

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.

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

- Information About Network Time Protocol, on page 1
- Best practices for NTP configuration, on page 8
- How to Configure Network Time Protocol, on page 9
- Configuration Examples for Network Time Protocol, on page 25
- Additional References for Network Time Protocol, on page 26
- Feature Information for Network Time Protocol, on page 27

Information About Network Time Protocol

Time and Calendar Services

The primary source for time data on your system is the software clock. This clock runs from the moment the system starts up and keeps track of the current date and time. The software clock can be set from a number of sources and in turn can be used to distribute the current time through various mechanisms to other systems. When a device with a hardware clock is initialized or rebooted, the software clock is initially set based on the time in the hardware clock. The software clock can then be updated from the following sources:

- Manual configuration (using the hardware clock)
- Network Time Protocol (NTP)
- Simple Network Time Protocol (SNTP)
- Virtual Integrated Network Service (VINES) Time Service

Because the software clock can be dynamically updated, it has the potential to be more accurate than the hardware clock.

The software clock can provide time to the following services:

- Access lists
- Logging and debugging messages

- NTP
- The hardware clock
- User **show** commands
- VINES Time Service



Note The software clock cannot provide time to the NTP or VINES Time Service if the clock was set using SNTP.

The software clock keeps track of time internally based on the Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that time is displayed correctly relative to the local time zone.

The software clock keeps track of whether the time is authoritative (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time will be available only for display purposes and will not be redistributed.

Network Time Protocol

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 Version 3 (NTPv3) 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 does not synchronize to a machine that is not in turn synchronized with the NTP. NTP compares the time reported by several machines and does 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.

Our 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). We recommend that the time service you derive for your network from the public NTP servers that are available in the IP Internet.

If the network is isolated from the Internet, our implementation of NTP allows a machine to be configured so that it acts as though it is synchronized via NTP, when in fact the network has determined the time by 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 devices.

The communication 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 only one way.

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

When multiple sources of time (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.

For more information about NTP, see the following sections:

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.

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.

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.

Orphan Mode

The NTP subnet is sometimes isolated from local reference clocks or Internet clock servers. During this period of isolation, the subnet servers and clients are synchronized to a common time scale. The local clock driver simulates a UTC source to provide a common time scale. A server connected to the driver directly or indirectly synchronizes the other hosts in the subnet.

Using a local clock driver may sometimes result in irrecoverable failures of the subnet, and maintaining redundancy using multiple servers is not feasible. The Orphan Mode feature, which does not have any such disadvantages, eliminates the need for a local clock driver. The Orphan Mode feature provides a single simulated UTC source with multiple servers and a seamless switching mechanism as servers recover from a failure.

In private networks, one or multiple core servers operating at the lowest stratum is normally included. You must configure each of these servers as backups for other servers using symmetric or broadcast modes. Even if one core server reaches a UTC source, the entire subnet synchronizes to the simulating server. If none of the servers reach a UTC source, one of the servers, which is known as the orphan parent, can simulate a UTC source, and serve as the simulated UTC source for all the other hosts, known as orphan children, in the subnet.

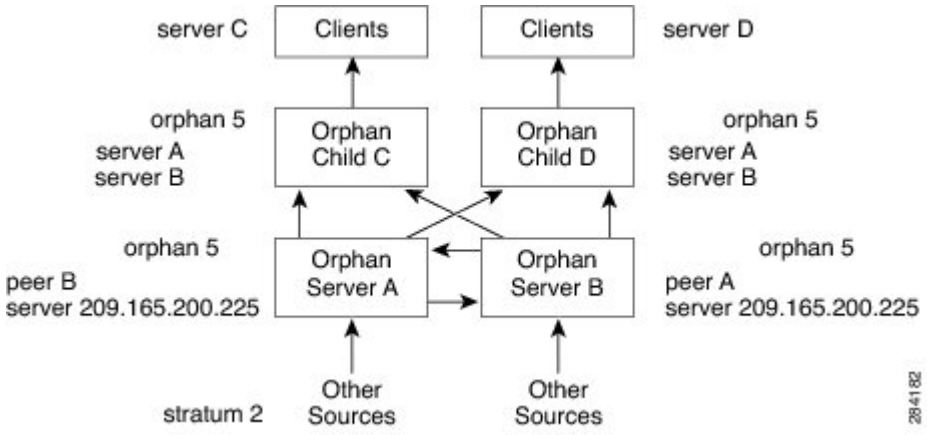
Use the **ntp orphan** *stratum* command to enable a host for orphan mode, where *stratum* is a stratum value less than 16 and greater than any stratum value that occurs in the configured Internet time servers. However, you must provide sufficient stratums so that every subnet host dependent on the orphan children has a stratum value less than 16. If no associations for other servers or reference clocks are configured, you must set the orphan stratum value to 1.

