Contents

Configuring NTP

Synchronize your device with a trusted time source by using the Network Time Protocol (NTP) or changing the system time before you run it on a live network. Various tasks, including network management, charging, auditing, and distributed computing depend on an accurate system time setting, because the timestamps of system messages and logs use the system time.

Overview

NTP is typically used in large networks to dynamically synchronize time among network devices. It guarantees higher clock accuracy than manual system clock setting. In a small network that does not require high clock accuracy, you can keep time synchronized among devices by changing their system clocks one by one.

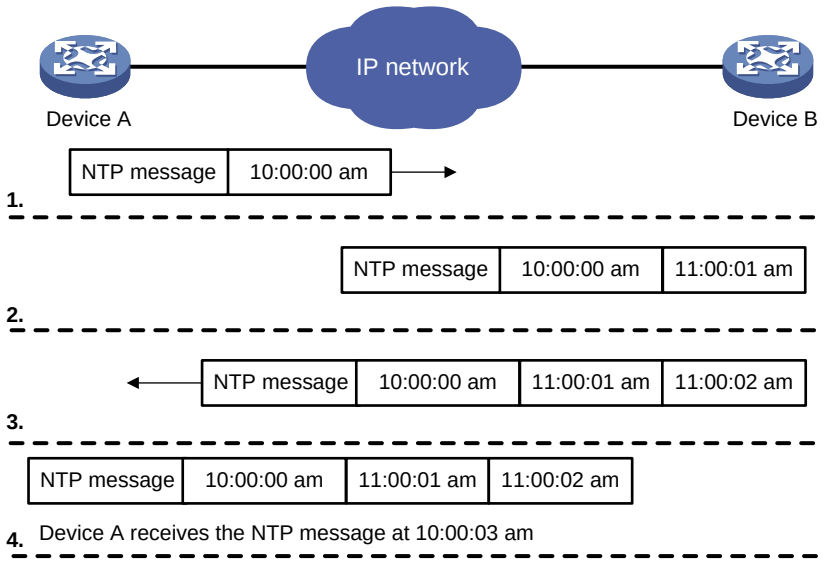
NTP runs over UDP and uses UDP port 123.

How NTP works

Figure 1 shows how NTP synchronizes the system time between two devices (Device A and Device B, in this example). Assume that:

- Prior to the time synchronization, the time is set to 10:00:00 am for Device A and 11:00:00 am for Device B.
- Device B is used as the NTP server. Device A is to be synchronized to Device B.
- It takes 1 second for an NTP message to travel from Device A to Device B, and from Device B to Device A.
- It takes 1 second for Device B to process the NTP message.

Figure 1 Basic work flow



The synchronization process is as follows:

1. Device A sends Device B an NTP message, which is timestamped when it leaves Device A. The time stamp is 10:00:00 am (T1).
2. When this NTP message arrives at Device B, Device B adds a timestamp showing the time when the message arrived at Device B. The timestamp is 11:00:01 am (T2).

3. When the NTP message leaves Device B, Device B adds a timestamp showing the time when the message left Device B. The timestamp is 11:00:02 am (T3).
4. When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

Up to now, Device A can calculate the following parameters based on the timestamps:

- The roundtrip delay of the NTP message: Delay = (T4 – T1) – (T3 – T2) = 2 seconds.
- Time difference between Device A and Device B: Offset = ((T2 – T1) + (T3 – T4)) /2 = 1 hour.

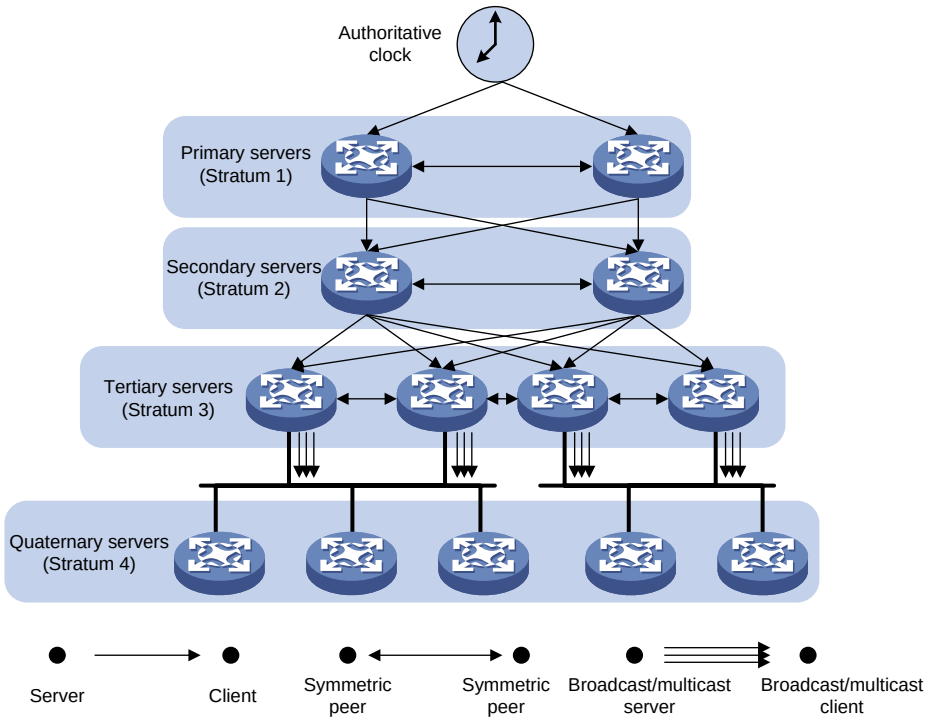
Based on these parameters, Device A can be synchronized to Device B.

This is only a rough description of the work mechanism of NTP. For more information, see the related protocols and standards.

NTP architecture

NTP uses stratums 1 to 16 to define clock accuracy, as shown in Figure 2. A lower stratum value represents higher accuracy. Clocks at stratums 1 through 15 are in synchronized state, and clocks at stratum 16 are not synchronized.

Figure 2 NTP architecture



A stratum 1 NTP server gets its time from an authoritative time source, such as an atomic clock. It provides time for other devices as the primary NTP server. A stratum 2 time server receives its time from a stratum 1 time server, and so on.

To ensure time accuracy and availability, you can specify multiple NTP servers for a device. The device selects an optimal NTP server as the clock source based on parameters such as stratum. The clock that the device selects is called the reference source. For more information about clock selection, see the related protocols and standards.

If the devices in a network cannot synchronize to an authoritative time source, you can perform the following tasks:

- Select a device that has a relatively accurate clock from the network.

- Use the local clock of the device as the reference clock to synchronize other devices in the network.

Association modes

NTP supports the following association modes:

- Client/server mode
- Symmetric active/passive mode
- Broadcast mode
- Multicast mode

Table 1 NTP association mode

Mode	Working process	Principle	Application scenario
Client/server	On the client, specify the IP address of the NTP server. A client sends a clock synchronization message to the NTP servers. Upon receiving the message, the servers automatically operate in server mode and send a reply. If the client can be synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source after receiving the replies from the servers.	A client can synchronize to a server, but a server cannot synchronize to a client.	As Figure 2 shows, this mode is intended for configurations where devices of a higher stratum synchronize to devices with a lower stratum.
Symmetric active/passive	On the symmetric active peer, specify the IP address of the symmetric passive peer. A symmetric active peer periodically sends clock synchronization messages to a symmetric passive peer. The symmetric passive peer automatically operates in symmetric passive mode and sends a reply. If the symmetric active peer can be synchronized to multiple time servers, it selects an optimal clock and synchronizes its local clock to the optimal reference source after receiving the replies from the servers.	A symmetric active peer and a symmetric passive peer can be synchronized to each other. If both of them are synchronized, the peer with a higher stratum is synchronized to the peer with a lower stratum.	As Figure 2 shows, this mode is most often used between servers with the same stratum to operate as a backup for one another. If a server fails to communicate with all the servers of a lower stratum, the server can still synchronize to the servers of the same stratum.

Mode	Working process	Principle	Application scenario
Broadcast	A server periodically sends clock synchronization messages to the broadcast address 255.255.255.255. Clients listen to the broadcast messages from the servers to synchronize to the server according to the broadcast messages. When a client receives the first broadcast message, the client and the server start to exchange messages to calculate the network delay between them. Then, only the broadcast server sends clock synchronization messages.	A broadcast client can synchronize to a broadcast server, but a broadcast server cannot synchronize to a broadcast client.	A broadcast server sends clock synchronization messages to synchronize clients in the same subnet. As Figure 2 shows, broadcast mode is intended for configurations involving one or a few servers and a potentially large client population. The broadcast mode has a lower time accuracy than the client/server and symmetric active/passive modes because only the broadcast servers send clock synchronization messages.
Multicast	A multicast server periodically sends clock synchronization messages to the user-configured multicast address. Clients listen to the multicast messages from servers and synchronize to the server according to the received messages.	A multicast client can synchronize to a multicast server, but a multicast server cannot synchronize to a multicast client.	A multicast server can provide time synchronization for clients in the same subnet or in different subnets. The multicast mode has a lower time accuracy than the client/server and symmetric active/passive modes.

