Contents

1 Configuring NTP

1.1 Introduction

1.1.1 Overview

Network Time Protocol (NTP) is an application-layer protocol that enables network devices to synchronize time. NTP enables network devices to synchronize time with their servers or clock sources and provides high-precision time correction (the difference from the standard time is smaller than one millisecond in a LAN and smaller than decades of milliseconds in a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment. NTP is implemented based on the transport protocol, User Datagram Protocol (UDP), and the UDP port used is 123.

Currently, Orion_B26Q devices can be used both as NTP clients and NTP servers. In other words, a Orion_B26Q device can synchronize time with a time server, or act as a time server to provide time synchronization for other devices.

1.1.2 Principles

1. Basic Concepts

- NTP server

  A device uses a local clock as the reference clock source to provide time synchronization for other devices in the network.

- NTP client

  A device synchronizes time with an NTP server in the network.

- **Stratum**

  In NTP, "stratum" is used to describe the hops from a device to an authority clock source. An NTP server whose stratum is 1 has a directly connected atomic clock or radio controlled clock; an NTP server whose stratum is 2 obtains time from the server whose stratum is 1; an NTP server whose stratum is 3 obtains time from the server whose stratum is 2; and so on. Therefore, clock sources with lower stratum have higher clock precision.

- Hardware Clock

  A hardware clock operates based on the frequency of the quartz crystal resonator on a device and is powered by the device battery. After the device is shut down, the hardware clock continues running. After the device is started, the device obtains time information from the hardware clock as the software time of the device.

2. NTP Principles

As shown in Figure 1-2, a client exchanges NTP packets with a server to implement time synchronization.

(1) The client sends a time synchronization request packet to all servers every 64 seconds.

(2) After receiving response packets from the servers, the client filters these response packets, and synchronizes time with an optimum server.

3. NTP Working Process

As shown in Figure 1-2, device B (B for short) acts as an NTP reference clock source, and device A (A for short) acts as an NTP client that synchronizes time with B. At a time point, the local clock of A is 19:00:00 and the local clock of B is 19:30:20.

(1) A sends an NTP request packet. The local time (T0) when the packet leaves from A is 19:00:00 and is filled in **Originate Timestamp**.

(1) After a network delay of 2s, the local time (T1) when B receives the request packet is 19:30:23 and is filled in **Receive Timestamp**.

(2) B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from B is 19:30:24 and is filled in **Transmit Timestamp**.

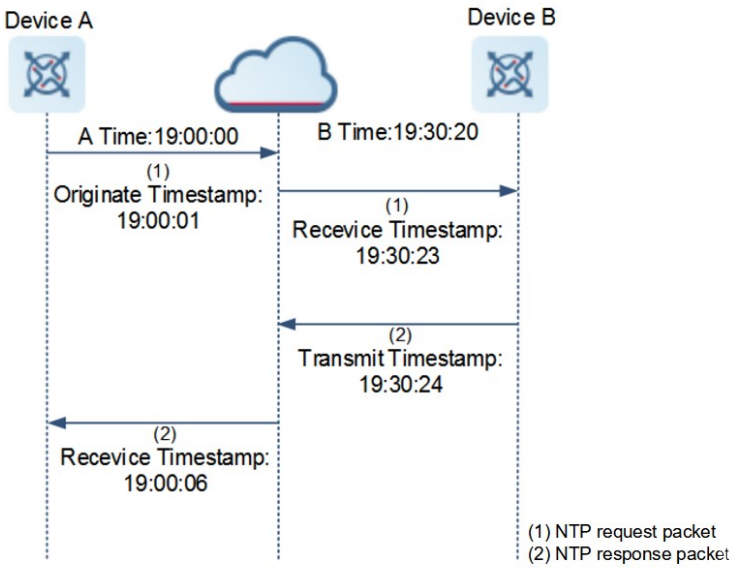
(3) After a network delay of 2s, A receives the response packet. The local time (T3) when the response packet arrives at A is 19:00:06.

The specific calculations for time synchronization are as follows:

a A obtains the time difference of 30 minutes and 20 seconds between B and A by using the formula ((T1-T0)+(T2-T3))/2.

b A obtains the packet round-trip delay of 4 seconds between A and B by using the formula (T3-T0)-(T2-T1).

Figure 1-2NTP Principles



- NTP working mode
  - External clock reference mode: In this mode, a device acts as both a server and a client. If receiving time synchronization requests from other clients, the device must synchronize time with the specified server, and then provide the time synchronization service for the clients only after successful synchronization with the specified server.

- Local clock reference mode: In this mode, a device uses the default local clock as the reliable clock source and provides the time synchronization service directly for other clients.

4. NTP Security Mechanism

To prevent malicious damage to the time server and improve the security of time synchronization, NTP provides security authentication and access control functions.

