CONTENTS

CHAPTER 1

Network Time Protocol 1
Finding Feature Information 1
Restrictions for Network Time Protocol 1
Information About Network Time Protocol 2
Network Time Protocol 2
Poll-Based NTP Associations 3
Broadcast-Based NTP Associations 4
NTP Access Group 4
NTP Services on a Specific Interface 5
Source IP Address for NTP Packets 6
System as an Authoritative NTP Server 6
How to Configure Network Time Protocol 6
Configuring NTP 6
Configuring Poll-Based NTP Associations 6
Configuring Broadcast-Based NTP Associations 7
Configuring an External Reference Clock 9
Configuring NTP Authentication 10
Verifying Network Time Protocol 12
Configuration Examples for Network Time Protocol 13
Example: Configuring Network Time Protocol 13
Additional References for Network Time Protocol 13
Feature Information for Network Time Protocol 14

CHAPTER 2

NTPv4 MIB 17
Finding Feature Information 17
Information About the NTPv4 MIB 17
NTPv4 MIB 17
How to Verify the NTPv4 MIB 18
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.

- Finding Feature Information, page 1
- Restrictions for Network Time Protocol, page 1
- Information About Network Time Protocol, page 2
- How to Configure Network Time Protocol, page 6
- Configuration Examples for Network Time Protocol, page 13
- Additional References for Network Time Protocol, page 13
- Feature Information for Network Time Protocol, page 14

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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.

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 master`
- `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.

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

Note

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.

**Information About Network Time Protocol**

**Network Time Protocol**

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

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

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

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

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

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

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

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

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

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

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

NTP services are disabled on all interfaces by default.

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.

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 master` 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.

How to Configure Network Time Protocol

Configuring NTP

Configuring Poll-Based NTP Associations

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ntp peer ip-address [normal-sync] [version number] [key key-id] [prefer]</td>
<td>Forms a peer association with another system.</td>
</tr>
<tr>
<td>Example: Device(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ntp server ip-address [version number] [key key-id] [prefer]</td>
<td>Forms a server association with another system.</td>
</tr>
<tr>
<td>Example: Device(config)# ntp server 192.168.10.1 version 2 prefer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
**Purpose**

- Enter your password if prompted.

### Step 2

**Command or Action:**

```
Device> enable
```

**Purpose:**

Enters global configuration mode.

### Step 3

**Command or Action:**

```
Device# configure terminal
```

**Purpose:**

Configures an interface and enters interface configuration mode.

### Step 4

**Command or Action:**

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

**Purpose:**

Configures the specified interface to send NTP broadcast packets.

### Step 5

**Command or Action:**

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

**Purpose:**

Configures the specified interface to receive NTP broadcast packets.

### Step 6

**Command or Action:**

```
Device(config-if)# ntp broadcastclient
```

**Purpose:**

Adjusts the estimated round-trip delay for NTP broadcasts.

### Step 7

**Command or Action:**

```
Device(config-if)# end
```

**Purpose:**

Exits interface 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

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

## Configuring NTP Authentication

### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td><code>ntp authenticate</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp authenticate</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ntp authentication-key number md5 key</code></td>
<td>Defines authentication keys.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp authentication-key 1 md5 key1</code></td>
<td>- Each key has a key number, a type, and a value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ntp authentication-key number md5 key</code></td>
<td>Defines authentication keys.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp authentication-key 2 md5 key2</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ntp authentication-key number md5 key</code></td>
<td>Defines authentication keys.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp authentication-key 3 md5 key3</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ntp trusted-key key-number [- end-key]</code></td>
<td>Defines trusted authentication keys.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp trusted-key 1 - 3</code></td>
<td>- If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ntp server ip-address key key-id</code></td>
<td>Allows the software clock to be synchronized by an NTP time server.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# ntp server 172.16.22.44 key 2</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Verifying Network Time Protocol

SUMMARY STEPS
1. show clock [detail]
2. show ntp associations detail
3. show ntp status

DETAILED STEPS

Step 1  show clock [detail]
This command displays the current software clock time. The following is sample output from this command.

Example:

Device# show clock detail
*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar

Step 2  show ntp associations detail
This command displays the status of NTP associations. The following is sample output from this command.

Example:

Device# show ntp associations detail
192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
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
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)
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
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 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4

Step 3  show ntp status
This command displays the status of NTP. The following is sample output from this command.
Example:

Device# show ntp status

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

Configuration Examples for Network Time Protocol

Example: Configuring Network Time Protocol

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

clock timezone PST -8
  clock summer-time PDT recurring
  ntp server 192.168.13.57
  ntp server 192.168.11.58
  interface GigabitEthernet 0/0
  ntp broadcast
  vines time use-system

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

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

Additional References for Network Time Protocol

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Basic System Management commands</td>
<td>Basic System Management Command Reference</td>
</tr>
<tr>
<td>NTP4 in IPv6</td>
<td>Cisco IOS Basic System Management Guide</td>
</tr>
</tbody>
</table>
## 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 . An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Standards and RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard/RFCs</strong></td>
</tr>
<tr>
<td>RFC 1305</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical Assistance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
Table 1: Feature Information for Network Time Protocol

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Time Protocol</td>
<td>15.1(2)SG</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.2SE</td>
<td>In Cisco IOS XE Release 3.5 SG, support was added for the Cisco Catalyst 4000 Series Switches.</td>
</tr>
</tbody>
</table>
NTPv4 MIB

The NTPv4 MIB feature introduces the Network Time Protocol Version 4 (NTPv4) MIB in Cisco software. It defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities. This module describes the NTPv4 MIB.