In this document, an "NTP server" or a "server" refers to a device that operates as an NTP server in client/server mode. Time servers refer to all the devices that can provide time synchronization, including NTP servers, NTP symmetric peers, broadcast servers, and multicast servers.

NTP security

To improve time synchronization security, NTP provides the access control and authentication functions.

NTP access control

You can control NTP access by using an ACL. The access rights are in the following order, from the least restrictive to the most restrictive:

- **Peer**—Allows time requests and NTP control queries (such as alarms, authentication status, and time server information) and allows the local device to synchronize itself to a peer device.
- **Server**—Allows time requests and NTP control queries, but does not allow the local device to synchronize itself to a peer device.
- **Synchronization**—Allows only time requests from a system whose address passes the access list criteria.
- **Query**—Allows only NTP control queries from a peer device to the local device.

When the device receives an NTP request, it matches the request against the access rights in the order from the least restrictive to the most restrictive: **peer**, **server**, **synchronization**, and **query**.

- If no NTP access control is configured, the **peer** access right applies.

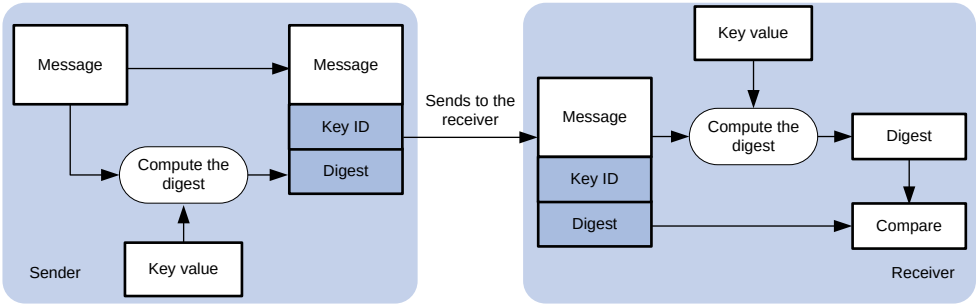
- If the IP address of the peer device matches a **permit** statement in an ACL, the access right is granted to the peer device. If a **deny** statement or no ACL is matched, no access right is granted.
- If no ACL is specified for an access right or the ACL specified for the access right is not created, the access right is not granted.
- If none of the ACLs specified for the access rights is created, the **peer** access right applies.
- If none of the ACLs specified for the access rights contains rules, no access right is granted.

This feature provides minimal security for a system running NTP. A more secure method is NTP authentication.

NTP authentication

Use this feature to authenticate the NTP messages for security purposes. If an NTP message passes authentication, the device can receive it and get time synchronization information. If not, the device discards the message. This function makes sure the device does not synchronize to an unauthorized time server.

Figure 3 NTP authentication



As shown in Figure 3, NTP authentication works as follows:

1. The sender uses the key identified by the key ID to calculate a digest for the NTP message through the specified authentication algorithm. Then it sends the calculated digest together with the NTP message and key ID to the receiver.
2. Upon receiving the message, the receiver performs the following tasks:
   a. Finds the key according to the key ID in the message.
   b. Uses the key and the same authentication algorithm to calculate the digest.
   c. Compares the digest with the digest contained in the NTP message.
      - If they are different, the receiver discards the message.
      - If they are the same and an NTP session is not required to be created, the receiver responds to the message. For information about NTP sessions, see "Configuring the maximum number of dynamic associations."
      - If they are the same and an NTP session is to be created or has been created, the local device determines whether the sender is allowed to use the authentication ID. If the sender is allowed to use the authentication ID, the receiver accepts the message. If the sender is not allowed to use the authentication ID, the receiver discards the message.

NTP for MPLS L3VPN instances

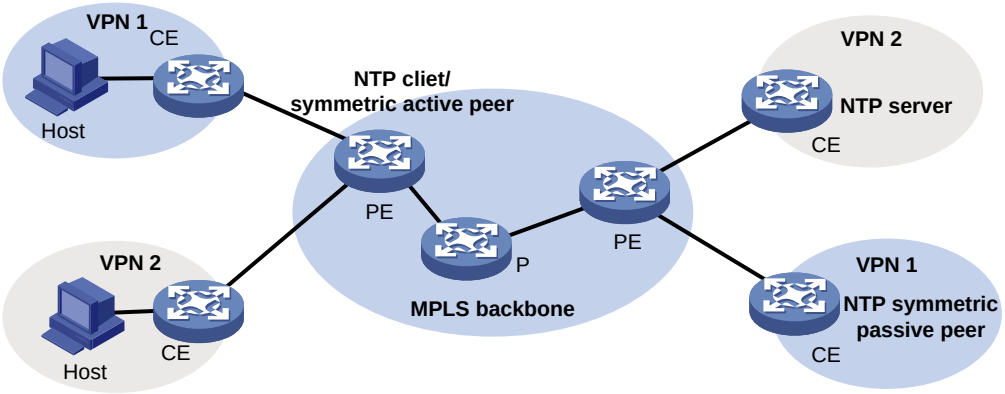
On an MPLS L3VPN network, a PE that acts as an NTP client or active peer can synchronize with the NTP server or passive peer in an MPLS L3VPN instance.

As shown in Figure 4, users in VPN 1 and VPN 2 are connected to the MPLS backbone network through provider edge (PE) devices. VPN instances vpn1 and vpn2 have been created for VPN 1 and VPN 2, respectively on the PEs. Services of the two VPN instances are isolated. Time

synchronization between PEs and devices in the two VPN instances can be realized if you perform the following tasks:

- Configure the PEs to operate in NTP client or symmetric active mode.
- Specify the VPN instance to which the NTP server or NTP symmetric passive peer belongs.

Figure 4 Network diagram



For more information about MPLS L3VPN, VPN instance, and PE, see *MPLS Configuration Guide*.

Protocols and standards

- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

Configuration restrictions and guidelines

When you configure NTP, follow these restrictions and guidelines:

- Do not configure both NTP and SNTP on the same device.
- You can configure NTP only on the following Layer 3 interfaces:
  - Layer 3 Ethernet interfaces.
  - Layer 3 Ethernet subinterfaces.
  - Layer 3 aggregate interfaces.
  - Layer 3 aggregate subinterfaces.
  - VLAN interfaces.
  - Tunnel interfaces.
- Do not configure NTP on an aggregate member port.
- The NTP service and SNTP service are mutually exclusive. You can only enable either NTP service or SNTP service at a time.
- To avoid frequent time changes or even synchronization failures, do not specify more than one reference source on a network.
- Make sure you use the **clock protocol** command to specify the time protocol as NTP. For more information about the **clock protocol** command, see device management commands in *Fundamentals Command Reference*.

Configuration task list

Tasks at a glance
(Required.) Enabling the NTP service
(Required.) Perform one or both of the following tasks: • Configuring NTP association mode • Configuring the local clock as a reference source
(Optional.) Configuring access control rights
(Optional.) Configuring NTP authentication
(Optional.) Configuring NTP optional parameters

Enabling the NTP service

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the NTP service.	**ntp-service enable**	By default, the NTP service is disabled.

Configuring NTP association mode

This section describes how to configure NTP association mode.

Configuring NTP in client/server mode

Follow these guidelines when you configure an NTP client:

- For the client to synchronize to an NTP server, make sure the server is synchronized by other devices or uses its local clock as a reference source.
- If the stratum level of a server is higher than or equal to a client, the client will not synchronize to that server.
- You can configure multiple servers by executing the **ntp-service unicast-server** or **ntp-service ipv6 unicast-server** commands multiple times.
- When the device operates in client/server mode, specify the IP address for the server on the client.

To configure an NTP client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Specify an NTP server for the device.	• Specify an NTP server for the device: **ntp-service unicast-server** { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] * • Specify an IPv6 NTP server for the device: **ntp-service ipv6 unicast-server** { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *	By default, no NTP server is specified.

Configuring NTP in symmetric active/passive mode

Follow these guidelines when you configure a symmetric-active peer:

- For a symmetric-passive peer to process NTP messages from a symmetric-active peer, execute the **ntp-service enable** command on the symmetric passive peer to enable NTP.
- For time synchronization between the symmetric-active peer and the symmetric-passive peer, make sure either or both of them are in synchronized state.
- You can configure multiple symmetric-passive peers by executing the **ntp-service unicast-peer** or **ntp-service ipv6 unicast-peer** command multiple times.
- When the device operates in symmetric active/passive mode, specify on a symmetric-active peer the IP address for a symmetric-passive peer.

To configure a symmetric-active peer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a symmetric-passive peer for the device.	• Specify a symmetric-passive peer: **ntp-service unicast-peer** { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] * • Specify an IPv6 symmetric-passive peer: **ntp-service ipv6 unicast-peer** { *peer-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *	By default, no symmetric-passive peer is specified.