An orphan parent operating at stratum 1 with no sources displays the reference ID LOOP. An orphan parent not operating at stratum 1 displays the UNIX loopback address 127.0.0.1. Ordinary NTP clients use a selection metric based on delay and dispersion, whereas orphan children use a metric computed from the IP address of each core server in the subnet. Each orphan child selects the orphan parent with the smallest metric as the root server.

A server that loses all sources, continuously synchronizes the local clock driver with other servers, thus backing up the server. Enable orphan mode only in core servers and orphan children.

The following figure illustrates how orphan mode is set up, and a peer network configuration, where two primary or secondary (stratum 2) servers are configured with reference clocks or public Internet primary servers, with each using symmetric modes.

Figure 1: Orphan Mode Setup



Prerequisites for Orphan Mode

To ensure smooth function of the orphan mode, you must configure each core server with available sources to operate at the same stratum. Configure the **ntp orphan** command in all the core servers and the orphan children. Configure each orphan child with all root servers.

Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP. SNTP can receive only the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection. An SNTP client is more vulnerable to servers that have unexpected behavior than an NTP client, and should be used only in situations where strong authentication is not required.

You can configure SNTP to request and accept packets from configured servers or to accept NTP broadcast packets from any source. When multiple sources are sending NTP packets, the server with the best stratum is selected. (See the *Network Time Protocol* section on page 3 for a description of strata.) If multiple servers are at the same stratum, a configured server is preferred over a broadcast server. If multiple servers pass both tests, the first one to send a time packet is selected. SNTP will choose a new server only if it stops receiving packets from the currently selected server, or if a better server (according to the criteria described) is discovered.

VINES Time Service

Time service is available when Banyan VINES is configured. This protocol is a standard part of VINES. The Cisco implementation allows the VINES time service to be used in two ways. First, if the system has learned the time from some other source, it can act as a VINES time server and provide time to other machines running VINES. Second, it can use the VINES time service to set the software clock if no other form of time service is available.



Note Support for Banyan VINES and Xerox Network Systems (XNS) is not available in all releases.

Hardware Clock

Some devices contain a battery-powered hardware clock that tracks the date and time across system restarts and power outages. The hardware clock is always used to initialize the software clock when the system is restarted.



Note Within the CLI command syntax, the hardware clock is referred to as the system calendar.

If no other source is available, the hardware clock can be considered as an authoritative source of time and be redistributed via NTP. If NTP is running, the hardware clock can be updated periodically from NTP, compensating for the inherent drift, which is the consistent gain or loss of time at a certain rate if the hardware clock is left to run.

You can configure a hardware clock (system calendar) on any device to be periodically updated from the software clock. We recommend that you use this configuration for any device using NTP, because the time and date on the software clock (set using NTP) will be more accurate than the hardware clock, because the time setting on the hardware clock has the potential to drift slightly over time.

Use the **ntp update-calendar** command in global configuration mode if a routing device is synchronized to an outside time source via NTP and you want the hardware clock to be synchronized to NTP time.

Time Ranges

The Cisco software allows implementation of features based on the time of day. The **time-range** global configuration command defines specific times of the day and week, which can then be referenced by a function, so that those time restrictions are imposed on the function itself.

