is created. Cryptographic checksum keys are generated using the message digest algorithm 5 (MD5) and are embedded into the NTP synchronization packet that is sent to a receiving client. Once a packet is received by a client, its cryptographic checksum key is decrypted and checked against a list of trusted keys. If the packet contains a matching authentication key, the time-stamp information that is contained within the packet is accepted by the receiving client. NTP synchronization packets that do not contain a matching authenticator key are ignored.

**Note** In large networks, where many trusted keys must be configured, the Range of Trusted Key Configuration feature enables configuring multiple keys simultaneously.

It is important to note that the encryption and decryption processes used in NTP authentication can be very CPU-intensive and can seriously degrade the accuracy of the time that is propagated within a network. If your network setup permits a more comprehensive model of access control, you should consider the use of the access list-based form of control.

After NTP authentication is properly configured, your networking device will synchronize with and provide synchronization only to trusted time sources.

## NTP Services on a Specific Interface

Network Time Protocol (NTP) services are disabled on all interfaces by default. NTP is enabled globally when any NTP commands are entered. You can selectively prevent NTP packets from being received through a specific interface by using the **ntp disable** command in interface configuration mode.

## Source IP Address for NTP Packets

When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** *interface* command in global configuration mode to configure a specific interface from which the IP source address will be taken.

This interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** command.

## System as an Authoritative NTP Server

Use the **ntp** command in global configuration mode if you want the system to be an authoritative NTP server, even if the system is not synchronized to an outside time source.

**Note** Use the **ntp primary** command with caution. It is very 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 **ntp primary** command can cause instability in timekeeping if the machines do not agree on the time.

# How to Configure Network Time Protocol

## Configuring NTP

There are different modes in which a NTP-enabled router gathers information about its peer with which it is associated. You can configure the router to synchronize its clock with the intended server by using several modes.

### Configuring Poll-Based NTP Associations

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ntp peer** *ip-address* \|*ipv4*\| \|*ipv6*\| [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**]<br>**Example:**<br>`Device(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer` | Forms a peer association with another system. |
| **Step 4** | **ntp server** *ip-address* \|*ipv4*\| \|*ipv6*\| [**version** *number*] [**key** *key-id*] [**prefer**]<br>**Example:**<br>`Device(config)# ntp server 192.168.10.1 version 2 prefer` | Forms a server association with another system. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring Broadcast-Based NTP Associations

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **ntp broadcast version** *number*<br>**Example:**<br>`Device(config-if)# ntp broadcast version 2` | Configures the specified interface to send NTP broadcast packets. |
| **Step 5** | **ntp broadcast client**<br>**Example:**<br>`Device(config-if)# ntp broadcast client` | Configures the specified interface to receive NTP broadcast packets. |
| **Step 6** | **ntp broadcastdelay** *microseconds*<br>**Example:**<br>`Device(config-if)# ntp broadcastdelay 100` | Adjusts the estimated round-trip delay for NTP broadcasts. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Configuring Multicast-Based NTP Associations

To facilitate the configuration of multicast-based NTP associations, you must configure the required interface to send and receive NTP multicast packets.

## Configuring an Interface to Send NTP Multicast Packets

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface fastethernet 0/0` | Specifies an interface type and number, and places the router in interface configuration mode. |
| **Step 4** | **ntp multicast** {*ip-address* \| *ipv6-address*} [**key** *key-id*] [**ttl** *value*] [**version** *number*]<br>**Example:**<br>`Router(config-if)# ntp multicast FF02::1:FF0E:8C6C` | Configures a system to send NTPv4 multicast packets on a specified interface. We support only IPv6 multicast addresses. |