- Finding Feature Information, page 17
- Information About the NTPv4 MIB, page 17
- How to Verify the NTPv4 MIB, page 18
- Configuration Examples for NTPv4 MIB, page 19
- Additional References, page 20
- Feature Information for the NTPv4 MIB, page 21

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 the NTPv4 MIB

NTPv4 MIB

The Network Time Protocol Version 4 (NTPv4) MIB feature, which is based on RFC 5907, defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities.
The data objects contain the following information about the NTP entities:

- Connectivity to the upstream NTP servers and to hardware reference clocks.
- Product
- Vendor
- Version

By using the information contained in the data objects, you can detect failures before the overall time synchronization of the network is impacted.

The following object groups that are addressed in RFC 5907 are supported in the NTPv4 MIB:

- ntpAssociation
- ntpEntInfo
- ntpEntStatus

The following object groups that are addressed in RFC 5907 are not supported in the NTPv4 MIB:

- ntpEntControl
- ntpEntNotifObjects

**How to Verify the NTPv4 MIB**

No special configuration is needed for this feature. This feature is enabled by default.

**Verifying NTPv4 MIB**

To verify information about the NTPv4 MIB, perform any or all of the following optional commands in any order.

**SUMMARY STEPS**

1. show ntp associations [detail]
2. show ntp status
3. show ntp info
4. show ntp packets

**DETAILED STEPS**

Step 1  show ntp associations [detail]

**Example:**
Device> show ntp associations detail

(Optional) Displays detailed status of NTP associations.
Step 2  show ntp status

Example:
Device> show ntp status
(Optional) Displays the status of NTP.

Step 3  show ntp info

Example:
Device> show ntp info
(Optional) Displays information about NTP entities.

Step 4  show ntp packets

Example:
Device> show ntp packets
(Optional) Displays information about NTP packets.

Configuration Examples for NTPv4 MIB

Example: Verifying the NTP4 MIB

Sample Output for the show ntp associations Command
Device> show ntp associations detail
172.31.32.2 configured, ipv4, our_master, sane, valid, stratum 1
ref ID .LOCAL., time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
our mode active, peer mode passive, our poll intvl 16, peer poll intvl 16
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 16.05
delay 0.00 msec, offset 0.0000 msec, dispersion 8.01, jitter 0.5 msec
precision 2**7, version 4
assoc ID 1, assoc name 192.0.2.1,
assoc in packets 60, assoc out packets 60, assoc error packets 0
org time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time D2352248.2337CCB8 (06:12:24.137 IST Tue Oct 4 2011)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtoffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 7.81 8.05 8.29 8.53 8.77 9.01 9.25 9.49
minpoll = 4, maxpoll = 4
192.168.13.33 configured, ipv6, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 1024, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15951.96
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50, jitter 1000.45 msec
precision 2**7, version 4
assoc ID 2, assoc name myserver
assoc in packets 0, assoc out packets 0, assoc error packets 0
org time D2351E93.2235F124 (05:56:35.133 IST Tue Oct 4 2011)
rec time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 IST Mon Jan 1 1900)
Sample Output for the show ntp status Command

```
Device> show ntp status

Clock is synchronized, stratum 2, reference assoc id 1, reference is 192.0.2.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**7
reference time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec, time resolution 1000 (1 msec),
root dispersion is 15.91 msec, peer dispersion is 8.01 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 6 sec ago.
system uptime (00:00:00.000) UTC,
system time is D2352258.243DDF14 (06:12:40.141 IST Tue Oct 4 2011)
leap time is D2352258.243DDF14 (24:00:00.000 IST Tue Dec 31 2011)
leap direction is 1
```

Sample Output for the show ntp info Command

```
Device> show ntp info

Ntp Software Name: Example
Ntp Software Version: ntp-1.1
Ntp Software Vendor: Example
Ntp System Type: Example_System
```

Sample Output for the show ntp packets Command

```
Device> show ntp packets

Ntp In packets: 100
Ntp Out packets: 110
Ntp bad version packets: 4
Ntp protocol error packets: 0
```

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Master Command List, All Releases</td>
</tr>
<tr>
<td>Basic System Management commands</td>
<td>Basic System Management Command Reference</td>
</tr>
<tr>
<td>Basic System Management configuration tasks</td>
<td>&quot;Setting Time and Calendar Services&quot; module in the Basic System Management Configuration Guide</td>
</tr>
</tbody>
</table>
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 5907</td>
<td><em>Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)</em></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTPv4-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for the NTPv4 MIB

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 . An account on Cisco.com is not required.
### Table 2: Feature Information for the NTPv4 MIB

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTPv4 MIB</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The NTPv4 MIB feature introduces the Network Time Protocol Version 4 (NTPv4) MIB in Cisco software. It defines data objects that represent the current status of NTP entities. These data objects are accessed using the Simple Network Management Protocol (SNMP) and are used to monitor and manage local NTP entities.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.6E</td>
<td></td>
</tr>
</tbody>
</table>

In Cisco IOS XE Release 3.4 SG, support was added for the Cisco Catalyst 4000 Series Switches.

In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.