

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.

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

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.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sntp authenticate** **Example:** `Device(config)# sntp authenticate`	Enables the SNTP Authentication feature.
Step 4	**sntp authentication-key** *number* { **md5** | **cmac-aes-128** | **hmac-sha1** | **hmac-sha2-256** } *key* **Example:** `Device(config)# sntp authentication-key 1 cmac-aes-128 key1`	Defines authentication keys. • Each key has a key number, a type, and a value. • Keys can be of the following types: • `md5`: Authentication using the MD5 algorithm.

	Command or Action	Purpose
		• `cmac-aes-128`: Authentication using Cipher-based message authentication codes (CMAC) with the AES-128 algorithm. The digest length is 128 bits and the key length is 16 or 32 bytes. `hmac-sha1`: Authentication using Hash-based Message Authentication Code (HMAC) using the SHA1 hash function. The digest length is 128 bits and the key length is 1 to 32 bytes. `hmac-sha2-256`: Authentication using HMAC using the SHA2 hash function. The digest length is 256 bits and the key length is 1 to 32 bytes. • Repeat this step to define additional authentication keys.
Step 5	**sntp trusted-key** *key-number* [**-** *end-key*] **Example:** `Device(config)# sntp trusted-key 1 - 3`	Defines trusted authentication keys. • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its SNTP packets.
Step 6	**sntp server** *ip-address* **key** *key-id* **Example:** `Device(config)# sntp server 172.16.22.44 key 2`	Allows the software clock to be synchronized by an SNTP time server.
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting Simple Network Time Protocol

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

•

SUMMARY STEPS

1. **enable**
2. **debug sntp packets** [**detail**]
3. **debug sntp select**
4. **show sntp**

DETAILED STEPS

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

Related Documents

Related Topic	Document Title
Basic System Management commands	Basic System Management Command Reference
NTP4 in IPv6	*Cisco IOS Basic System Management Guide*
IP extended access lists	*Cisco IOS IP Addressing Configuration Guide*
IPX extended access lists	*Novell IPX Configuration Guide*
NTP package vulnerability	*Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability*
Cisco IOS and NX-OS software releases	*White Paper: Cisco IOS and NX-OS Software Reference Guide*

Standards and RFCs

Standard/RFCs	Title
RFC 1305	*Network Time Protocol (Version 3) Specification, Implementation and Analysis*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for 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

Feature Name	Releases	Feature Information
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. The following commands were introduced or modified: **sntp server**, **sntp authenticate**, **sntp authentication-key**, **sntp multicast**, **sntp trusted-key**.