Configuring NTP in broadcast mode

For a broadcast client to synchronize to a broadcast server, make sure the broadcast server is synchronized by other devices or uses its local clock as a reference source.

Configure NTP in broadcast mode on both the broadcast server and client.

Configuring a broadcast client

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	Enter the interface for receiving NTP broadcast messages.
3. Configure the device to operate in broadcast client mode.	**ntp-service broadcast-client**	By default, the device does not operate in any NTP association mode. After you execute the command, the device receives NTP broadcast messages from the specified interface.

Configuring the broadcast server

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	Enter the interface for sending NTP broadcast messages.
3. Configure the device to operate in NTP broadcast server mode.	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *	By default, the device does not operate in any NTP association mode. After you execute the command, the device sends NTP broadcast messages from the specified interface.

Configuring NTP in multicast mode

For a multicast client to synchronize to a multicast server, make sure the multicast server is synchronized by other devices or uses its local clock as a reference source.

For an IPv6 NTP multicast client to synchronize to an IPv6 NTP multicast server, make sure the client and server do not reside on different ends of a Layer 3 tunnel.

Configure NTP in multicast mode on both the multicast server and client.

Configuring a multicast client

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	Enter the interface for receiving NTP multicast messages.
3. Configure the device to operate in multicast client mode.	• Configure the device to operate in multicast client mode: **ntp-service multicast-client** [*ip-address*] • Configure the device to operate in IPv6 multicast client mode: **ntp-service ipv6 multicast-client** *ipv6-address*	By default, the device does not operate in any NTP association mode. After you execute the command, the device receives NTP multicast messages from the specified interface.

Configuring the multicast server

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	Enter the interface for sending NTP multicast message.
3. Configure the device to operate in multicast server mode.	• Configure the device to operate in multicast server mode: **ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] * • Configure the device to operate in multicast server mode: **ntp-service ipv6 multicast-server** *ipv6-address* [**authentication-keyid** *keyid* | **ttl** *ttl-number*] *	By default, the device does not operate in any NTP association mode. After you execute the command, the device receives NTP multicast messages from the specified interface.

Configuring access control rights

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the right for the peer devices to access the NTP services on the local device.	• Configure the right for the peer devices to access the IPv4 NTP services on the local device: **ntp-service access** { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number* • Configure the right for the peer devices to access the IPv6 NTP services on the local device: **ntp-service ipv6** { **peer** | **query** | **server** | **synchronization** } **acl** *ipv6-acl-number*	By default, the right for the peer devices to access the IPv6 NTP services on the local device is **peer**.

Before you configure the NTP service access control right to the local device, create and configure an ACL associated with the access control right. For more information about ACL, see *ACL and QoS Configuration Guide*.

Configuring NTP authentication

This section provides instructions for configuring NTP authentication.

Configuring NTP authentication in client/server mode

To ensure a successful NTP authentication, configure the same authentication key ID, algorithm, and key on the server and client. Make sure the peer device is allowed to use the key ID on the local device.

To configure NTP authentication for a client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.
5. Associate the specified key with an NTP server.	• Associate the specified key with an NTP server: **ntp-service unicast-server** { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid* • Associate the specified key with an IPv6 NTP server: **ntp-service ipv6 unicast-server** { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid*	N/A

To configure NTP authentication for a server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.

NTP authentication results differ when different configurations are performed on client and server. For more information, see Table 2. (N/A in the table means that whether the configuration is performed does not make any difference.)

Table 2 NTP authentication results

Client			Server		Authentication result
Enable NTP authentication	**Configure a key and configure it as a trusted key**	**Associate the key with an NTP server**	**Enable NTP authentication**	**Configure a key and configure it as a trusted key**	
Yes	Yes	Yes	Yes	Yes	Succeeded
Yes	Yes	Yes	Yes	No	Failed
Yes	Yes	Yes	No	N/A	Failed
Yes	No	Yes	N/A	N/A	Failed
Yes	N/A	No	N/A	N/A	No authentication
No	N/A	N/A	N/A	N/A	No authentication

Configuring NTP authentication in symmetric active/passive mode

To ensure a successful NTP authentication, configure the same authentication key ID, algorithm, and key on the active peer and passive peer. Make sure the peer device is allowed to use the key ID on the local device.

To configure NTP authentication for an active peer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.
5. Associate the specified key with a passive peer.	• Associate the specified key with a passive peer: **ntp-service unicast-peer** { *ip-address* | *peer-name* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid* • Associate the specified key with a passive peer: **ntp-service ipv6 unicast-peer** { *ipv6-address* | *peer-name* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid*	N/A

To configure NTP authentication for a passive peer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.

NTP authentication results differ when different configurations are performed on active peer and passive peer. For more information, see Table 3. (N/A in the table means that whether the configuration is performed does not make any difference.)

Table 3 NTP authentication results

Active peer			Passive peer		Authentication result
Enable NTP authentication	**Configure a key and configure it as a trusted key**	**Associate the key with a passive peer**	**Enable NTP authentication**	**Configure a key and configure it as a trusted key**	
Stratum level of the active and passive peers is not considered.					
Yes	Yes	Yes	Yes	Yes	Succeeded
Yes	Yes	Yes	Yes	No	Failed
Yes	Yes	Yes	No	N/A	Failed
Yes	N/A	No	Yes	N/A	Failed
Yes	N/A	No	No	N/A	No authentication
No	N/A	N/A	Yes	N/A	Failed
No	N/A	N/A	No	N/A	No authentication
The active peer has a higher stratum than the passive peer.					
Yes	No	Yes	N/A	N/A	Failed
The passive peer has a higher stratum than the active peer.					
Yes	No	Yes	Yes	N/A	Failed
Yes	No	Yes	No	N/A	No authentication

Configuring NTP authentication in broadcast mode

To ensure a successful NTP authentication, configure the same authentication key ID, algorithm, and key on the broadcast server and client. Make sure the peer device is allowed to use the authentication ID on the local device.

To configure NTP authentication for a broadcast client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.

To configure NTP authentication for a broadcast server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. Associate the specified key with the broadcast server.	**ntp-service broadcast-server authentication-keyid** *keyid*	By default, the broadcast server is not associated with any key.

NTP authentication results differ when different configurations are performed on broadcast client and server. For more information, see Table 4. (N/A in the table means that whether the configuration is performed does not make any difference.)

Table 4 NTP authentication results

Broadcast server			Broadcast client		
Enable NTP authentication	**Configure a key and configure it as a trusted key**	**Associate the key with a broadcast server**	**Enable NTP authentication**	**Configure a key and configure it as a trusted key**	**Authentication result**
Yes	Yes	Yes	Yes	Yes	Succeeded
Yes	Yes	Yes	Yes	No	Failed
Yes	Yes	Yes	No	N/A	Failed

Broadcast server			Broadcast client		Authentication result
Enable NTP authentication	**Configure a key and configure it as a trusted key**	**Associate the key with a broadcast server**	**Enable NTP authentication**	**Configure a key and configure it as a trusted key**	
Yes	No	Yes	Yes	N/A	Failed
Yes	No	Yes	No	N/A	No authentication
Yes	N/A	No	Yes	N/A	Failed
Yes	N/A	No	No	N/A	No authentication
No	N/A	N/A	Yes	N/A	Failed
No	N/A	N/A	No	N/A	No authentication

Configuring NTP authentication in multicast mode

To ensure a successful NTP authentication, configure the same authentication key ID, algorithm, and key on the multicast server and client. Make sure the peer device is allowed to use the authentication ID on the local device.

To configure NTP authentication for a multicast client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.

To configure NTP authentication for a multicast server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable NTP authentication.	**ntp-service authentication enable**	By default, NTP authentication is disabled.
3. Configure an NTP authentication key.	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no NTP authentication key exists.

Step	Command	Remarks
4. Configure the key as a trusted key.	**ntp-service reliable authentication-keyid** *keyid*	By default, no authentication key is configured as a trusted key.
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. Associate the specified key with the multicast server.	• Associate the specified key with a multicast server: **ntp-service multicast-server** [*ip-address*] **authentication-keyid** *keyid* • Associate the specified key with an IPv6 multicast server: **ntp-service ipv6 multicast-server** *ipv6-multicast-address* **authentication-keyid** *keyid*	By default, no multicast server is associated with the specified key.

NTP authentication results differ when different configurations are performed on broadcast client and server. For more information, see Table 5. (N/A in the table means that whether the configuration is performed does not make any difference.)

