



Setting Time and Calendar Services

Last Updated: August 09, 2011

All Cisco routers provide an array of time-of-day services. These services allow the products to accurately keep track of the current time and date, to synchronize multiple devices to the same time, and to provide time services to other systems.

Most Cisco routers have two clocks: a battery-powered hardware clock (referenced in CLI commands as the calendar) and a software clock (referenced in CLI commands as the clock). These two clocks are managed separately.

This module describes how to update the software clock from various sources.

- [Finding Feature Information, page 1](#)
- [Information About Setting Time and Calendar Services, page 2](#)
- [How to Set Time and Calendar Services, page 7](#)
- [Configuration Examples for Setting Time and Calendar Services, page 26](#)
- [Additional References, page 26](#)
- [Feature Information for Setting Time and Calendar Services, page 28](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Information About Setting Time and Calendar Services

- [Time and Calendar Services, page 2](#)
- [Network Time Protocol, page 2](#)
- [Simple Network Time Protocol, page 6](#)
- [VINES Time Service, page 6](#)
- [Hardware Clock, page 7](#)

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 router 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)
- 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 it 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

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 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; in other words, 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 by exchanging 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 (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, page 3](#)
- [Broadcast-Based NTP Associations, page 4](#)
- [NTP Access Group, page 5](#)
- [NTP Services on a Specific Interface, page 5](#)
- [Source IP Address for NTP Packets, page 5](#)
- [System as an Authoritative NTP Server, page 6](#)

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 focusses on the poll-based association modes. Broadcast-based NTP associations are discussed in the [Broadcast-Based NTP Associations, page 4](#) 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-serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode.

When a networking device is operating in the symmetric active mode, it polls its assigned time-serving hosts for the current time and it responds to polls by its hosts. Because this is a peer-to-peer relationship, the host 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 each of your networking devices to depends primarily on the role that you want them to assume as a timekeeping device (server or client) and its 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 exact a toll 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. In order for broadcast client mode to work, the broadcast server and its clients must be located on the same subnet. The time server that is transmitting NTP broadcast packets will also have to be enabled on the interface of the given device 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** {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*} [**kod**] command in global configuration mode.

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

- 1 **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.
- 2 **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.
- 3 **serve-only** --Allows only time requests from a system whose address passes the access list criteria.
- 4 **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 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 it is accepted by the receiving client. NTP synchronization packets that do not contain a matching authenticator key are ignored.

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 instead.

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

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 if you want 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 master** [*stratum*] 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 master** 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 master** command can cause instability in timekeeping if the machines do not agree on the time.

Simple Network Time Protocol

SNTP is a simplified, client-only version of NTP for use on Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, and Cisco 1750 routers. 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 misbehaving servers 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, page 2](#)” section 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 XNS is removed from Cisco IOS software in Cisco IOS Release 12.2(13)T and later releases.

Hardware Clock

Some routers 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 to be an authoritative source of time and be redistributed via NTP or VINES Time Service. If NTP is running, the hardware clock can be updated periodically from NTP, compensating for the inherent drift in the hardware clock.

You can configure a hardware clock (system calendar) on any device to be periodically updated from the software clock. This is advisable 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.

How to Set Time and Calendar Services

- [Configuring NTP, page 7](#)
- [Configuring SNTP, page 15](#)
- [Configuring VINES Time Service, page 16](#)
- [Configuring the Time and Date Manually, page 17](#)
- [Setting the Hardware Clock, page 19](#)
- [Configuring Time Ranges, page 22](#)
- [Verifying Time and Calendar Services, page 24](#)

Configuring NTP

NTP services are disabled on all interfaces by default. Perform the following tasks to configure NTP service on your networking device.

- [Restrictions, page 7](#)
- [Configuring Poll-Based NTP Associations, page 8](#)
- [Configuring Broadcast-Based NTP Associations, page 10](#)
- [Configuring NTP Authentication, page 11](#)
- [Configuring an External Reference Clock, page 13](#)

Restrictions

The NTP package contains a vulnerability that could allow an unauthenticated, remote attacker to cause a DoS condition. NTP versions 4.2.4p7 and earlier are vulnerable.