## Configuring an Interface to Receive NTP Multicast Packets

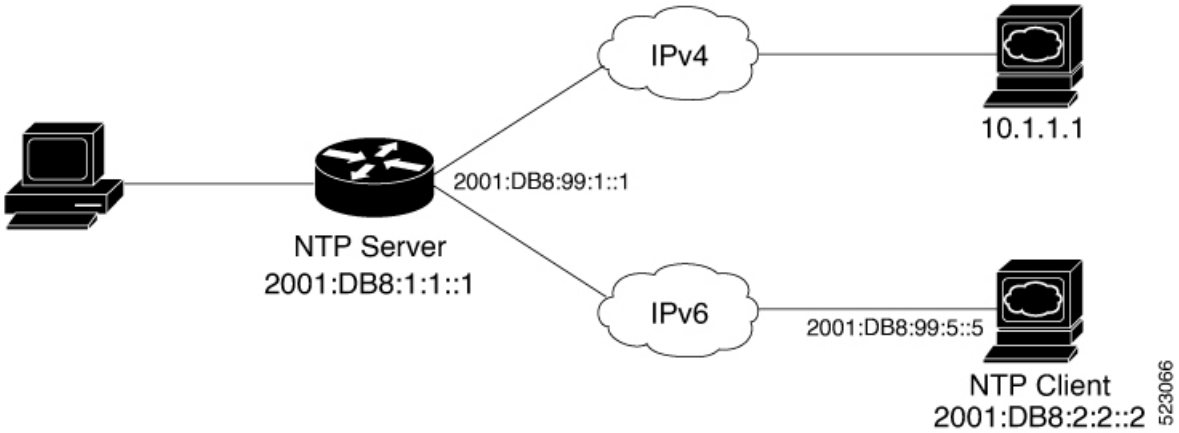
### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface FastEthernet 0/0` | Specifies an interface type and number, and places the router in interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ntp multicast client** {*ip-address* \| *ipv6-address*} [**novolley**]<br>**Example:**<br>`Router(config-if)# ntp multicast client FF02::2:FF0E:8C6C` | Configures the system to receive NTP multicast packets on a specified interface. We support only IPv6 multicast addresses. |

## Configuring NTP for IPv6 Networks

The configuration is based on the following topology:




The following sections cover the NTP server and client configurations.

### Configuring NTP on the Server

#### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ntp master**<br>**Example:**<br>`Router(config)#ntp master` | Enables NTP on the server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ntp peer** *NTP client IPv6 address*<br>**Example:**<br>`Router(config)#ntp peer <2001:DB8::2>` | Specify the NTP client's IPv6 address on the server to send the synchronization request to the client. |

*Verification-NTP Server*

This output shows that the NTP server clock synchronizes time with its own clock. The address 127.127.1.1 is the loopback IP address that is assigned by the **ntp master** command. The NTP server may take several minutes before it synchronizes its clock with itself.

```
NTPserver# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0011 Hz, precision is 2**10
ntp uptime is 60200 (1/100 of seconds), resolution is 4000
reference time is E78DDD9B.F7CEDBC0 (14:06:43.968 IST Wed Feb 8 2023)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000004627 s/s
system poll interval is 16, last update was 10 sec ago.
```

This shows the peer device of the NTP server.

```
R2#show ntp associations
address         ref clock       st   when   poll reach  delay  offset   disp
~2001:DB8:2:2::2 .TIME.         16    -     64    0     0.000   0.000  15937.
*~127.127.1.1     .LOCL.        7     11    16   377    0.000   0.000  1.204
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

## Configuring NTP on the Client

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ntp client**<br>**Example:**<br>`Router(config)#ntp client` | Enables NTP on the client. |
| **Step 4** | **ntp peer** *NTP server IPv6 address*<br>**Example:**<br>`Router(config)#ntp server 2001:DB8::1` | Specify the server IPv6 address. The client listens to the synchronization request sent by the server, and synchronizes its clock with the server. |

*Verification-NTP Client*

This output shows that the NTP client clock is synchronized with the NTP server. It also displays its stratum value and the IP address of the clock that it references.

```
NTPserver# show ntp status
Clock is synchronized, stratum 9, reference is 2001:DB8:1:1::1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 69300 (1/100 of seconds), resolution is 4000
reference time is E78DDDFB.99581208 (14:08:19.599 IST Wed Feb 8 2023)
clock offset is -6.5000 msec, root delay is 3.00 msec
root dispersion is 14.70 msec, peer dispersion is 2.56 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000199 s/s
system poll interval is 128, last update was 13 sec ago.
```

This output shows the peer device of the NTP client.