Depending on your release, IP and Internetwork Packet Exchange (IPX) extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to the introduction of this feature, access list statements were always in effect once they were applied. Both named and numbered access lists can reference a time range.



Note The time range relies on the system's software clock. For the time range feature to work the way you intend, you need a reliable clock source. We recommend that you use NTP to synchronize the system's software clock.

Benefits of time ranges include the following:

- The network administrator has more control over permitting or denying a user access to resources. These resources could be an application (identified by an IP address/mask pair and a port number), policy routing, or an on-demand link (identified as interesting traffic to the dialer).
- Network administrators can set a time-based security policy, including the following:
  - Perimeter security using the Cisco Firewall feature set or access lists.
  - Data confidentiality with Cisco Encryption Technology or IP security.
- Policy-based routing and queueing functions are enhanced.
- When provider access rates vary by time of day, traffic can be rerouted automatically and cost-effectively.
- Service providers can dynamically change a committed access rate (CAR) configuration to support the quality of service (QoS) service level agreements (SLAs) that are negotiated for certain times of the day.

Network administrators can control logging messages. Access list entries can log traffic at certain times of the day, but not constantly. Therefore, administrators can deny access without the need to analyze the many logs generated during peak hours.

Best practices for NTP configuration

Use these instructions to 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.

1. Configuration checks:
   - Configure multiple redundant NTP time sources to avoid reliance on a single server and improve reliability by using the **ntp server** <*ip-address*> [**minpoll** <*value*>] [**maxpoll** <*value*>] command.
   - Use **ntp source Loopback0** command to set a loopback interface as the NTP source for consistency across device reboots and interface changes.

- Configure NTP authentication to secure communications and prevent malicious time alterations by using these commands:
  - **ntp authenticate**
  - **ntp authentication-key**
  - **ntp trusted-key**
- Configure the **ntp panic-threshold-apply** command to check the configuration sanity checks, which reject large clock changes and prevent network instability.
- Configure multiple authentication keys with overlapping lifetimes using **ntp authentication-key** and appropriate key management to prevent routing disruptions caused by expired keys during key transitions.

2. Monitoring checks:
   - Regularly monitor and validate NTP synchronization status using **show ntp status** and **show ntp associations** commands to ensures timely detection of synchronization issue.

How to Configure Network Time Protocol

Configuring NTP

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 the Network 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**

For more information on understanding Cisco software releases, see the White Paper: Cisco IOS and NX-OS Software Reference Guide.

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.

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. A networking device can obtain time information on a network in two ways: by polling host servers and by listening to NTP broadcasts.

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.