- Security authentication

  NTP uses the authentication mechanism to check whether the time synchronization information really comes from the announced server and check the information return path to provide an anti-interference protection mechanism.

  An NTP client and an NTP server are configured with the same key. When sending request and response packets, a device calculates the hash values of the packets by using the MD5 algorithm based on the specified key and NTP packet content, and fills the hash values into the packet authentication information. The receiving device checks whether the packets are sent by a trusted device or modified based on the authentication information.

- NTP access control using the kiss-o-death (KoD) packet

  NTP provides a minimum security measure by using an ACL. Normally, the denial-of-service packets are discarded, and there is no operation other than incrementing the statistics counter. Sometimes a more proactive response is required. For example, the client is explicitly requested to stop sending packets to the server and to leave a message for the system operator. Therefore, open-source NTP proposes a KoD packet, which can be used to respond to special processing of the client when access control is configured on the server.

  The format of a KoD packet is the same as that of a common NTP packet, except that the **Leap Indicator** field is set to **clock unsynchronized**, the **Stratum** field is set to **0**, and the **Reference ID** field is set to a 4-byte ASCII code. The code is "RATE" if the limited flag is set and the rate threshold is exceeded. After the NTP client receives the KoD packet with the code "RATE", it limits the rate according to the minimum interval specified in the packet.

1.1.3 Protocols and Standards

- RFC 1305: Network Time Protocol (Version 3)
- RFC 5905: Network Time Protocol (Version 4)

1.2 Restrictions and Guidelines

- You cannot configure both the NTP and SNTP functions on the same device.
- Only L3 interfaces support NTP.
- To ensure accuracy of time synchronization, avoid configuring two or more clock sources whenever possible to prevent clock flapping.
- You can run the **ntp service disable** command to disable the NTP server function so that the device acts only as a client. This command cannot be configured together with **ntp master**.

1.3 Configuration Task Summary

NTP configuration includes the following tasks:

(1) (Optional) Configuring NTP Security Authentication

(2) Configuring NTP in Client/Server Mode

(3) (Optional) Configuring NTP-Related Parameters

(4) (Optional) Configuring NTP Access Control

1.4 Configuring NTP Security Authentication

1.4.1 Overview

- Synchronizing time from a trusted reference clock source: Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock.
- Providing time synchronization for a trusted device: Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

1.4.2 Restrictions and Guidelines

- The authentication keys of the client and server must be the same.
- To provide time synchronization for a trusted device, you must specify a trusted authentication key by using the key ID. Only one trusted key can be configured. The specified authentication key must be consistent with that of the trusted device.
- To synchronize time with a trusted reference clock source, you must specify a trusted authentication key by using the key ID. Each trusted reference clock source is mapped to an authentication key. The authentication keys must be consistent with the keys of trusted reference clock sources.
- By default, a client does not use a global security authentication mechanism. If no security authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that the communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must also be configured for initiating encrypted communication between the client and server.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a global security authentication mechanism for NTP.

ntp authenticate

(4) Configure a global authentication key for NTP.

ntp authentication-key *authentication-key-id* **md5** *authentication-key-string* [*enc-type*]

The NTP global authentication mechanism is disabled by default.

(5) (Optional) Configure a globally trusted key ID for NTP.

ntp trusted-key *trusted-key-id*

(6) (Optional) Configure an authentication key ID for an external reference clock source.

ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-addr* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *interface-type interface-number*] [**key** *keyid*] [**prefer**] [**via** *mgmt-name*]

By default, no authentication key ID is configured for an external reference clock source.

1.5 Configuring NTP in Client/Server Mode

1. Overview

This section describes how to configure a device as a client to synchronize time from an external reference clock source to the local clock. After successful time synchronization, the device can act as a time synchronization server to provide the time synchronization service.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an NTP server.

ntp server [**oob** | **vrf** *vrf-name*] { *ipv4-address* | *ipv6-address* | *peer-hostname* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *interface-type interface-number*] [**key** *keyid*] [**prefer**] [**via** *mgmt-name*]

No NTP server is configured by default.

1.6 Configuring NTP-Related Parameters

1.6.1 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the interval for time synchronization with the external server.

ntp interval *synchronization-interval-time*

By default, the NTP synchronization interval is 64s.

(4) (Optional) Configure automatic update of the hardware clock.

ntp update-calendar

Automatic update of the hardware clock is not configured by default.

(5) (Optional) Configure the NTP master clock.

ntp master [*stratum*]

The NTP master clock is disabled by default.

stratum: specifies the stratum of a local clock, ranging from 1 to 15. The default value is 8.