Table 5 NTP authentication results

Multicast server			Multicast client		
Enable NTP authentication	**Configure a key and configure it as a trusted key**	**Associate the key with a multicast server**	**Enable NTP authentication**	**Configure a key and configure it as a trusted key**	**Authentication result**
Yes	Yes	Yes	Yes	Yes	Succeeded
Yes	Yes	Yes	Yes	No	Failed
Yes	Yes	Yes	No	N/A	Failed
Yes	No	Yes	Yes	N/A	Failed
Yes	No	Yes	No	N/A	No authentication
Yes	N/A	No	Yes	N/A	Failed
Yes	N/A	No	No	N/A	No authentication
No	N/A	N/A	Yes	N/A	Failed
No	N/A	N/A	No	N/A	No authentication

Configuring NTP optional parameters

The configuration tasks in this section are optional tasks. Configure them to improve NTP security, performance, or reliability.

Specifying the source interface for NTP messages

To prevent interface status changes from causing NTP communication failures, configure the device to use the IP address of an interface that is always up. For example, you can configure the device to use a loopback interface as the source IP address for the NTP messages to be sent.

When the device responds to an NTP request, the source IP address of the NTP response is always the IP address of the interface that has received the NTP request.

Follow these guidelines when you specify the source interface for NTP messages:

- If you have specified the source interface for NTP messages in the **ntp-service unicast-server/ntp-service ipv6 unicast-server** or **ntp-service unicast-peer/ntp-service ipv6 unicast-peer** command, the specified interface acts as the source interface for NTP messages.
- If you have configured the **ntp-service broadcast-server** or **ntp-service multicast-server/ntp-service ipv6 multicast-server** command in an interface view, this interface acts as the source interface for broadcast or multicast NTP messages.

To specify the source interface for NTP messages:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the source interface for NTP messages.	• Specify the source interface for NTP messages: **ntp-service source** *interface-type interface-number* • Specify the source interface for IPv6 NTP messages: **ntp-service ipv6 source** *interface-type interface-number*	By default, no source interface is specified for NTP messages.

Disabling an interface from receiving NTP messages

When NTP is enabled, all interfaces by default can receive NTP messages. For security purposes, you can disable some of the interfaces to receive NTP messages.

To disable an interface to receive NTP messages:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Disable the interface to receive NTP messages.	• For IPv4: **undo ntp-service inbound enable** • For IPv6: **undo ntp-service ipv6 inbound enable**	By default, an interface receives NTP messages.

Configuring the maximum number of dynamic associations

NTP has the following types of associations:

- **Static association**—A manually created association.
- **Dynamic association**—Temporary association created by the system during NTP operation. A dynamic association is removed if no messages are exchanged within about 12 minutes.

The following describes how an association is established in different association modes:

- **Client/server mode**—After you specify an NTP server, the system creates a static association on the client. The server simply responds passively upon the receipt of a message, rather than creating an association (static or dynamic).
- **Symmetric active/passive mode**—After you specify a symmetric-passive peer on a symmetric active peer, static associations are created on the symmetric-active peer, and dynamic associations are created on the symmetric-passive peer.
- **Broadcast or multicast mode**—Static associations are created on the server, and dynamic associations are created on the client.

A single device can have a maximum of 128 concurrent associations, including static associations and dynamic associations.

Perform this task to restrict the number of dynamic associations to prevent dynamic associations from occupying too many system resources.

To configure the maximum number of dynamic associations:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the maximum number of dynamic sessions allowed to be established.	**ntp-service max-dynamic-sessions** *number*	By default, the command can establish up to 100 dynamic sessions.

Setting a DSCP value for NTP packets

The DSCP value determines the sending precedence of a packet.

To set a DSCP value for NTP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set a DSCP value for NTP packets.	• IPv4 packets: **ntp-service dscp** *dscp-value* • IPv6 packets: **ntp-service ipv6 dscp** *dscp-value*	The default DSCP value is 48 for IPv4 packets and 56 for IPv6 packets.

Configuring the local clock as a reference source

Follow these guidelines when you configure the local clock as a reference source:

- Make sure the local clock can provide the time accuracy required for the network. After you configure the local clock as a reference source, the local clock is synchronized, and can operate as a time server to synchronize other devices in the network. If the local clock is incorrect, timing errors occur.
- Before you configure this feature, adjust the local system time to make sure it is accurate.
- The system time reverts to the initial BIOS default after a cold reboot. As a best practice, do not configure the local clock as a reference source or configure the device as a time server.
- Devices differ in clock precision. To avoid network flapping and clock synchronization failure, do not configure multiple reference sources on the same network segment.

To configure the local clock as a reference source:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the local clock as a reference source.	**ntp-service refclock-master** [*ip-address*] [*stratum*]	By default, the device does not use the local clock as a reference source.

Displaying and maintaining NTP

Execute **display** commands in any view.

Task	Command
Display information about IPv6 NTP associations.	**display ntp-service ipv6 sessions** [**verbose**]
Display information about IPv4 NTP associations.	**display ntp-service sessions** [**verbose**]
Display information about NTP service status.	**display ntp-service status**
Display brief information about the NTP servers from the local device back to the primary reference source.	**display ntp-service trace** [**source** *interface-type interface-number*]

NTP configuration examples

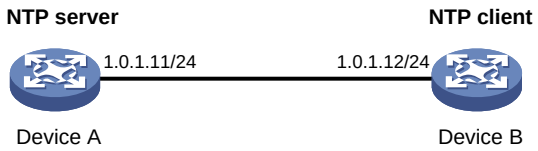
NTP client/server mode configuration example

Network requirements

As shown in Figure 5, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device B to operate in client mode and Device A to be used as the NTP server for Device B.

Figure 5 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 5. (Details not shown.)
2. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [DeviceA] ntp-service refclock-master 2
   ```
3. Configure Device B:

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Specify the time protocol as NTP.

```
[DeviceB] clock protocol ntp
```

Specify Device A as the NTP server of Device B so that Device B is synchronized to Device A.

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

4. Verify the configuration:

Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2010 18:58:07.724
```

Verify that an IPv4 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11        127.127.1.0        2     1   64   15   -4.0 0.0038 16.262
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

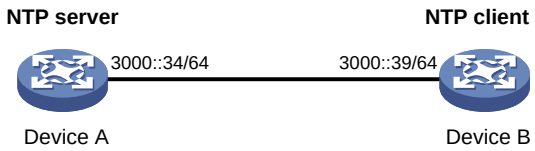
IPv6 NTP client/server mode configuration example

Network requirements

As shown in Figure 6, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device B to operate in client mode and Device A to be used as the IPv6 NTP server for Device B.

Figure 6 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 6. (Details not shown.)

2. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [DeviceA] ntp-service refclock-master 2
   ```

3. Configure Device B:

   # Enable the NTP service.

   ```
   <DeviceB> system-view
   [DeviceB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceB] clock protocol ntp
   ```

   # Specify Device A as the IPv6 NTP server of Device B so that Device B is synchronized to Device A.

   ```
   [DeviceB] ntp-service ipv6 unicast-server 3000::34
   ```

4. Verify the configuration:

   # Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

   ```
   [DeviceB] display ntp-service status
    Clock status: synchronized
    Clock stratum: 3
    System peer: 3000::34
    Local mode: client
    Reference clock ID: 163.29.247.19
    Leap indicator: 00
    Clock jitter: 0.000977 s
    Stability: 0.000 pps
    Clock precision: 2^-17
    Root delay: 0.02649 ms
    Root dispersion: 12.24641 ms
    Reference time: d0c60419.9952fb3e  Wed, Dec 29 2010 19:01:45.598
   ```

   # Verify that an IPv6 NTP association has been established between Device B and Device A.

   ```
   [DeviceB] display ntp-service ipv6 sessions
   Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

    Source: [12345]3000::34
    Reference: 127.127.1.0          Clock stratum: 2
    Reachabilities: 15              Poll interval: 64
    Last receive time: 19           Offset: 0.0
    Roundtrip delay: 0.0            Dispersion: 0.0

    Total sessions: 1
   ```

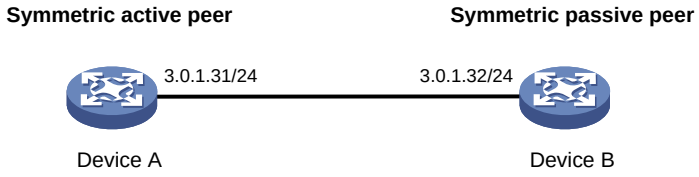
NTP symmetric active/passive mode configuration example

Network requirements

As shown in Figure 7, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device A to operate in symmetric-active mode and specify Device B as the passive peer of Device A.

Figure 7 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 7. (Details not shown.)
2. Configure Device B:

   # Enable the NTP service.

   ```
   <DeviceB> system-view
   [DeviceB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceB] clock protocol ntp
   ```

3. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceA] clock protocol ntp
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [DeviceA] ntp-service refclock-master 2
   ```