The vulnerability is due to an error in handling 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 writing messages to log files, and consume the network bandwidth. 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 IOS software releases that supports NTPv4 are not affected. All other versions of Cisco IOS and Cisco IOS XE 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 master**
- **ntp multicast client**
- **ntp peer**
- **ntp server**

For more information on understanding Cisco IOS software releases, see the [White Paper: Cisco IOS Reference Guide](#).

There are no workarounds 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.

Releases later than Cisco IOS Release 12.2(33)SXH7 will not process NTP mode 7 packets, and will display the message “NTP: Receive: dropping message: Received NTP private mode packet .7” 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 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 contains the following tasks:

Configuring Poll-Based NTP Associations

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.

You can specify the time-serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode or in the symmetric active mode.

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

Perform the following task to configure the NTP server-peer relationship.

Note that only one end of an association needs to be configured; the other system will automatically establish the association.



Caution

The **ntp clock-period** command is automatically generated to display the constantly changing correction factor when the **copy running-configuration startup-configuration** command is entered to save the configuration to NVRAM. Do not attempt to manually use the **ntp clock-period** command. Ensure that you remove this command line when copying configuration files to other devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp peer** *ip-address* [**normal-sync**] [**version number**] [**key key-id**] [**source interface-type interface-number**] [**prefer**]
4. **ntp server** *ip-address* [**version number**] [**key key-id**] [**source interface-type interface-number**] [**prefer**]
5. **end**

DETAILED STEPS

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 peer <i>ip-address</i> [normal-sync] [version number] [key key-id] [source interface-type interface-number] [prefer] Example: Router(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer	Forms a peer association with another system.

Command or Action	Purpose
Step 4 <code>ntp server ip-address [version number] [key key-id] [source interface-type interface-number] [prefer]</code> Example: Router(config)# ntp server 192.168.10.1 version 2 prefer	Forms a server association with another system.
Step 5 <code>end</code> Example: Router(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Broadcast-Based NTP Associations

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.

You can set your networking device to listen for NTP broadcast packets propagated through a network. The time server that is transmitting NTP broadcast packets will also have to be enabled on the interface of the given device.

Perform the following task to configure broadcast-based NTP associations.



Caution

The **ntp clock-period** command is automatically generated to reflect the constantly changing correction factor when the **copy running-configuration startup-configuration** command is entered to save the configuration to NVRAM. Do not attempt to manually use the **ntp clock-period** command. Ensure that you remove this command line from the configuration when copying configuration files to other devices.

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

	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	interface <i>type number</i> Example: Router(config)# interface ethernet 0/0	Configures an interface and enters interface configuration mode.
Step 4	ntp broadcast version <i>number</i> Example: Router(config-if)# ntp broadcast version 2	Configures the specified interface to send NTP broadcast packets.
Step 5	ntp broadcast client Example: Router(config-if)# ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
Step 6	ntp broadcastdelay <i>microseconds</i> Example: Router(config-if)# ntp broadcastdelay 100	Adjusts the estimated round-trip delay for NTP broadcasts.
Step 7	end Example: Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NTP Authentication

After NTP authentication is properly configured, your networking device will synchronize with and provide synchronization only to trusted time sources. To configure NTP authentication, perform the following task.

**Note**

In Cisco IOS software earlier than Release 12.0, the cryptotype value is displayed along with the NTP authentication key MD5 value when the **show running-config** command is entered. Copying and pasting the string cryptotype value that is displayed with the authentication key will result in authentication failure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* **md5** *key*
5. **ntp trusted-key** *key-id*
6. **ntp server** *ip-address* **key** *key-id*
7. **end**

DETAILED STEPS

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 authenticate Example: Router(config)# ntp authenticate	Enables the NTP authentication feature.
Step 4 ntp authentication-key <i>number</i> md5 <i>key</i> Example: Router(config)# ntp authentication-key 42 md5 key1	Defines the authentication keys. Each key has a key number, a type, and a value. As of Cisco IOS Release 10.0 the only key type supported is md5.