Configuring Poll-Based NTP Associations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp peer** [**vrf** *vrf-name*] {*ip-address*|*ipv6-address*|**ip**|**ipv6**] *hostname*} [**version number**] [**key** *key-id*] [**minpoll** *minpoll-value*] [**maxpoll***maxpoll-value*] [**prefer**] [**source**] [**periodic**]
4. **ntp server** [**vrf** *vrf-name*] {*ip-address*|*ipv6-address*|**ip**|**ipv6**] *hostname*} [**version number**] [**key** *key-id*] [**minpoll** *minpoll-value*] [**maxpoll** *maxpoll-value*] [**prefer**] [**source**] [**periodic**]
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Device# configure terminal`	
Step 3	**ntp peer** [**vrf** *vrf-name*] {*ip-address*|*ipv6-address*|**ip**|**ipv6**] *hostname*} [**version number**] [**key** *key-id*] [**minpoll** *minpoll-value*] [**maxpoll***maxpoll-value*] [**prefer**] [**source**] [**periodic**] **Example:** `Device(config)# ntp peer 192.168.10.1 version 2 prefer`	Forms a peer association with another system. • **VRF** *vrf-name*: Specifies the VRF instance for routing to the NTP server. • **ip-address**: IPv4 address of the NTP server. • **IPv6-address**: Accepts full IPv6 addresses for the NTP server. • **IP hostname**: Forces DNS resolution to IPv4 when configuring by hostname. • **IPv6 hostname**: Forces DNS resolution to IPv6 when configuring by hostname. • **Hostname**: A DNS hostname can be used instead of an IP address. • **Version number**: Defines the NTP version number (range 1 to 4). The default value is four. • **Key** *key-id*: Specifies the authentication key ID (1 to 4294967295) used for communication with the NTP server. • **Minpoll**: Minimum polling interval in powers of two seconds (e.g., 4 = 16s, 6 = 64s). The default value is six (64 seconds). • **Maxpoll**: Maximum polling interval in powers of two seconds (e.g., 10 = 1024s). The default value is ten (1024 seconds). • **Prefer**: Marks this server as the preferred NTP server. • **Source**: Specifies the source interface for NTP packets. • **Periodic**: Valid only with hostname; periodically re-resolves DNS and switches to a new server if the current one becomes unavailable. **Note** NTP peers cannot be configured using both hostname and IP simultaneously. To switch methods, you must delete the existing entry before configuring the new one.
Step 4	**ntp server** [**vrf** *vrf-name*] {*ip-address*|*ipv6-address*|**ip**|**ipv6**] *hostname*} [**version number**] [**key** *key-id*] [**minpoll** *minpoll-value*] [**maxpoll** *maxpoll-value*] [**prefer**] [**source**] [**periodic**]	Forms a server association with another system. • **VRF** *vrf-name*: Specifies the VRF instance for routing to the NTP server.

	Command or Action	Purpose
	Example: `Device(config)# ntp server ipv6 2001:db8::1 version 4 key 10 minpoll 6 maxpoll 10 prefer source GigabitEthernet0/1`	• **ip-address**: IPv4 address of the NTP server. • **IPv6-address**: Accepts full IPv6 addresses for the NTP server. • **IP hostname**: Forces DNS resolution to IPv4 when configuring by hostname. • **IPv6 hostname**: Forces DNS resolution to IPv6 when configuring by hostname. • **Hostname**: A DNS hostname can be used instead of an IP address. • **Version number**: Defines the NTP version number (range 1 to 4). The default value is four. • **Key** *key-id*: Specifies the authentication key ID (1 to 4294967295) used for communication with the NTP server. • **Minpoll**: Minimum polling interval in powers of two seconds (e.g., 4 = 16s, 6 = 64s). The default value is six. (64 seconds). • **Maxpoll**: Maximum polling interval in powers of two seconds (e.g., 10 = 1024s). The default value is ten (1024 seconds). • **Prefer**: Marks this server as the preferred NTP server. • **Source**: Specifies the source interface for NTP packets. • **Periodic**: Valid only with hostname; periodically re-resolves DNS and switches to a new server if the current one becomes unavailable.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Broadcast-Based NTP Associations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp broadcast version** *number*
5. **ntp broadcast client**
6. **ntp broadcastdelay** *microseconds*

7. **end**

DETAILED STEPS

Procedure

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

Configuring NTP Authentication

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* { **md5** | **cmac-aes-128** | **hmac-sha1** | **hmac-sha2-256** | **sha1** | **sha2** } *key*
5. **ntp trusted-key** *key-number* [- *end-key*]
6. **ntp server** *ip-address* **key** *key-id*
7. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ntp authenticate** **Example:** `Device(config)# ntp authenticate`	Enables the NTP Authentication feature.

Step 4	**ntp authentication-key** *number* { **md5**	**cmac-aes-128**	**hmac-sha1**	**hmac-sha2-256**	**sha1**	**sha2** } *key*
						Example:
						`Device(config)# ntp authentication-key 1 md5 key1`
						`Device(config)# ntp authentication-key 1 cmac-aes-128 key1`
							Defines authentication keys.
							• Each key has a key number, a type, and a value.
							• Keys can be one of the following types:
							• `md5`: Authentication using the MD5 algorithm.
							• `cmac-aes-128`: Authentication using Cipher-based message authentication codes (CMAC) with the AES-128 algorithm. The digest length is 128 bits and the key length is 16 or 32 bytes.
							• `hmac-sha1`: Authentication using Hash-based Message Authentication Code (HMAC) using the SHA1 hash function. The digest length is 128 bits and the key length is 1 to 32 bytes.
							• `hmac-sha2-256`: Authentication using HMAC using the SHA2 hash function. The digest length is 256 bits and the key length is 1 to 32 bytes.