   # Configure Device B as a symmetric passive peer.

   ```
   [DeviceA] ntp-service unicast-peer 3.0.1.32
   ```

4. Verify the configuration:

   # Verify that Device B has synchronized to Device A.

   ```
   [DeviceB] display ntp-service status
    Clock status: synchronized
    Clock stratum: 3
    System peer: 3.0.1.31
    Local mode: sym_passive
    Reference clock ID: 3.0.1.31
    Leap indicator: 00
    Clock jitter: 0.000916 s
    Stability: 0.000 pps
    Clock precision: 2^-17
    Root delay: 0.00609 ms
    Root dispersion: 1.95859 ms
    Reference time: 83aec681.deb6d3e5  Wed, Jan  8 2014 14:33:11.081
   ```

   # Verify that an IPv4 NTP association has been established between Device B and Device A.

   ```
   [DeviceB] display ntp-service sessions
   ```

```
      source          reference       stra reach poll  now offset  delay disper
******************************************************************************
   [12]3.0.1.31       127.127.1.0        2    62   64   34 0.4251 6.0882 1392.1
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

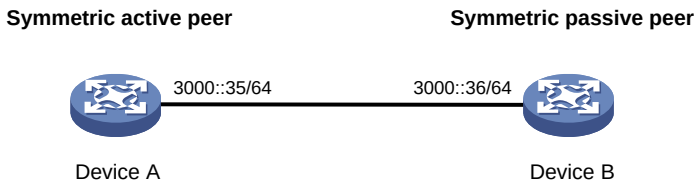
IPv6 NTP symmetric active/passive mode configuration example

Network requirements

As shown in Figure 8, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device A to operate in symmetric-active mode and specify Device B as the IPv6 passive peer of Device A.

Figure 8 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 8. (Details not shown.)
2. Configure Device B:

   # Enable the NTP service.

   ```
   <DeviceB> system-view
   [DeviceB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceB] clock protocol ntp
   ```
3. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceA] clock protocol ntp
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [DeviceA] ntp-service refclock-master 2
   ```

   # Configure Device B as an IPv6 symmetric passive peer.

   ```
   [DeviceA] ntp-service ipv6 unicast-peer 3000::36
   ```
4. Verify the configuration:

   # Verify that Device B has synchronized to Device A.

   ```
   [DeviceB] display ntp-service status
    Clock status: synchronized
    Clock stratum: 3
   ```

```
 System peer: 3000::35
 Local mode: sym_passive
 Reference clock ID: 251.73.79.32
 Leap indicator: 11
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.01855 ms
 Root dispersion: 9.23483 ms
 Reference time: d0c6047c.97199f9f  Wed, Dec 29 2010 19:03:24.590
```

Verify that an IPv6 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:  [1234]3000::35
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 15              Poll interval: 64
 Last receive time: 19           Offset: 0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions: 1
```

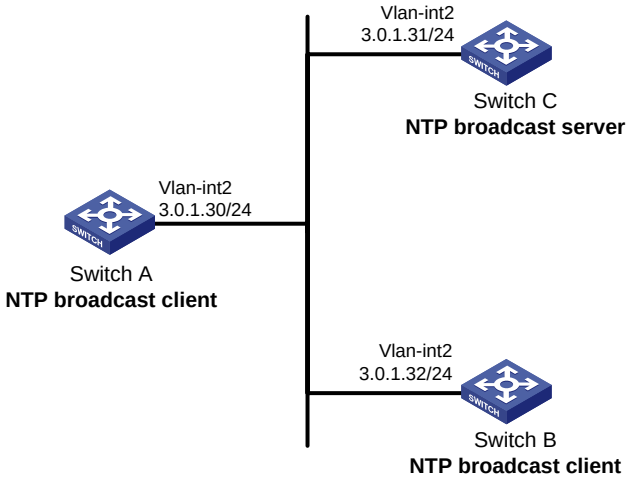
NTP broadcast mode configuration example

Network requirements

As shown in Figure 9, Switch C functions as the NTP server for multiple devices on a network segment and synchronizes the time among multiple devices.

- Configure Switch C's local clock as a reference source, with stratum level 2.
- Configure Switch C to operate in broadcast server mode and send broadcast messages from VLAN-interface 2.
- Configure Switch A and Switch B to operate in broadcast client mode, and listen to broadcast messages through VLAN-interface 2.

Figure 9 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Switch A, Switch B, and Switch C can reach each other, as shown in Figure 9. (Details not shown.)
2. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchC] clock protocol ntp
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [SwitchC] ntp-service refclock-master 2
   ```

   # Configure Switch C to operate in broadcast server mode and send broadcast messages through VLAN-interface 2.

   ```
   [SwitchC] interface vlan-interface 2
   [SwitchC-Vlan-interface2] ntp-service broadcast-server
   ```

3. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchA] clock protocol ntp
   ```

   # Configure Switch A to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ntp-service broadcast-client
   ```

4. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchB] clock protocol ntp
   ```

   # Configure Switch B to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

   ```
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ntp-service broadcast-client
   ```

5. Verify the configuration:

   # Verify that Switch A has synchronized to Switch C, and the clock stratum level is 3 on Switch A and 2 on Switch C.

   ```
   [SwitchA-Vlan-interface2] display ntp-service status
    Clock status: synchronized
    Clock stratum: 3
    System peer: 3.0.1.31
    Local mode: bclient
    Reference clock ID: 3.0.1.31
    Leap indicator: 00
    Clock jitter: 0.044281 s
    Stability: 0.000 pps
   ```

```
 Clock precision: 2^-17
 Root delay: 0.00229 ms
 Root dispersion: 4.12572 ms
 Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
```

Verify that an IPv4 NTP association has been established between Switch A and Switch C.

```
[SwitchA-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31        127.127.1.0        2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

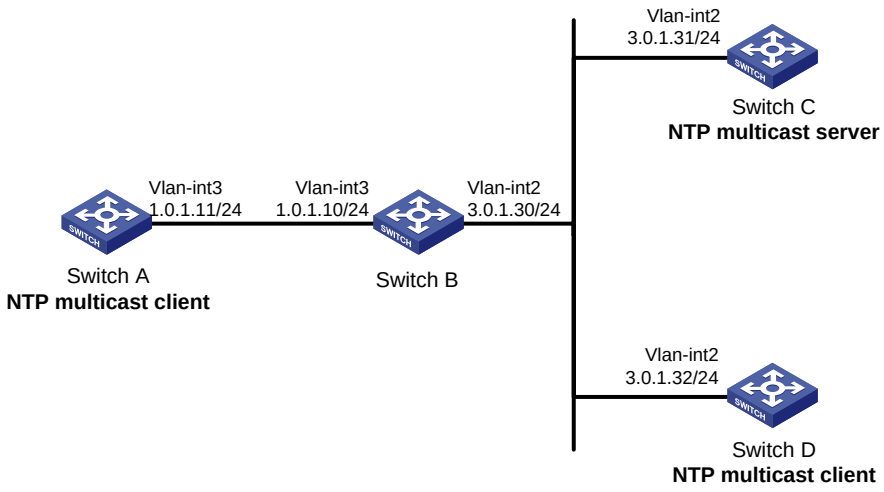
NTP multicast mode configuration example

Network requirements

As shown in Figure 10, Switch C functions as the NTP server for multiple devices on different network segments and synchronizes the time among multiple devices.

- Configure Switch C's local clock as a reference source, with stratum level 2.
- Configure Switch C to operate in multicast server mode and send multicast messages from VLAN-interface 2.
- Configure Switch A and Switch D to operate in multicast client mode and receive multicast messages through VLAN-interface 3 and VLAN-interface 2, respectively.

Figure 10 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure the switches can reach each other, as shown in Figure 10. (Details not shown.)
2. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchC] clock protocol ntp
   ```

Specify the local clock as the reference source, with stratum level 2.

```
[SwitchC] ntp-service refclock-master 2
```

Configure Switch C to operate in multicast server mode and send multicast messages through VLAN-interface 2.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

3. Configure Switch D:

Enable the NTP service.

```
<SwitchD> system-view
[SwitchD] ntp-service enable
```

Specify the time protocol as NTP.

```
[SwitchD] clock protocol ntp
```

Configure Switch D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

4. Verify the configuration:

Switch D and Switch C are on the same subnet, so Switch D can do the following:

- Receive the multicast messages from Switch C without being enabled with the multicast functions.
- Synchronize to Switch C.

Verify that Switch D has synchronized to Switch C, and the clock stratum level is 3 on Switch D and 2 on Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.044281 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00229 ms
 Root dispersion: 4.12572 ms
 Reference time: d0d289fe.ec43c720  Sat, Jan  8 2011  7:00:14.922
```

Verify that an IPv4 NTP association has been established between Switch D and Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]3.0.1.31        127.127.1.0        2     1   64  519   -0.0 0.0022 4.1257
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

5. Configure Switch B:

Because Switch A and Switch C are on different subnets, you must enable the multicast functions on Switch B before Switch A can receive multicast messages from Switch C.

Enable IP multicast routing and IGMP.

```
<SwitchB> system-view
```

```
[SwitchB] multicast routing
[SwitchB-mrib] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port ten-gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] igmp enable
[SwitchB-Vlan-interface3] igmp static-group 224.0.1.1
[SwitchB-Vlan-interface3] quit
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

6. Configure Switch A:

Enable the NTP service.

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Specify the time protocol as NTP.