Command or Action	Purpose
Step 5 <code>ntp trusted-key <i>key-id</i></code> Example: Router(config)# ntp trusted-key 42	Defines trusted authentication keys. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.
Step 6 <code>ntp server <i>ip-address</i> key <i>key-id</i></code> Example: Router(config)# ntp server 172.16.22.44 key 2	Allows the software clock to be synchronized by an NTP time server.
Step 7 <code>end</code> Example: Router(config)# end	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an External Reference Clock

Because Cisco's implementation of NTP does not support stratum 1 service, you cannot connect to a radio or atomic clock (for some specific platforms, however, you can connect to a GPS time source device). However, certain Cisco devices allow you to connect to an external GPS-based time source device for the purposes of distributing a time signal to your network using NTP.

For example, the Trimble Palisade NTP Synchronization Kit can be connected to the auxiliary port of a Cisco 7200 series router. Also, selected platforms support the use of GPS clocks from Symmetricom (formerly Telecom-Solutions). The refclock (reference clock) drivers on these platforms provide the ability to receive an Request to Send (RTS) time-stamp signal on the auxiliary port of your routing device.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `line aux line-number`
4. `ntp refclock {trimble | telecom-solutions} pps {cts | ri | none} [inverted] [pps-offset number] [stratum number] [timestamp-offset number]`
5. `end`
6. `show ntp associations`
7. `show ntp status`
8. `debug ntp refclock`

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3 <code>line aux line-number</code> Example: Router(config)# <code>line aux 0</code>	Enters line configuration mode for the auxiliary port 0.
Step 4 <code>ntp refclock {trimble telecom-solutions} pps {cts ri none} [inverted] [pps-offset number] [stratum number] [timestamp-offset number]</code> Example: Router(config-line)# <code>ntp refclock trimble pps none stratum 1</code>	Configures an external reference clock. - To configure a Trimble Palisade GPS product connected to the auxiliary port of a Cisco 7200 series router as the NTP reference clock, use the ntp refclock trimble pps none stratum number form of the command. Use this command to enable the driver that allows the Trimble Palisade NTP Synchronization Kit to be used as the NTP reference clock source (Cisco 7200 series routers only). - To configure a Symmetricom GPS product connected to the auxiliary port of a supported router or switch as the NTP reference clock, use the ntp refclock telecom-solutions pps cts stratum number form of the command. Use this command to enable the driver that allows the Symmetricom GPS product to be used as the NTP reference clock source. - To configure a pulse per second (PPS) signal as the source for NTP synchronization, use the ntp refclock telecom-solutions pps cts stratum number form of the command. - To configure a PPS signal as the source for NTP synchronization, use the ntp refclock {trimble telecom-solutions} pps {cts ri} [inverted] [pps-offset number] [stratum number] [timestamp-offset number].
Step 5 <code>end</code> Example: Router(config-line)# <code>end</code>	Exits line configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show ntp associations Example: Router# show ntp associations	Displays the status of NTP associations, including the status of the GPS reference clock.
Step 7	show ntp status Example: Router# show ntp status	Displays the status of NTP.
Step 8	debug ntp refclock Example: Router# debug ntp refclock	Allows advanced monitoring of reference clock activities for the purposes of debugging.

Configuring SNTP

SNTP generally is supported on those platforms that do not provide support for NTP, such as the Cisco 1000 series, 1600 series, and 1700 series platforms. SNTP is disabled by default. To configure SNTP, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sntp server** {address | hostname}[versionnumber]
4. **sntp broadcast client**
5. **exit**
6. **show sntp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

Command or Action	Purpose
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 sntp server {address hostname} [versionnumber] Example: Router(config)# sntp server 192.168.2.1 version 2	Configures SNTP to request NTP packets from an NTP server. Enter the sntp server command once for each NTP server. The NTP servers must be configured to respond to the SNTP messages from the router.
Step 4 sntp broadcast client Example: Router(config)# sntp broadcast client	Configures SNTP to accept NTP packets from any NTP broadcast server. Note If you enter both the sntp server command and the sntp broadcast client command, the router will accept time from a broadcast server but will prefer time from a configured server, assuming that the strata are equal.
Step 5 exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 6 show sntp Example: Router# show sntp	Displays information about SNTP.