	Command or Action	Purpose
		• `sha1`: Authentication using the SHA1 hash function for interoperability with opensource NTP implementations (such as chrony and ntpd). The digest length is 160 bits and the key length is 1 to 32 bytes. • `sha2`: Authentication using the SHA2-256 hash function for interoperability with opensource NTP implementations (such as chrony and ntpd). The digest length is 256 bits and the key length is 1 to 32 bytes. **Note** The keywords `sha1` and `sha2` were introduced in Cisco IOS XE Bengaluru 17.4.
Step 5	**ntp trusted-key** *key-number* [- *end-key*] **Example:** `Device(config)# ntp trusted-key 1 - 3`	Defines trusted authentication keys. • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets.
Step 6	**ntp server** *ip-address* **key** *key-id* **Example:** `Device(config)# ntp server 172.16.22.44 key 2`	Allows the software clock to be synchronized by an NTP time server. **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. `Device(config)# ntp server ip-address [version number] [key key-id] [prefer]`
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an External Reference Clock

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line aux** *line-number*
4. **end**
5. **show ntp associations**
6. **show ntp status**

7. **debug ntp refclock**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line aux** *line-number* **Example:** `Device(config)# line aux 0`	Enters line configuration mode for the auxiliary port 0.
Step 4	**end** **Example:** `Device(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.
Step 5	**show ntp associations** **Example:** `Device# show ntp associations`	Displays the status of NTP associations, including the status of the GPS reference clock.
Step 6	**show ntp status** **Example:** `Device# show ntp status`	Displays the status of NTP.
Step 7	**debug ntp refclock** **Example:** `Device# debug ntp refclock`	Allows advanced monitoring of reference clock activities for the purposes of debugging.

Configuring Orphan Mode

To configure orphan mode, you would require at least two clients. The following task shows how to configure orphan mode on one client. Repeat the steps in the other client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp server** *ip-address*
4. **ntp peer** *ip-address*
5. **ntp orphan** *stratum*
6. Repeat steps 1 to 5 on the other client.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ntp server** *ip-address* **Example:** `Router(config)# ntp server 10.1.1.1`	Forms a server association with another system.
Step 4	**ntp peer** *ip-address* **Example:** `Router(config)# ntp peer 172.16.0.1`	Forms a peer association with another system. **Note** Use an IP address that is different from the one you just configured, such as 172.16.0.2, while configuring the peer in the other client.
Step 5	**ntp orphan** *stratum* **Example:** `Router(config)# ntp orphan 4`	Enables orphan mode in the host.
Step 6	Repeat steps 1 to 5 on the other client.	

Configuring Rate-Limiting Delay

use the following example to configure rate-limiting delay to NTP mode-6 queries:

```
Router(config)#ntp allow mode control ?
  <0-15>  Rate limiting delay (s)
  <cr>    <cr>
```

```
Router(config)#ntp allow mode control 7
Router(config)#
```

Configuring VINES Time Service

Time service is available when Banyan VINES is configured. This protocol is a standard part of VINES. Perform the following task to configure VINES Time Service.



Note Depending on your release, the Banyan VINES and XNS is available in the Cisco software. The **vines time set-system** and **vines time use-system** commands are not available in some releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vines time use-system**
4. **vines time set-system**
5. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vines time use-system** **Example:** `Device(config)# vines time use-system`	Distributes the system software clock time to other VINES systems.
Step 4	**vines time set-system** **Example:** `Device(config)# vines time set-system`	Sets the software clock system time and date as derived from VINES time services.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Time and Date

If no other source of time is available, you can manually configure the current time and date after the system is restarted. The time will remain accurate until the next system restart. We recommend that you use manual configuration only as a last resort.

