



Implementing NTPv4 in IPv6

First Published: June 12, 2009

Last Updated: March 21, 2011

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IPv4. NTP Version 4 (NTPv4) is an extension of NTP version 3, which supports both IPv4 and IPv6.

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 for Implementing NTPv4 in IPv6”](#) section on page 18.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About Implementing NTPv4 in IPv6, page 1](#)
- [How to Implement NTPv4 in IPv6, page 3](#)
- [Configuration Examples for NTPv4 in IPv6, page 15](#)
- [Additional References, page 16](#)
- [Feature Information for Implementing NTPv4 in IPv6, page 18](#)

Information About Implementing NTPv4 in IPv6

- [NTP Version 4, page 2](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [NTPv4 Overview, page 2](#)

NTP Version 4

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IPv4. NTP Version 4 (NTPv4) is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides the following capabilities:

- NTPv4 supports IPv6, making NTP time synchronization possible over IPv6.
- Security is improved over NTPv3. The NTPv4 protocol provides a whole security framework based on public key cryptography and standard X509 certificates.
- Using specific multicast groups, NTPv4 can automatically calculate its time-distribution hierarchy through an entire network. NTPv4 automatically configures the hierarchy of the servers in order to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

NTPv4 Overview

NTPv4 works in much the same way as does NTP. 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 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 avoids synchronizing to a machine whose time may not be accurate in two ways. First, NTP never synchronizes to a machine that is not in turn synchronized itself. Second, NTP compares the time reported by several machines, and will not synchronize to a machine whose time is significantly different than the 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, it is not possible to connect to a radio or atomic clock (for some specific platforms, however, you can connect a GPS time-source device).

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 and its various derivatives is also available. 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 IPv4 or IPv6 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.

NTPv4 Features

NTPv4 includes the following features:

- [IPv6 Multicast Mode, page 3](#)
- [NTP Access Groups versus Symmetric Key Authentication, page 3](#)
- [DNS Support for IPv6 in NTPv4, page 3](#)

IPv6 Multicast Mode

NTPv3 supports sending and receiving clock updates using IPv4 broadcast messages. Many network administrators use this feature to distribute time on LANs with minimum client configuration. For example, Cisco corporate LANs use this feature over IPv4 on local gateways. End-user workstations are configured to listen to NTP broadcast messages and synchronize their clocks accordingly.

In NTPv4 for IPv6, IPv6 multicast messages instead of IPv4 broadcast messages are used to send and receive clock updates.

NTP Access Groups versus Symmetric Key Authentication

NTPv3 access group functionality is based on IPv4 numbered access lists. NTPv4 access group functionality accepts IPv6 named access lists as well as IPv4 numbered access lists.

NTP access groups are very useful for assigning NTP permission groups to Cisco IOS access lists. For example, all hosts in a subnet can be allowed to synchronize their clocks from a router but not to provide clock updates to the router. NTP access groups are built on the Cisco IOS access-list infrastructure and deliver fully flexible access-list-based matching functionality.

Although more flexible than NTP symmetric key authentication and easier to deploy, access groups do not provide the same level of security. NTP symmetric key authentication provides a cryptographically strong authentication mechanism, but requires the manual distribution of keys on the NTP devices across the network.

NTP symmetric key authentication is also less flexible than access groups regarding the type of permission that can be associated with different peers. NTP symmetric key authentication is mainly intended for protecting the local router from being updated with wrong clock information from an intruder.

DNS Support for IPv6 in NTPv4

NTPv4 adds DNS support for IPv6. NTPv3 resolves hostnames into IPv4 addresses at configuration (when the command is parsed). Then, only the resolved IPv4 address is kept in memory and stored in NVRAM during NVGEN. The hostname given by the user is lost.

NTPv4 keeps the hostname in memory, so that it can be saved during NVGEN. Configurations saved with hostnames are still readable by NTPv3.

How to Implement NTPv4 in IPv6

NTP services are disabled on all interfaces by default. The following sections contain optional tasks that you can perform on your networking device:

- [Configuring Poll-Based NTPv4 Associations, page 4](#)
- [Configuring Multicast-Based NTPv4 Associations, page 6](#)
- [Defining an NTPv4 Access Group, page 8](#)
- [Configuring NTPv4 Authentication, page 9](#)
- [Disabling NTPv4 Services on a Specific Interface, page 10](#)
- [Configuring the Source IPv6 Address for NTPv4 Packets, page 11](#)
- [Configuring the System as an Authoritative NTP Server, page 12](#)
- [Updating the Hardware Clock, page 13](#)

Configuring Poll-Based NTPv4 Associations

Networking devices running NTPv4 can be configured to operate in variety of association modes when synchronizing time with reference time sources. There are two ways that a networking device can obtain time information on a network: by polling host servers and by listening to NTPv4 broadcasts.