(6) (Optional) Disable the NTP time synchronization service provided for other devices.

ntp service disable

The NTP time synchronization service is enabled by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) (Optional) Disable receiving of NTP packets on an interface.

ntp disable

The function of receiving NTP packets on an interface is enabled by default.

1.7 Configuring NTP Access Control

1.7.1 Overview

NTP access control provides a minimum security measure. A more secure method is to use the NTP authentication mechanism.

1.7.2 Restrictions and Guidelines

- If no access control rule is configured, all NTP services can be accessed. If access control rules are configured, only NTP services that comply with the access control rules can be accessed.
- The system currently does not support the access control query function.
- If the packet request interval of the NTP client is smaller than that allowed by the server, the NTP server discards the packets. This function takes effect only after the **ntp access-group limited access-list-number** | **access-list-name** [**kod**] command is configured. When the KoD-enabled NTP device acts as a client, it reduces the rate after receiving a KoD packet. A KoD-disabled device does not reduce the rate. Note that KoD cannot be triggered by specifying the interval in the **ntp interval** command.
- You can run the **ntp discard** command to configure the packet request interval allowed by the server. If the packet request interval of the NTP client is smaller than that allowed by the server, the NTP server discards the packets. This function takes effect only after the **ntp access-group limited access-list-number** | **access-list-name** [**kod**] command is configured.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the NTP access control rights.

ntp access-group { **limited** | **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name* [**kod**]

No NTP access control rule is configured by default.

(4) (Optional) Configure the minimum packet interval allowed by NTP.

ntp discard min-spacing *discard-min-spacing-interval* **avg-spacing** *avg-spacing-interval*

By default, the minimum packet request interval allowed by NTP is 2s, and the average packet request interval is 8s.

1.8 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1NTP Monitoring

Command	Purpose
show ntp status	Displays the current NTP information.
show ntp packets	Displays the sent and received NTP packets.
show ntp server	Displays the NTP server information.
show ntp server	Displays the NTP server list.
debug ntp	Debugs the DNS function.
no debug ntp	Disables the debugging function.

1.9 Configuration Examples

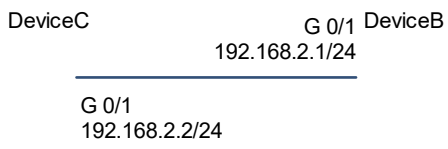
1.9.1 Configuring the Local Clock Reference Mode of NTP

1. Requirements

Use the local clock of a device as the NTP reference clock source to provide time synchronization.

2. Topology

Figure 1-1Local Clock Reference Mode of NTP



3. Notes

- Configure the local clock of device B as the NTP reference clock source.

- Device C synchronizes time from device B.

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device C to 192.168.2.2/24.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure device B as the NTP server.

```
DeviceB(config)# ntp master
```

Enable the NTP function on device C.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# ntp server 192.168.2.1
DeviceC(config)# ntp enable
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device C.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device B.

```
DeviceB# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device C to check whether time synchronization is successful.

```
DeviceC# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
```

```
ntp master
!
end
```

- Device C configuration file

```
hostname DeviceC
!
ntp server 192.168.2.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
end
```

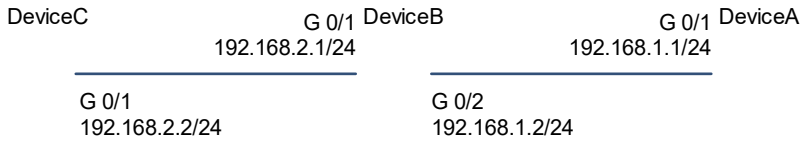
1.9.2 Configuring the External Clock Reference Mode of NTP

1. Requirements

Use a device as a client to synchronize time from an external reference clock source to the local clock. After successful time synchronization, the device can act as a time synchronization server to provide the time synchronization service.

2. Topology

Figure 1-1Topology for the External Clock Reference Mode of NTP



3. Notes

- Configure the NTP external clock reference mode on device B.
- Configure device A as the reference clock source of device B.
- Device C synchronizes time from device B.

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.1.1/24.

```
DeviceA> enble
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24, and the IP address of GigabitEthernet 0/2 to 192.168.1.2/24.

```
DeviceB> enble
```

```
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
DeviceB(config)# interface gigabitEthernet 0/2
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device C to 192.168.2.2/24.

```
DeviceC> enble
DeviceC# configure terminal
DeviceC(config)# interface gigabitEthernet 0/1
DeviceC(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceC(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B.

```
DeviceA(config)# ntp master
```

Configure the NTP external clock reference mode on device B.

```
DeviceB(config)# ntp server 192.168.1.1
```

Enable device C to synchronize time from device B.

```
DeviceC(config)# ntp server 192.168.2.1
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.1.1
Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command to verify L3 reachability between device B and device C.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **show ntp status** command to display the NTP configuration.