If you have an outside source to which the device can synchronize, you need not manually set the software clock. Perform the following task to configure the time and date manually.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock timezone** *zone hours-offset* [*minutes-offset*]
4. **clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
5. **clock summer-time** *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*]
6. **exit**
7. **clock set** *hh*:*mm*:*ss date month year*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**clock timezone** *zone hours-offset* [*minutes-offset*] **Example:** `Device(config)# clock timezone PST 2 30`	Configures the time zone used by the Cisco software. **Note** The *minutes-offset* argument of the **clock timezone** command is available for those cases where a local time zone is a percentage of an hour different from UTC/GMT. For example, the time zone for some sections of Atlantic

	Command or Action	Purpose
		Canada (AST) is UTC –3.5. In this case, the necessary command would be **clock timezone AST –3 30**.
Step 4	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]] **Example:** `Device(config)# clock summer-time PST recurring 1 monday january 12:12 4 Tuesday december 12:12 120`	Configures summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year.
Step 5	**clock summer-time** *zone* **date** *date month year hh*:*mm date month year hh*:*mm* [*offset*] **Example:** `Device(config)# clock summer-time PST date 1 january 1999 12:12 4 december 2001 12:12 120`	Configures a specific summer time start and end date. • The *offset* argument is used to indicate the number of minutes to add to the clock during summer time.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**clock set** *hh*:*mm*:*ss date month year* **Example:** `Device# clock set 12:12:12 1 january 2011`	Sets the software clock. • Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone. **Note** Generally, if the system is synchronized by a valid outside timing mechanism, such as an NTP or VINES clock source, or if you have a device with a hardware clock, you need not set the software clock.

Setting the Hardware Clock

Most Cisco devices have a separate hardware-based clock in addition to the software-based clock. The hardware clock is a chip with a rechargeable backup battery that can retain the time and date information across reboots of the device.

To maintain the most accurate time update from an authoritative time source on the network, the software clock should receive time updates from an authoritative time on the network. The hardware clock should in turn be updated at regular intervals from the software clock while the system is running.

The hardware clock (system calendar) maintains time separately from the software clock. The hardware clock continues to run when the system is restarted or when the power is turned off. Typically, the hardware clock needs to be manually set only once, when the system is installed.

You should avoid setting the hardware clock if you have access to a reliable external time source. Time synchronization should instead be established using NTP.

Perform the following task to set the hardware clock.

Before you begin

Note Depending on your release, NTP runs within IOS daemon (IOSd), which updates the time on the Linux kernel. As the Linux kernel updates the hardware clock every 11 minutes, NTP does not interact with the hardware clock directly. So, the calendar-related commands are not required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **clock calendar-valid**
4. **exit**
5. **clock read-calendar**
6. **clock update-calendar**
7. **show calendar**
8. **show clock** [**detail**]
9. **show ntp associations** [**detail**]
10. **show ntp status**
11. **show sntp**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**clock calendar-valid** **Example:** `Device(config)# clock calendar-valid`	Enables the device to act as a valid time source to which network peers can synchronize. • By default, the time maintained on the software clock is not considered to be reliable and will not be synchronized with NTP or VINES time service. To set the hardware clock as a valid time source, use this command.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**clock read-calendar** **Example:** `Device# clock read-calendar`	Sets the software clock to the new hardware clock setting.
Step 6	**clock update-calendar** **Example:** `Device# clock update-calendar`	Updates the hardware clock with a new software clock setting.
Step 7	**show calendar** **Example:** `Device# show calendar`	Displays the current hardware clock time.
Step 8	**show clock** [**detail**] **Example:** `Device# show clock detail`	Displays the current software clock time.
Step 9	**show ntp associations** [**detail**] **Example:** `Device# show ntp associations detail`	Displays the status of NTP associations.
Step 10	**show ntp status** **Example:** `Device# show ntp status`	Displays the status of NTP.
Step 11	**show sntp** **Example:** `Device# show sntp`	Displays information about SNTP.