The following are two most commonly used poll-based association modes:

- Client mode
- Symmetric active mode

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 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 about the local networking device that it is communicating with. This mode should be used when there are several mutually redundant servers that are interconnected using diverse network paths. Most Stratum 1 and stratum 2 servers on the Internet today adopt this form of network setup. Use the **ntp peer** command to specify individually 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 it to assume as a timekeeping device (server or client) and its proximity to a stratum 1 timekeeping server.

Configuring Symmetric Active Mode

SUMMARY STEPS

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

3. **ntp peer** { *vrf vrf-name* | *ip-address* | *ipv6 address* | **ipv4** | **ipv6** | *hostname* } [**normal-sync**][**version number**] [**key key-id**] [**source interface**] [**prefer**] [**maxpoll number**] [**minpoll number**] [**burst**] [**iburst**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ntp peer { <i>vrf vrf-name</i> <i>ip-address</i> <i>ipv6 address</i> ipv4 ipv6 <i>hostname</i> } [normal-sync] [version number] [key key-id] [source interface] [prefer] [maxpoll number] [minpoll number] [burst] [iburst] Example: Router(config)# ntp peer 2001:DB8:0:0:8:800:200C:417A version 4	Configures the software clock to synchronize a peer or to be synchronized by a peer.

Configuring Client Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp server** { *vrf vrf-name* | *ip-address* | *ipv6 address* | **ipv4** | **ipv6** | *hostname* } [**normal-sync**] [**version number**] [**key key-id**] [**source interface**] [**prefer**] [**maxpoll number**] [**minpoll number**] [**burst**] [**iburst**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ntp server {vrf vrf-name ip-address ipv6-address ipv4 ipv6 hostname}[normal-sync][version number] [key key-id] [source interface] [prefer] [maxpoll number] [minpoll number] [burst] [iburst] Example: Router(config)# ntp server 2001:DB8:0:0:8:800:200C:417A version 4	Allows the software clock to be synchronized by an NTP time server.

Configuring Multicast-Based NTPv4 Associations

- [Configuring an Interface to Send NTPv4 Multicast Packets, page 6](#)
- [Configuring an Interface to Receive NTPv4 Multicast Packets, page 7](#)

Configuring an Interface to Send NTPv4 Multicast Packets

SUMMARY STEPS

- enable
- configure terminal
- interface *type number*
- ntp multicast {ip-address | ipv6-address} [key key-id] [ttl value] [version number]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• 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 fastethernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	ntp multicast { <i>ip-address</i> <i>ipv6-address</i> } [key <i>key-id</i>] [t <i>t</i> l <i>value</i>] [v <i>e</i> r s i o n <i>number</i>] Example: Router(config-if)# ntp multicast FF02::1:FF0E:8C6C	Configures a system to send NTPv4 multicast packets on a specified interface.

Configuring an Interface to Receive NTPv4 Multicast Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp multicast client** {*ip-address* | *ipv6-address*} [**novolley**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• 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 FastEthernet 0/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	ntp multicast client { <i>ip-address</i> <i>ipv6-address</i> } [novolley] Example: Router(config-if)# ntp multicast client FF02::2:FF0E:8C6C	Configures the system to receive NTP multicast packets on a specified interface.

Defining an NTPv4 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} {*access-list-number* | *access-list-name*} [**kod**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ntp access-group {query-only serve-only serve peer} {access-list-number access-list-name} [kod] Example: Router(config)# ntp access-group serve acl1 kod	Controls access to the NTPv4 services on the system.

Configuring NTPv4 Authentication

The encrypted NTPv4 authentication scheme should be used when a reliable form of access control is required. Unlike the access list-based restriction scheme, the encrypted authentication scheme uses authentication keys and an authentication process to determine if NTPv4 synchronization packets sent by designated peers or servers on a local network are deemed as trusted before the time information that it carries along with it, is accepted.

After NTPv4 authentication is properly configured, your networking device will only synchronize with and provide synchronization to trusted time sources.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key number md5 value**
5. **ntp trusted-key key-number**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• 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 NTPv4 authentication.
Step 4	ntp authentication-key <i>number</i> md5 <i>value</i> Example: Router(config)# ntp authentication-key 42 md5 keyname	Defines an authentication key for NTPv4.
Step 5	ntp trusted-key <i>key-number</i> Example: Router(config)# ntp trusted-key 42	Authenticates the identity of a system to which NTPv4 will synchronize.