```
[SwitchA] clock protocol ntp
```

Configure Switch A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

7. Verify the configuration:

Verify that Switch A has synchronized to Switch C, and the clock stratum level is 3 on Switch A and 2 on Switch C.

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.165741 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00534 ms
 Root dispersion: 4.51282 ms
 Reference time: d0c61289.10b1193f  Wed, Dec 29 2010 20:03:21.065
```

Verify that an IPv4 NTP association has been established between Switch A and Switch C.

```
[SwitchA-Vlan-interface3] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1234]3.0.1.31        127.127.1.0        2   247   64  381   -0.0 0.0053 4.5128
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
```

```
Total sessions: 1
```

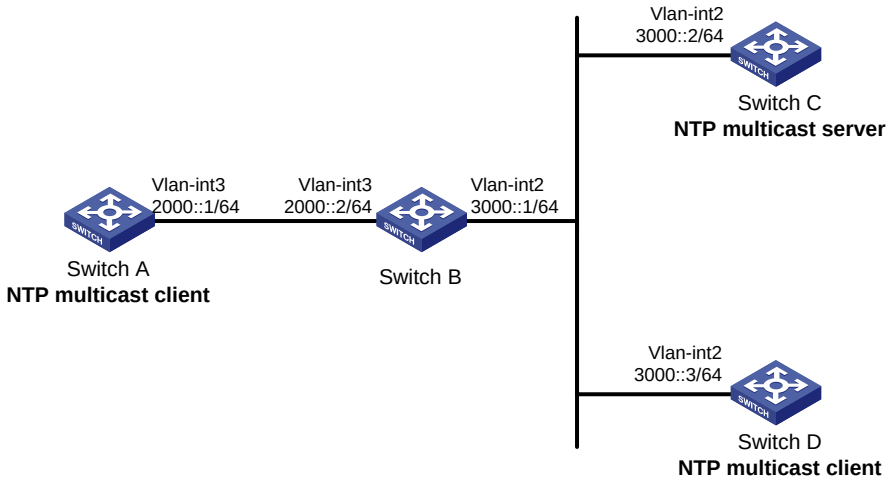
IPv6 NTP multicast mode configuration example

Network requirements

As shown in Figure 11, Switch C functions as the NTP server for multiple devices on different network segments and synchronizes the time among multiple devices.

- Configure Switch C's local clock as a reference source, with stratum level 2.
- Configure Switch C to operate in IPv6 multicast server mode and send IPv6 multicast messages from VLAN-interface 2.
- Configure Switch A and Switch D to operate in IPv6 multicast client mode and receive IPv6 multicast messages through VLAN-interface 3 and VLAN-interface 2, respectively.

Figure 11 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure the switches can reach each other, as shown in Figure 11. (Details not shown.)
2. Configure Switch C:

   # Enable the NTP service.

   ```
   <SwitchC> system-view
   [SwitchC] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchC] clock protocol ntp
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [SwitchC] ntp-service refclock-master 2
   ```

   # Configure Switch C to operate in IPv6 multicast server mode and send multicast messages through VLAN-interface 2.

   ```
   [SwitchC] interface vlan-interface 2
   [SwitchC-Vlan-interface2] ntp-service ipv6 multicast-server ff24::1
   ```

3. Configure Switch D:

   # Enable the NTP service.

   ```
   <SwitchD> system-view
   [SwitchD] ntp-service enable
   ```

Specify the time protocol as NTP.

```
[SwitchD] clock protocol ntp
```

Configure Switch D to operate in IPv6 multicast client mode and receive multicast messages on VLAN-interface 2.

```
[SwitchD] interface vlan-interface 2
[SwitchD-Vlan-interface2] ntp-service ipv6 multicast-client ff24::1
```

4. Verify the configuration:

Switch D and Switch C are on the same subnet, so Switch D can do the following:

- Receive the IPv6 multicast messages from Switch C without being enabled with the IPv6 multicast functions.
- Synchronize to Switch C.

Verify that Switch D has synchronized to Switch C, and the clock stratum level is 3 on Switch D and 2 on Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::2
 Local mode: bclient
 Reference clock ID: 165.84.121.65
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00000 ms
 Root dispersion: 8.00578 ms
 Reference time: d0c60680.9754fb17  Wed, Dec 29 2010 19:12:00.591
```

Verify that an IPv6 NTP association has been established between Switch D and Switch C.

```
[SwitchD-Vlan-interface2] display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:  [1234]3000::2
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 111             Poll interval: 64
 Last receive time: 23           Offset: -0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions: 1
```

5. Configure Switch B:

Because Switch A and Switch C are on different subnets, you must enable the IPv6 multicast functions on Switch B before Switch A can receive IPv6 multicast messages from Switch C.

Enable IPv6 multicast functions.

```
<SwitchB> system-view
[SwitchB] ipv6 multicast routing
[SwitchB-mrib6] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 pim dm
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port ten-gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] mld enable
[SwitchB-Vlan-interface3] mld static-group ff24::1
[SwitchB-Vlan-interface3] quit
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
[SwitchB] interface ten-gigabitethernet 1/0/1
[SwitchB-Ten-GigabitEthernet1/0/1] mld-snooping static-group ff24::1 vlan 3
```

6. Configure Switch A:

Enable the NTP service.

```
<SwitchA> system-view
[SwitchA] ntp-service enable
```

Specify the time protocol as NTP.

```
[SwitchA] clock protocol ntp
```

Configure Switch A to operate in IPv6 multicast client mode and receive IPv6 multicast messages on VLAN-interface 3.

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ntp-service ipv6 multicast-client ff24::1
```

7. Verify the configuration:

Verify that Switch A has synchronized to Switch C, and the clock stratum level is 3 on Switch A and 2 on Switch C.

```
[SwitchA-Vlan-interface3] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::2
 Local mode: bclient
 Reference clock ID: 165.84.121.65
 Leap indicator: 00
 Clock jitter: 0.165741 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00534 ms
 Root dispersion: 4.51282 ms
 Reference time: d0c61289.10b1193f  Wed, Dec 29 2010 20:03:21.065
```

Verify that an IPv6 NTP association has been established between Switch A and Switch C.

```
[SwitchA-Vlan-interface3] display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source:   [124]3000::2
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 2               Poll interval: 64
 Last receive time: 71           Offset: -0.0
 Roundtrip delay: 0.0            Dispersion: 0.0

 Total sessions: 1
```

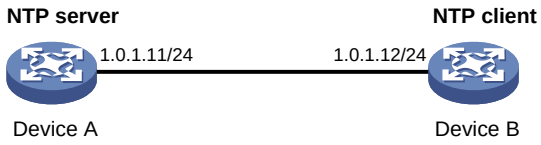
Configuration example for NTP client/server mode with authentication

Network requirements

As shown in Figure 12, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device B to operate in client mode and specify Device A as the NTP server of Device B.
- Configure NTP authentication on both Device A and Device B.

Figure 12 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 12. (Details not shown.)
2. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [DeviceA] ntp-service refclock-master 2
   ```
3. Configure Device B:

   # Enable the NTP service.

   ```
   <DeviceB> system-view
   [DeviceB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceB] clock protocol ntp
   ```

   # Enable NTP authentication on Device B.

   ```
   [DeviceB] ntp-service authentication enable
   ```

   # Set an authentication key, and input the key in plain text.

   ```
   [DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple
   aNiceKey
   ```

   # Specify the key as a trusted key.

   ```
   [DeviceB] ntp-service reliable authentication-keyid 42
   ```

   # Specify Device A as the NTP server of Device B, and associate the server with key 42.

   ```
   [DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
   ```

   Before Device B can synchronize its clock to that of Device A, enable NTP authentication for Device A.
4. Configure NTP authentication on Device A:

   # Enable NTP authentication.

   ```
   [DeviceA] ntp-service authentication enable
   ```

   # Set an authentication key, and input the key in plain text.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple
aNiceKey
```

Specify the key as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

5. Verify the configuration:

Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

Verify that an IPv4 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

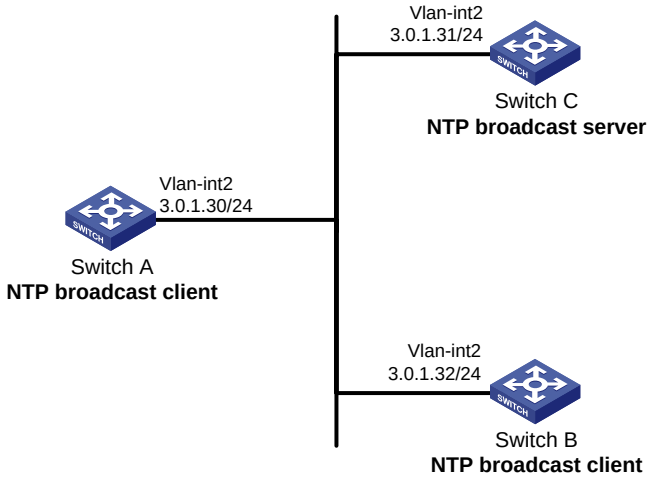
Configuration example for NTP broadcast mode with authentication

Network requirements

As shown in Figure 13, Switch C functions as the NTP server for multiple devices on different network segments and synchronizes the time among multiple devices. Switch A and Switch B authenticate the reference source.

