Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP). This module describes how to configure Simple Network Time Protocol on Cisco devices.

- Finding Feature Information, page 1
- Restrictions for Simple Network Time Protocol, page 1
- Information About Simple Network Time Protocol, page 2
- How to Configure Simple Network Time Protocol, page 2
- Configuration Examples for Simple Network Time Protocol, page 4
- Additional References for Simple Network Time Protocol, page 4
- Feature Information for the SNTP, page 5

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 Simple Network Time Protocol

- Simple Network Time Protocol (SNTP) and Network Time Protocol (NTP) cannot coexist on the same machine as they use the same port. This means that these two services cannot be configured on the system at the same time.
- Support for IPv6 addresses is available only if the image supports IPv6 addressing.
Information About Simple Network Time Protocol

Simple Network Time Protocol

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

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

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

How to Configure Simple Network Time Protocol

Configuring Simple Network Time Protocol (SNTP) Authentication

Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (SNTP). This module describes how to configure SNTP on Cisco devices.

 Procedure

<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>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</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> sntp authenticate</td>
<td>Enables the SNTP Authentication feature.</td>
</tr>
<tr>
<td>Example: Device(config)# sntp authenticate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sntp authentication-key number md5 key</td>
<td>Defines authentication keys.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Example:** Device(config)# sntp authentication-key 1 md5 key1 | • Each key has a key number, a type, and a value.  
• Repeat this step to define additional authentication keys. |

### Step 5

**sntp trusted-key key-number [-end-key]**

- Defines trusted authentication keys.
- • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its SNTP packets.

**Example:** 
Device(config)# sntp trusted-key 1 - 3

### Step 6

**sntp server ip-address key key-id**

- Allows the software clock to be synchronized by an SNTP time server.

**Example:** 
Device(config)# sntp server 172.16.22.44 key 2

### Step 7

**end**

- Exits global configuration mode and returns to privileged EXEC mode.

**Example:** 
Device(config)# end

---

**Verifying and Troubleshooting Simple Network Time Protocol**

To verify and troubleshoot Simple Network Time Protocol configuration, use the following commands.

- •

**Procedure**

**Step 1** **enable**

**Example:**
Device> enable
Enables privileged EXEC mode.

  - Enter your password if prompted.

**Step 2** **debug sntp packets [detail]**

**Example:**
Device> debug sntp packets
Displays the NTP packet sent and received along with the SNTP packet fields.

**Step 3** **debug sntp select**
Example:
Device> debug sntp select
Displays the SNTP server selection for IPv4 and IPv6 servers.

Step 4 show sntp

Example:
Device# 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.
Displays information about SNTP available in Cisco devices.

Configuration Examples for Simple Network Time Protocol

Example: Configuring Simple Network Time Protocol

    clock timezone PST -8
    clock summer-time PDT recurring
    sntp update-calendar
    sntp server 192.168.13.57
    sntp server 192.168.11.58
    interface Ethernet 0/0
    sntp broadcast

Additional References for Simple 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>
<tr>
<td>IP extended access lists</td>
<td>Cisco IOS IP Addressing Configuration Guide</td>
</tr>
<tr>
<td>IPX extended access lists</td>
<td>Novell IPX Configuration Guide</td>
</tr>
<tr>
<td>NTP package vulnerability</td>
<td>Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability</td>
</tr>
</tbody>
</table>
Feature Information for the SNTP

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 the SNTPv4

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple Network Time Protocol</td>
<td></td>
<td>Simple Network Time Protocol (SNTP) is a simplified version of Network Time Protocol (NTP). This module describes how to configure Simple Network Time Protocol on Cisco devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced or modified: <code>sntp server</code>, <code>sntp authenticate</code>, <code>sntp authentication-key</code>, <code>sntp multicast</code>, <code>sntp trusted-key</code>.</td>
</tr>
</tbody>
</table>