Disabling NTPv4 Services on a Specific Interface

NTP and NTPv4 services are disabled on all interfaces by default. NTP or NTPv4 is enabled globally when any NTP commands are entered.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp disable [ipv4 | ipv6]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ntp disable [ipv4 ipv6]</code> Example: Router(config)# ntp disable ipv6	Controls access to the NTPv4 services on the system.

Configuring the Source IPv6 Address for NTPv4 Packets

When the system sends an NTPv4 packet, the source IPv6 address is normally set to the address of the interface through which the NTPv4 packet is sent.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ntp source type number`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ntp source type number</code> Example: Router(config)# ntp source FastEthernet 0/0	Configures the use of a particular source address in NTPv4 packets. The specified interface is configured with IPv6 addresses.

Configuring the System as an Authoritative NTP Server

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ntp master [stratum]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ntp master [stratum]</code> Example: Router(config)# ntp master	Configures the Cisco IOS software as an NTPv4 master clock to which peers synchronize themselves when an external NTPv4 source is not available.

**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.

Updating the Hardware Clock

On devices that have hardware clocks (system calendars), you can configure the hardware clock to be periodically updated from the software clock. This is advisable for any device using NTPv4, because the time and date on the software clock (set using NTPv4) will be more accurate than the hardware clock, because the time setting on the hardware clock has the potential to drift slightly over time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp update-calendar**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ntp update-calendar Example: Router(config)# ntp update-calendar	Periodically updates the hardware clock (calendar) from an NTPv4 time source.

Resetting the Drift Value in the Persistent Data File

The drift is the frequency offset between the local clock hardware and the authoritative time from the Network Time Protocol version 4 (NTPv4) servers. NTPv4 automatically computes this drift and uses it to compensate permanently for local clock imperfections.

SUMMARY STEPS

1. **enable**
2. **ntp drift clear**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	ntp drift clear Example: Router# ntp drift clear	Resets the drift value stored in the persistent data file.

Troubleshooting NTPv4 in IPv6**SUMMARY STEPS**

1. enable
2. show clock [detail]
3. show ntp associations [detail]
4. show ntp status
5. debug ntp {adjust | authentication | events | loopfilter | packets | params | refclock | select | sync | validity}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	show clock [detail] Example: Router# show clock	Displays the time and date from the system software clock.
Step 3	show ntp associations [detail] Example: Router# show ntp associations	Shows the status of NTP associations.
Step 4	show ntp status Example: Router# show ntp status	Shows the status of the NTPv4.
Step 5	debug ntp {adjust authentication events loopfilter packets params refclock select sync validity} Example: Router# debug ntp	Displays debugging messages for NTPv4 features.

Configuration Examples for NTPv4 in IPv6

- [Example: Defining an NTPv4 Access Group, page 15](#)

Example: Defining an NTPv4 Access Group

In the following IPv6 example, an NTPv4 access group is enabled and a KOD packet is sent to any host that tries to send a packet that is not compliant with the access-group policy:

```
Router> enable
Router# configure terminal
Router(config)# ntp access-group serve acl1 kod
```

Additional References

Related Documents

Related Topic	Document Title
NTP for IPv4	<i>Performing Basic System Management</i>
IPv6 supported feature list	“Start Here: Cisco IOS Software Release Specifics for IPv6 Features,” <i>Cisco IOS IPv6 Configuration Guide</i>
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IPv6 Command Reference</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

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, Implementation and Analysis</i>
RFC 5905	<i>Network Time Protocol Version 4: Protocol and Algorithms Specification</i>

Technical Assistance

Description	Link
<p>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.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Implementing NTPv4 in IPv6

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 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.

Table 1 Feature Information for Implementing Selective Packet Discard in IPv6

Feature Name	Releases	Feature Information
IPv6 NTPv4	12.4(20)T 12.2(33)SXJ	The following commands were introduced or modified: debug ntp, ntp access-group, ntp authenticate, ntp authentication-key, ntp broadcast, ntp broadcast client, ntp broadcastdelay, ntp disable, ntp drift clear, ntp logging, ntp master, ntp max-associations, ntp multicast, ntp multicast client, ntp peer, ntp refclock, ntp server, ntp source, ntp trusted-key, ntp update-calendar, show clock, show ntp associations, show ntp status.

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, and 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.

© 2009–2010 Cisco Systems, Inc. All rights reserved.