- Configure Switch C's local clock as a reference source, with stratum level 3.
- Configure Switch C to operate in broadcast server mode and send broadcast messages from VLAN-interface 2.
- Configure Switch A and Switch B to operate in broadcast client mode and receive broadcast messages through VLAN-interface 2.
- Enable NTP authentication on Switch A, Switch B, and Switch C.

Figure 13 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Switch A, Switch B, and Switch C can reach each other, as shown in Figure 13. (Details not shown.)
2. Configure Switch A:

   # Enable the NTP service.

   ```
   <SwitchA> system-view
   [SwitchA] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchA] clock protocol ntp
   ```

   # Enable NTP authentication on Switch A. Configure an NTP authentication key, with the key ID of 88 and key value of 123456. Input the key in plain text, and specify it as a trusted key.

   ```
   [SwitchA] ntp-service authentication enable
   [SwitchA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
   [SwitchA] ntp-service reliable authentication-keyid 88
   ```

   # Configure Switch A to operate in NTP broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ntp-service broadcast-client
   ```

3. Configure Switch B:

   # Enable the NTP service.

   ```
   <SwitchB> system-view
   [SwitchB] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [SwitchB] clock protocol ntp
   ```

   # Enable NTP authentication on Switch B. Configure an NTP authentication key, with the key ID of 88 and key value of 123456. Input the key in plain text and specify it as a trusted key.

   ```
   [SwitchB] ntp-service authentication enable
   [SwitchB] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
   [SwitchB] ntp-service reliable authentication-keyid 88
   ```

   # Configure Switch B to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

   ```
   [SwitchB] interface vlan-interface 2
   ```

```
[SwitchB-Vlan-interface2] ntp-service broadcast-client
```

4. Configure Switch C:

Enable the NTP service.

```
<SwitchC> system-view
[SwitchC] ntp-service enable
```

Specify the time protocol as NTP.

```
[SwitchC] clock protocol ntp
```

Specify the local clock as the reference source, with stratum level 3.

```
[SwitchC] ntp-service refclock-master 3
```

Configure Switch C to operate in NTP broadcast server mode and use VLAN-interface 2 to send NTP broadcast packets.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server
[SwitchC-Vlan-interface2] quit
```

5. Verify the configuration:

NTP authentication is enabled on Switch A and Switch B, but not on Switch C, so Switch A and Switch B cannot synchronize their local clocks to Switch C.

Verify that Switch B has not synchronized to Switch C.

```
[SwitchB-Vlan-interface2] display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
```

6. Enable NTP authentication on Switch C:

Enable NTP authentication on Switch C. Configure an NTP authentication key, with the key ID of 88 and key value of 123456. Input the key in plain text, and specify it as a trusted key.

```
[SwitchC] ntp-service authentication enable
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[SwitchC] ntp-service reliable authentication-keyid 88
```

Specify Switch C as an NTP broadcast server, and associate the key 88 with Switch C.

```
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

7. Verify the configuration:

Verify that Switch B has synchronized to Switch C, and the clock stratum level is 4 on Switch B and 3 on Switch C.

```
[SwitchB-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 4
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.006683 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00127 ms
 Root dispersion: 2.89877 ms
 Reference time: d0d287a7.3119666f  Sat, Jan  8 2011  6:50:15.191
```

Verify that an IPv4 NTP association has been established between Switch B and Switch C.

```
[SwitchB-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
 [1245]3.0.1.31        127.127.1.0        3     3   64   68   -0.0 0.0000    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

Configuration example for MPLS L3VPN network time synchronization in client/server mode

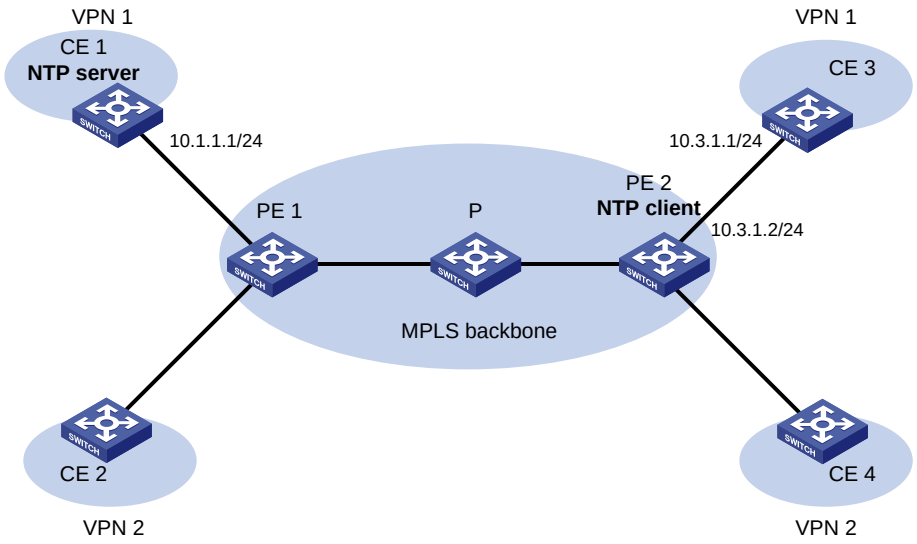
Network requirements

As shown in Figure 14, two MPLS L3VPN instances are present on PE 1 and PE 2: vpn1 and vpn2. CE 1 and CE 3 are devices in VPN 1.

To synchronize time between PE 2 and CE 1 in VPN 1, perform the following tasks:

- Configure CE 1's local clock as a reference source, with stratum level 2.
- Configure CE 1 in the VPN instance vpn1 as the NTP server of PE 2.

Figure 14 Network diagram



Configuration procedure

Before you perform the following configuration, be sure you have completed MPLS L3VPN-related configurations. For information about configuring MPLS L3VPN, see *MPLS Configuration Guide*.

1. Assign an IP address to each interface, as shown in Figure 14. Make sure CE 1 and PE 1, PE 1 and PE 2, and PE 2 and CE 3 can reach each other. (Details not shown.)
2. Configure CE 1:

   # Enable the NTP service.

   ```
   <CE1> system-view
   [CE1] ntp-service enable
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [CE1] ntp-service refclock-master 2
   ```
3. Configure PE 2:

   # Enable the NTP service.

```
<PE2> system-view
[PE2] ntp-service enable
```

Specify the time protocol as NTP.

```
[PE2] clock protocol ntp
```

Specify CE 1 in the VPN instance vpn1 as the NTP server of PE 2.

```
[PE2] ntp-service unicast-server 10.1.1.1 vpn-instance vpn1
```

4. Verify the configuration:

Verify that PE 2 has synchronized to CE 1, with stratum level 3.

```
[PE2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 10.1.1.1
 Local mode: client
 Reference clock ID: 10.1.1.1
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

Verify that an IPv4 NTP association has been established between PE 2 and CE 1.

```
[PE2] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
 [1245]10.1.1.1        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

Verify that server 127.0.0.1 has synchronized to server 10.1.1.1, and server 10.1.1.1 has synchronized to the local clock.

```
[PE2] display ntp-service trace
Server     127.0.0.1
Stratum    3 , jitter  0.000, synch distance 796.50.
Server     10.1.1.1
Stratum    2 , jitter 939.00, synch distance 0.0000.
RefID      127.127.1.0
```

Configuration example for MPLS L3VPN network time synchronization in symmetric active/passive mode

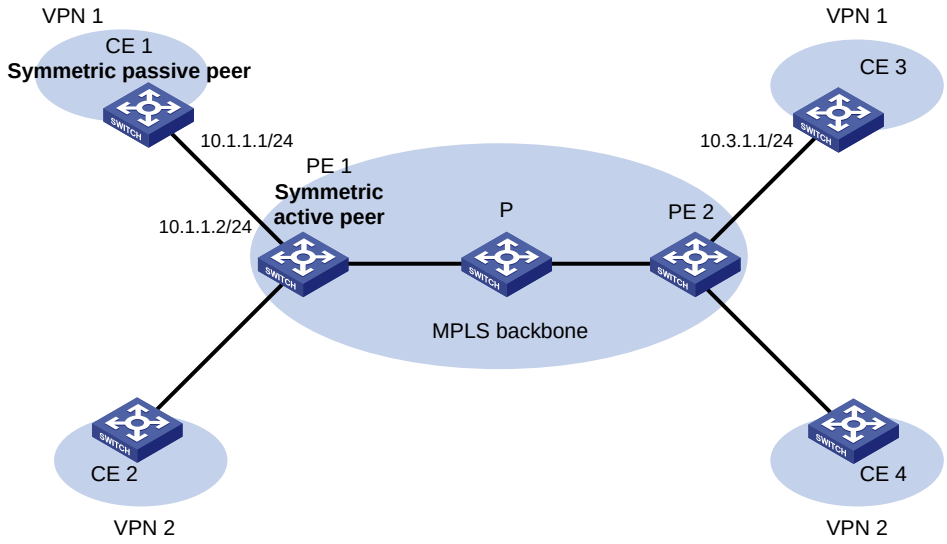
Network requirements

As shown in Figure 15, two VPN instances are present on PE 1 and PE 2: vpn1 and vpn2. CE 1 and CE 3 belong to VPN 1.