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

Support for Banyan VINES and XNS was removed from Cisco IOS software beginning in Cisco IOS Release 12.2(13)T. The following VINES commands are not available in releases derived from 12.2(13)T, such as the 12.3 mainline release.

SUMMARY STEPS

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

DETAILED STEPS

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 vines time use-system Example: Router(config)# vines time use-system	Distributes the system software clock time to other VINES systems.
Step 4 vines time set-system Example: Router(config)# vines time set-system	Sets the software clock system time and date as derived from VINES time services.
Step 5 exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Time and Date Manually

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 router 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

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 clock timezone <i>zone hours-offset [minutes-offset]</i> Example: Router(config)# clock timezone PST 2 30	Configures the time zone used by the Cisco IOS software. The <i>zone</i> argument is the name of the time zone (typically a standard acronym). The <i>hours-offset</i> argument is the number of hours the time zone is different from UTC. The <i>minutes-offset</i> argument is the number of minutes the time zone is different from UTC. Note The <i>minutes-offset</i> 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 Canada (AST) is UTC -3.5. In this case, the necessary command would be clock timezone AST -3 30.

Command or Action	Purpose
Step 4 clock summer-time zone recurring <i>[week day month hh : mm week day month hh : mm [offset]]</i> Example: <pre>Router(config)# clock summer-time PST recurring 1 monday january 12:12 4 Tuesday december 12:12 120</pre>	Configures summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year . The <i>offset</i> argument is used to indicate the number of minutes to add to the clock during summer time.
Step 5 clock summer-time zone date <i>date month year hh:mm date month year hh : mm [offset]</i> Example: <pre>Router(config)# clock summer-time PST date 1 january 1999 12:12 4 december 2001 12:12 120</pre>	Configures a specific summer time start and end date. The <i>offset</i> argument is used to indicate the number of minutes to add to the clock during summer time.
Step 6 exit Example: <pre>Router(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 7 clock set <i>hh : mm : ss date month year</i> Example: <pre>Router# clock set 12:12:12 1 january 2011</pre>	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 router 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 manually 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.

SUMMARY STEPS

1. **enable**
2. **calendar set** *hh : mm : ss day month year*
3. **configure terminal**
4. **clock calendar-valid**
5. **exit**
6. **clock read-calendar**
7. **clock update-calendar**
8. **show calendar**
9. **show clock** [detail]
10. **show ntp associations** [detail]
11. **show ntp status**
12. **show sntp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	calendar set <i>hh : mm : ss day month year</i> Example: Router# calendar set 10:12:15 monday june 1999	Sets the hardware clock manually. Note Use this command when you have no access to an external time source.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	clock calendar-valid Example: Router(config)# clock calendar-valid	Enables the router 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 5	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	clock read-calendar Example: Router# clock read-calendar	Sets the software clock to the new hardware clock setting.
Step 7	clock update-calendar Example: Router# clock update-calendar	Updates the hardware clock with a new software clock setting.
Step 8	show calendar Example: Router# show calendar	Displays the current hardware clock time.
Step 9	show clock [detail] Example: Router# show clock detail	Displays the current software clock time .
Step 10	show ntp associations [detail] Example: Router# show ntp associations detail	Displays the status of NTP associations.
Step 11	show ntp status Example: Router# show ntp status	Displays the status of NTP.

Command or Action	Purpose
Step 12 <code>show sntp</code> Example: Router# <code>show sntp</code>	Displays information about SNTP (Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 routers only).