```
R2#show ntp associations
          address           ref clock      st   when   poll reach  delay  offset   disp
*~2001:DB8::12001:DB8::1     8     17    128   377  3.000  -6.500  2.565
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

## Configuring an External Reference Clock

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **line aux** *line-number*<br>**Example:**<br>`Device(config)# line aux 0` | Enters line configuration mode for the auxiliary port 0. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-line)# end` | Exits line configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **show ntp associations**<br>**Example:**<br>`Device# show ntp associations` | Displays the status of NTP associations, including the status of the GPS reference clock. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show ntp status**<br>**Example:**<br>`Device# show ntp status` | Displays the status of NTP. |
| **Step 7** | **debug ntp refclock**<br>**Example:**<br>`Device# debug ntp refclock` | Allows advanced monitoring of reference clock activities for the purposes of debugging. |

## Configuring NTP Authentication

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ntp authenticate**<br>**Example:**<br>`Device(config)# ntp authenticate` | Enables the NTP Authentication feature. |
| **Step 4** | **ntp authentication-key** *number* **md5** *key*<br>**Example:** | Defines authentication keys.<br>• Each key has a key number, a type, and a value. |
| **Step 5** | **ntp authentication-key** *number* **md5** *key*<br>**Example:** | Defines authentication keys.<br>• Each key has a key number, a type, and a value. |
| **Step 6** | **ntp authentication-key** *number* **md5** *key*<br>**Example:** | Defines authentication keys.<br>• Each key has a key number, a type, and a value. |
| **Step 7** | **ntp trusted-key** *key-number* [- *end-key*] | Defines trusted authentication keys. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# ntp trusted-key 1 - 3` | • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets. |
| **Step 8** | **ntp server** *ip-address* **key** *key-id*<br>**Example:**<br>`Device(config)# ntp server 172.16.22.44 key 2` | Allows the software clock to be synchronized by an NTP time server.<br>**Note** When multiple NTP servers are configured and logging is enabled, clock synchronization lost messages are randomly seen on the device. To resolve this issue, configure the NTP server using **peer** keyword.<br>`Device(config)# ntp server ip-address [version number] [key key-id] [prefer]` |
| **Step 9** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Verifying Network Time Protocol

**Procedure**

**Step 1** **show clock** [**detail**]

This command displays the current software clock time. The following is sample output from this command.

**Example:**

```
Device# show clock detail

*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar
```

**Step 2** **show ntp associations detail**

This command displays the status of NTP associations. The following is sample output from this command.

**Example:**

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
```

```
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D0CDE881.9A6A9005 (18:42:09.603 UTC Tue Jan 4 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
192.168.45.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

**Step 3** **show ntp status**

This command displays the status of NTP. The following is sample output from this command.

**Example:**

```
Device# show ntp status

Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
reference time is D25AF07C.4B439650 (15:26:04.294 PDT Tue Oct 21 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 10 sec ago.
```

# Configuration Examples for Network Time Protocol

## Example: Configuring Network Time Protocol

In the following example, a device with a hardware clock that has server associations with two other systems sends broadcast NTP packets, periodically updates the hardware clock, and redistributes time into VINES:

```
clock timezone PST -8
clock summer-time PDT recurring

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
```

In the following example, a device with a hardware clock has no outside time source, so it uses the hardware clock as an authoritative time source and distributes the time via NTP broadcast packets:

```
clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
```

The following example shows Line Aux 0 option is disabled by default.

```
config-register 0x0
reload
rommon 1 > set
rommon 2 >  AUX_PORT=1
rommon 3 > SYNC
rommon 4 > reset
rommon 1 > set
rommon 2 > confreg 0x2102
rommon 3 > reset
```

# Additional References for Network Time Protocol

### Related Documents

| Related Topic | Document Title |
|---|---|
| Basic System Management commands | Basic System Management Command Reference |
| NTP4 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* |
| 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 Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Network Time Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

*Table 2: Feature Information for Network Time Protocol*

| Feature Name | Releases | 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. |