To synchronize time between PE 1 and CE 1 in VPN 1, perform the following tasks:

- Configure CE 1's local clock as a reference source, with stratum level 2.
- Configure CE 1 in the VPN instance vpn1 as the symmetric-passive peer of PE 1.

Figure 15 Network diagram



Configuration procedure

Before you perform the following configuration, be sure you have completed MPLS L3VPN-related configurations. For information about configuring MPLS L3VPN, see *MPLS Configuration Guide*.

1. Assign an IP address to each interface, as shown in Figure 15. Make sure CE 1 and PE 1, PE 1 and PE 2, and PE 2 and CE 3 can reach each other. (Details not shown.)
2. Configure CE 1:

   # Enable the NTP service.

   ```
   <CE1> system-view
   [CE1] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [CE1] clock protocol ntp
   ```

   # Specify the local clock as the reference source, with stratum level 2.

   ```
   [CE1] ntp-service refclock-master 2
   ```

3. Configure PE 1:

   # Enable the NTP service.

   ```
   <PE1> system-view
   [PE1] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [PE1] clock protocol ntp
   ```

   # Specify CE 1 in the VPN instance vpn1 as the symmetric-passive peer of PE 1.

   ```
   [PE1] ntp-service unicast-peer 10.1.1.1 vpn-instance vpn1
   ```

4. Verify the configuration:

   # Verify that PE 1 has synchronized to CE 1, with stratum level 3.

   ```
   [PE1] display ntp-service status
    Clock status: synchronized
    Clock stratum: 3
    System peer: 10.1.1.1
    Local mode: sym_active
    Reference clock ID: 10.1.1.1
    Leap indicator: 00
   ```

```
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-17
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

Verify that an IPv4 NTP association has been established between PE 1 and CE 1.

```
[PE1] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
********************************************************************************
 [1245]10.1.1.1        127.127.1.0        2     1   64  519   -0.0 0.0000    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

Verify that server 127.0.0.1 has synchronized to server 10.1.1.1, and server 10.1.1.1 has synchronized to the local clock.

```
[PE1] display ntp-service trace
Server     127.0.0.1
Stratum    3 , jitter  0.000, synch distance 796.50.
Server     10.1.1.1
Stratum    2 , jitter 939.00, synch distance 0.0000.
RefID      127.127.1.0
```

Configuring SNTP

SNTP is a simplified, client-only version of NTP specified in RFC 4330. SNTP supports only the client/server mode. An SNTP-enabled device can receive time from NTP servers, but cannot provide time services to other devices.

SNTP uses the same packet format and packet exchange procedure as NTP, but provides faster synchronization at the price of time accuracy.

If you specify multiple NTP servers for an SNTP client, the server with the best stratum is selected. If multiple servers are at the same stratum, the NTP server whose time packet is first received is selected.

Configuration restrictions and guidelines

When you configure SNTP, follow these restrictions and guidelines:

- You cannot configure both NTP and SNTP on the same device.
- Make sure you use the **clock protocol** command to specify the time protocol as NTP.

Configuration task list

Tasks at a glance
(Required.) Enabling the SNTP service
(Required.) Specifying an NTP server for the device
(Optional.) Configuring SNTP authentication

Enabling the SNTP service

The NTP service and SNTP service are mutually exclusive. You can only enable either NTP service or SNTP service at a time.

To enable the SNTP service:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SNTP service.	**sntp enable**	By default, the SNTP service is not enabled.

Specifying an NTP server for the device

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Specify an NTP server for the device.	• For IPv4: **sntp unicast-server** { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **source** *interface-type interface-number* | **version** *number*] * • For IPv6: **sntp ipv6 unicast-server** { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **source** *interface-type interface-number*] *	By default, no NTP server is specified for the device. Repeat this step to specify multiple NTP servers. To use authentication, you must specify the **authentication-keyid** *keyid* option.

To use an NTP server as the time source, make sure its clock has been synchronized. If the stratum level of the NTP server is greater than or equal to that of the client, the client does not synchronize with the NTP server.

Configuring SNTP authentication

SNTP authentication ensures that an SNTP client is synchronized only to an authenticated trustworthy NTP server.

Follow these guidelines when you configure SNTP authentication:

- Enable authentication on both the NTP server and the SNTP client.
- Use the same authentication key ID, algorithm, and key on the NTP server and SNTP client. Specify the key as a trusted key on both the NTP server and the SNTP client. For information about configuring NTP authentication on an NTP server, see "Configuring NTP."
- On the SNTP client, associate the specified key with an NTP server on the SNTP client. Make sure the server is allowed to use the key ID for authentication on the client.

With authentication disabled, the SNTP client can synchronize with the NTP server regardless of whether the NTP server is enabled with authentication.

To configure SNTP authentication on the SNTP client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable SNTP authentication.	**sntp authentication enable**	By default, SNTP authentication is disabled.
3. Configure an SNTP authentication key.	**sntp authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number* | **ipv6 acl** *ipv6-acl-number*] *	By default, no SNTP authentication key exists.
4. Specify the key as a trusted key.	**sntp reliable authentication-keyid** *keyid*	By default, no trusted key is specified.

Step	Command	Remarks
5. Associate the SNTP authentication key with an NTP server.	• For IPv4: **sntp unicast-server** { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid* • For IPv6: **sntp ipv6 unicast-server** { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] **authentication-keyid** *keyid*	By default, no NTP server is specified.

Displaying and maintaining SNTP

Execute **display** commands in any view.

Task	Command
Display information about all IPv6 SNTP associations.	**display sntp ipv6 sessions**
Display information about all IPv4 SNTP associations.	**display sntp sessions**

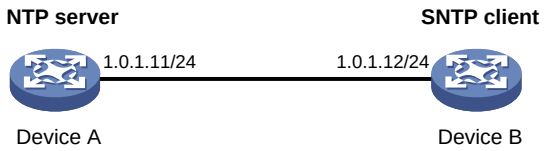
SNTP configuration example

Network requirements

As shown in Figure 16, perform the following tasks:

- Configure the local clock of Device A as a reference source, with stratum level 2.
- Configure Device B to operate in SNTP client mode, and specify Device A as the NTP server.
- Configure NTP authentication on Device A and SNTP authentication on Device B.

Figure 16 Network diagram



Configuration procedure

1. Assign an IP address to each interface, and make sure Device A and Device B can reach each other, as shown in Figure 16. (Details not shown.)
2. Configure Device A:

   # Enable the NTP service.

   ```
   <DeviceA> system-view
   [DeviceA] ntp-service enable
   ```

   # Specify the time protocol as NTP.

   ```
   [DeviceA] clock protocol ntp
   ```

Configure the local clock of Device A as a reference source, with stratum level 2.

```
[DeviceA] ntp-service refclock-master 2
```

Enable NTP authentication on Device A.

```
[DeviceA] ntp-service authentication enable
```

Configure an NTP authentication key, with the key ID of **10** and key value of **aNiceKey**. Input the key in plain text.

```
[DeviceA] ntp-service authentication-keyid 10 authentication-mode md5 simple
aNiceKey
```

Specify the key as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 10
```

3. Configure Device B:

Enable the SNTP service.

```
<DeviceB> system-view
[DeviceB] sntp enable
```

Specify the time protocol as NTP.

```
[DeviceB] clock protocol ntp
```

Enable SNTP authentication on Device B.

```
[DeviceB] sntp authentication enable
```

Configure an SNTP authentication key, with the key ID of **10** and key value of **aNiceKey**. Input the key in plain text.

```
[DeviceB] sntp authentication-keyid 10 authentication-mode md5 simple aNiceKey
```

Specify the key as a trusted key.

```
[DeviceB] sntp reliable authentication-keyid 10
```

Specify Device A as the NTP server of Device B, and associate the server with key 10.

```
[DeviceB] sntp unicast-server 1.0.1.11 authentication-keyid 10
```

4. Verify the configuration:

Verify that an SNTP association has been established between Device B and Device A, and Device B has synchronized to Device A.

```
[DeviceB] display sntp sessions
NTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Tue, May 17 2011  9:11:20.833 (Synced)
```