Configuring Time Ranges

Cisco IOS 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 then can be referenced by a function, so that those time restrictions are imposed on the function itself.

In Cisco IOS Release 12.2, IP and 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. Cisco recommends 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 IOS 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 simply deny access without the need to analyze the many logs generated during peak hours.

SUMMARY STEPS

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

DETAILED STEPS

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 time-range <i>time-range-name</i> Example: Router(config)# time-range range1	Assigns a name to the time range to be configured and enters time range configuration mode.

Command or Action	Purpose
Step 4 Do one of the following: absolute [start <i>time date month year</i>] [end <i>time date month year</i>] . . periodic <i>day-of-the-week hh : mm to [day-of-the-week] hh : mm</i> Example: <pre>Router(config-time-range)# absolute start 12:12 30 January 1999 end 12:12 30 December 2000</pre> Example: or Example: <pre>Router(config-time-range)# periodic monday 12:12 to friday 12:12</pre>	Specifies when the time range will be in effect. Use some combination of these commands; multiple periodic commands are allowed; only one absolute command is allowed.
Step 5 end Example: <pre>Router(config-time-range)# end</pre>	Exits time range configuration mode and returns to privileged EXEC mode.

Verifying Time and Calendar Services

To monitor clock, calendar, and NTP EXEC services, use the following commands in privileged EXEC mode, as needed:

SUMMARY STEPS

1. **show calendar**
2. **show clock [detail]**
3. **show ntp associations detail**
4. **show ntp status**
5. **show sntp**

DETAILED STEPS

Step 1 **show calendar**

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

Example:

```
Router# 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:

```
Router# 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:

```
Router# 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
filtererror = 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
filtererror = 16000.0 16000.0 16000.0 16000.0 16000.0 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:

```
Router# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.19 msec, peer dispersion is 0.00 msec
```

```
loopfilter state is 'FSET' (Drift set from file), drift is 0.000000000 s/s
system poll interval is 64, never updated.
```

Step 5**show sntp**

This command displays information about SNTp (Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 routers only). The following is sample output from this command:

Example:

```
Router# show sntp
Sntp server      Stratum   Version   Last Receive
172.168.10.1     16          1         never
Broadcast client mode is enabled.
Multicast client 224.0.1.1 is enabled.
```

Configuration Examples for Setting Time and Calendar Services

- [Example Configuring Clock Calendar and NTP, page 26](#)

Example Configuring Clock Calendar and NTP

In the following example, a router 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 update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58
interface Ethernet 0/0
 ntp broadcast
vines time use-system
```

In the following example, a router 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 fddi 0/0
 ntp broadcast
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Network Management commands	<i>Cisco IOS Network Management Command Reference</i>
IP extended access lists	"Configuring IPv4 Addresses" chapter of the <i>Cisco IOS IP Addressing Configuration Guide</i>
IPX extended access lists	"Configuring Novell IPX" chapter of the <i>Cisco IOS Novell IPX Configuration Guide</i>
NTP package vulnerability	Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability
Cisco IOS software releases	White Paper: Cisco IOS Reference Guide

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1305	<i>Network Time Protocol (Version 3) Specification, Impl</i>

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 Setting Time and Calendar Services

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 Setting Time and Calendar Services*

Feature Name	Releases	Feature Information
Network Time Protocol	11.2(1)	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.
	12.2(28)SB	
	12.2(33)SRA	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 master , ntp max-associations , ntp multicast , ntp multicast client , ntp server , ntp source , ntp trusted-key , ntp update-calendar .
	12.2(33)SXI	
	12.2(33)SXJ	
	12.2(50)SY	
	12.2(58)SE	
	15.0(1)M	
	15.1(2)S	

Feature Name	Releases	Feature Information
Simple Network Time Protocol	12.0(2)T 12.2(4)T	SNTP is a simplified, client-only version of NTP for use on Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, and Cisco 1750 routers. SNTP can receive only time from NTP servers; it cannot be used to provide time services to other systems. The following commands were introduced or modified: sntp broadcast client, sntp server.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.