```
DeviceB# sh ntp status
Clock is synchronized, stratum 9, reference is 192.168.1.1
nominal freq is 250.000 Hz, actual freq is 250.000 Hz, precision is 2**18
reference time is E3527947.D5254A29 (14:03:51.000 UTC Sun, Nov 8, 2020)
clock offset is -0.00012 sec, root delay is 0.00282 sec
root dispersion is 0.01153 msec, peer dispersion is 0.00025 msec
system poll interval is 64, last update was 43 sec ago
system time(GMT) is E3527973.740AB522 (14:04:35.000 GMT Sun, Nov 8, 2020)
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device C to check whether time synchronization is successful.

```
DeviceC# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 192.168.1.1 255.255.255.0
ntp master
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ntp server 192.168.1.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
interface GigabitEthernet 0/2
 ip address 192.168.1.2 255.255.255.0
!
end
```

- Device C configuration file

```
hostname DeviceC
!
ntp server 192.168.2.1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
end
```

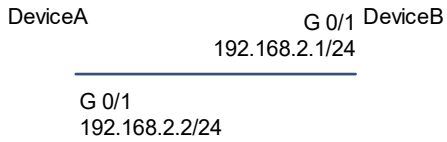
1.9.3 Configuring NTP Security Authentication

1. Requirements

Use a device as a client to synchronize time only from a trusted external reference clock source to the local clock. Use the local clock of a device as the NTP reference clock source to provide time synchronization for only a trusted device.

2. Topology

Figure 1-1Topology for NTP Security Authentication



3. Notes

- Configure device A as the reference clock source of device B, enable device A to provide device B with the NTP service that requires security authentication, and set the authentication key to "abcd".

4. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.2.2/24.

```
DeviceA> enble
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B, enable device A to provide device B with the NTP service that requires security authentication, and set the authentication key to "abcd".

```
DeviceB(config)# ntp authenticate
DeviceB(config)# ntp authentication-key 1 md5 abcd
DeviceB(config)# ntp trusted-key 1
DeviceB(config)# ntp server 192.168.2.2
```

5. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
```

```
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
ntp master
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ntp authentication-key 1 md5 abcd
ntp authenticate
ntp trusted-key 1
ntp server 192.168.2.2
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
end
```

1.9.4 Configuring NTP Access Control Rights

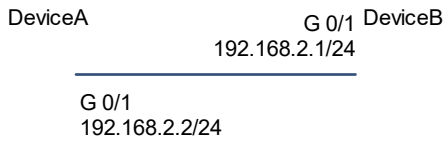
1. Requirements

Configure the access control function to prevent malicious damage to the time server and improve the security of time synchronization.

Use a device as a client to synchronize time only from the specified external reference clock source to the local clock.

2. Topology

Figure 1-1Topology for Implementing NTP Access Control Rights



3. Procedure

Set the IP address of GigabitEthernet 0/1 on device A to 192.168.2.2/24.

```
DeviceA> enble
DeviceA# configure terminal
DeviceA(config)# interface gigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.168.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Set the IP address of GigabitEthernet 0/1 on device B to 192.168.2.1/24.

```
DeviceB> enble
DeviceB# configure terminal
DeviceB(config)# interface gigabitEthernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure device A as the reference clock source of device B. Allow only the device with the IP address of 192.168.2.2 to send a time synchronization request to the local device.

```
DeviceB(config)# ntp server 192.168.2.2
DeviceB(config)# access-list 1 permit host 192.168.2.2
DeviceB(config)# ntp access-group serve-only 1
```

Configure device A as the NTP server, limit the request packet interval of the client, and send KoD packets.

```
DeviceA(config)# ip access-list standard limited1
DeviceA(config-std-nacl)# 10 permit any
DeviceA(config)# exit
DeviceA(config)# ntp access-group limited limited1 kod
DeviceA(config)# ntp discard min-spacing 5 avg-spacing 5
DeviceA(config)# ntp master
```

4. Verification

Run the **ping** command to verify L3 reachability between device B and device A.

```
DeviceB# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **clock set** command to modify the time on device A.

```
DeviceA# clock set 11:00:00
Set system clock: 11:00:00 UTC Fri, Feb 26, 2021
```

Run the **show clock** command on device B to check whether time synchronization is successful.

```
DeviceB# show clock
11:00:01 UTC Fri, Feb 26, 2021
```

5. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
ip access-list standard limited1
 10 permit any
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
ntp master
ntp access-group limited limited1 kod
!
end
```

- Device B configuration file

```
hostname DeviceB
!
ip access-list standard 1
 10 permit 192.168.2.2
!
ntp server 192.168.2.2
ntp access-group serve-only 1
!
interface GigabitEthernet 0/1
 ip address 192.168.2.1 255.255.255.0
!
end
```