Configuring Time Ranges

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **time-range** *time-range-name*
4. Enter one of the following:
   - **absolute** [**start** *hh*:*mm date month year*] [**end** *hh*:*mm date month year*]
   - **periodic** *day-of-the-week hh*:*mm* **to** [*day-of-the-week*] *hh*:*mm*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**time-range** *time-range-name* **Example:** `Device(config)# time-range range1`	Assigns a name to the time range to be configured and enters time range configuration mode.

Step 4	Enter one of the following:
	• **absolute** [**start** *hh*:*mm date month year*] [**end** *hh*:*mm date month year*]
	• **periodic** *day-of-the-week hh*:*mm* **to** [*day-of-the-week*] *hh*:*mm*
	Example:
	`Device(config-time-range)# absolute start 12:12 30 January 1999 end 12:12 30 December 2000`
	`Device(config-time-range)# periodic monday 12:12 to friday 12:12`
		Specifies when the time range will be in effect.
		• Use a combination of these commands; multiple **periodic** commands are allowed; only one **absolute** command is allowed.

Step 5	**end** **Example:** `Device(config-time-range)# end`	Exits time range configuration mode and returns to privileged EXEC mode.

Verifying Network Time Protocol

SUMMARY STEPS

1. **show calendar**
2. **show clock** [**detail**]
3. **show ntp associations detail**
4. **show ntp status**
5. **show running-config| i-ntp**

DETAILED STEPS

Procedure

Step 1 **show calendar**

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

Example:

```
Device# show calendar

18:34:29 UTC Tue Jan 4 2011
```

Step 2 **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 3 **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


10.76.239.131 configured, ipv4, authenticated ('*' sys.peer), authtype (cmac-aes-128), our_master,
sane, valid, stratum 2
ref ID 127.127.1.1    , time E15808BD.778D5128 (10:36:45.467 UTC Mon Oct 21 2019)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 2.34, reach 1, sync dist 443.84
delay 2.00 msec, offset 0.0000 msec, dispersion 439.44, jitter 0.97 msec
precision 2**10, version 4
assoc id 63678, assoc name 10.76.239.131
assoc in packets 8, assoc out packets 8, assoc error packets 0
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time E15808C9.80418A98 (10:36:57.501 UTC Mon Oct 21 2019)
xmt time E15808C9.80418A98 (10:36:57.501 UTC Mon Oct 21 2019)
```

```
filtdelay =     3.00    2.00    2.00    2.00    2.00    0.00    0.00    0.00
filtoffset =   -0.50    0.00    0.00    0.00    1.00    0.00    0.00    0.00
filterror =     1.95    1.98    2.01    2.04    2.07 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

Step 4 **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.
```

Step 5 **show running-config| i-ntp**

This command displays the configured rate-limiting delay. The following is sample output from this command, with rate-limiting delay set to 7 seconds:

Example:

```
device# show running-config | i ntp
ntp allow mode control 7

device# show running-config all | i ntp mode
ntp allow mode control 7
```

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Network Time Protocol

Feature Name	Releases	Feature Information
Network Time Protocol	11.2(1) 12.2(28)SB 12.2(33)SRA 12.2(33)SXI 12.2(33)SXJ 12.2(50)SY 12.2(58)SE 15.0(1)M 15.1(2)S 15.1(2)SG Cisco IOS XE Release 3E	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. The following commands were introduced or modified: **ntp access-group**, **ntp allow mode passive**, **ntp authenticate**, **ntp authentication-key**, **ntp broadcast, ntp broadcast client**, **ntp broadcastdelay**, **ntp clear drift**, **ntp clock-period**, **ntp disable**, **ntp logging**, **ntp primary**, **ntp max-associations**, **ntp multicast**, **ntp multicast client**, **ntp server**, **ntp source**, **ntp trusted-key** and **ntp update-calendar**.