

14 Clock and Time

[14.1 Clock and Time Feature Updates](#)

[14.2 Clock and Time Overview](#)

[14.3 Physical Layer Clock/Time Synchronization](#)

This section describes the definition and principle of the physical clock and time system of the Access devices, and describes the specific applications of physical clock and time synchronization.

[14.4 1588v2 \(based on IEEE\)](#)

The IEEE organization proposed the IEEE 1588v2 precision time synchronization protocol, which supports system-wide synchronization accuracy within the sub-microsecond range. In contrast to the GPS solution, the IEEE 1588v2 solution achieves the same time precision but has advantages in terms of cost, maintenance, and security. It has become the most popular time synchronization protocol in the industry.

[14.5 1588v2 \(Based on G.8275.1\)](#)

G.8275.1 defines precision time protocol telecom profile for phase/time synchronization with full timing support from the network based on the IEEE 1588v2 precision time synchronization protocol.

[14.6 1588 ACR](#)

1588 Adaptive Clock Recover (ACR) enables a master device that supports IEEE 1588v2 to encapsulate the local system clock information into 1588v2 packets and transparently send them to peer slave devices through a third-party network. The slave devices obtain the timestamp from the 1588v2 packets and restore the clock to implement frequency synchronization between devices at both ends of a packet switched network (PSN).

[14.7 NTP](#)

The Network Time Protocol (NTP) is used to synchronize the time between the distributed time server and the client.

14.1 Clock and Time Feature Updates

Version	Change Description
V100R019C10	Unified version release is implemented since V100R019C10.

14.2 Clock and Time Overview

14.2.1 Network Synchronization Requirements

Definition

IP-nization is the trend of future network and service development. Difficulties, however, currently exist in the transition from the SDH-based traditional network to the IP-based Ethernet bearer network. One key technology involved is how to bear traditional TDM service on the new network. Traditional TDM service has two major applications: voice service and clock synchronization service.

In a traditional communications network architecture, the TDM service of the fixed network is mainly voice service. Cumulative inconsistency between the clocks at both ends of the bearer network over a long time causes bit slip. The ITU-T Recommendation G.823 defines the requirements on and the test standards of the TDM service of the fixed network. The definition is called the G.823 traffic interface standard. Apart from the bearer network, a traditional communications network usually contains an independent clock-issuing network, which adopts PDH/SDH for issuing clock signals. As specified by the ITU-T, the clock must meet the G.823 Synchronization interface requirements.

In a communications network, the wireless application has the most rigorous requirements on the clock frequency. The frequencies of different BTSs must be synchronized within specified precision. Otherwise, re-synchronization occurs during the BTS switching. Current wireless technologies are in different systems. Different systems have different requirements on the clock bearing. European systems, of which the GSM/WCDMA is a representative, adopt the asynchronous base station technologies. In this case, only frequency synchronization is required, at a precision of 0.05 ppm (or 50 ppb). The clock needs to be provided by the bearer network. The traditional solution is to provide the clock through PDH/SDH. After the IP-nization, the clock needs to be provided by the IP network. The synchronous BTS technologies, of which the CDMA/CDMA2000/TD-SCDMA are representatives, require phase synchronization of the clock (also called time synchronization). [Table 14-1](#) lists the detailed requirements on clocks.

NOTE

Clock synchronization is frequency synchronization.

Time synchronization is phase synchronization, which requires both phase synchronization and frequency synchronization at the same time.

Table 14-1 Requirements of different standards on the clock and time

Wireless System	Frequency Precision	Phase Synchronization Precision
GSM	0.05 ppm	N/A
WCDMA	0.05 ppm	N/A
TD-SCDMA	0.05 ppm	± 1.5 us
CDMA2000	0.05 ppm	± 3 us
WiMax FDD	0.05 ppm	N/A
WiMax TDD	0.05 ppm	± 0.5 us
LTE TDD	0.05 ppm	± 1.5 us

Purpose

The purpose is to ensure the clock and time synchronization between communications devices and communications networks.

14.2.2 Synchronization Overview

Synchronization is classified into clock synchronization and time synchronization. Clock synchronization is also called frequency synchronization, and time synchronization is also called phase synchronization.

The synchronization methods are used depending on system types. For SDH networks, frequency synchronization is used, requiring that NEs on the network synchronize their frequencies to ensure normal transmission of SDH services. Wireless stations form a time synchronization system, requiring time synchronization between neighboring stations to ensure switching among stations.

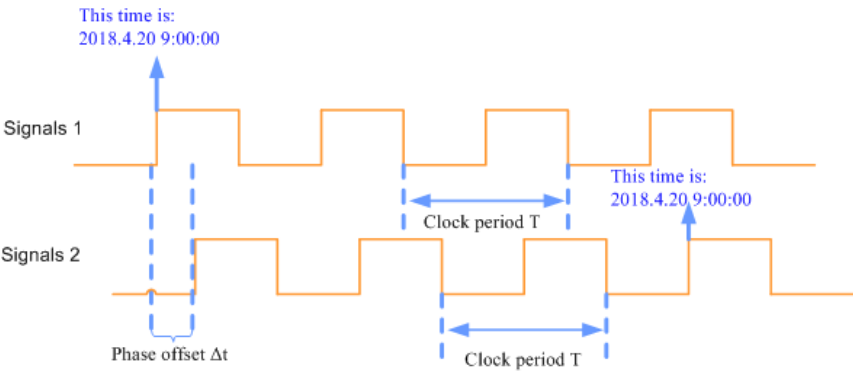
Clock Synchronization

Clock synchronization, also called frequency synchronization, means that signals maintain a specific relationship in frequency or phase. Significant instants of a clock signal occur at the same rate to ensure that equipment in the entire communication network runs at the same rate. In other words, signals maintain a constant phase offset.

Figure 14-1 shows two clocks that synchronize their frequencies to each other. The relationship between the two clocks is summarized as follows:

- The two clocks have the same clock frequency (their clock periods T_s are the same).
- The clock pulses of the two clocks may have different phases (the phase difference is not 0).

Figure 14-1 Frequency synchronization



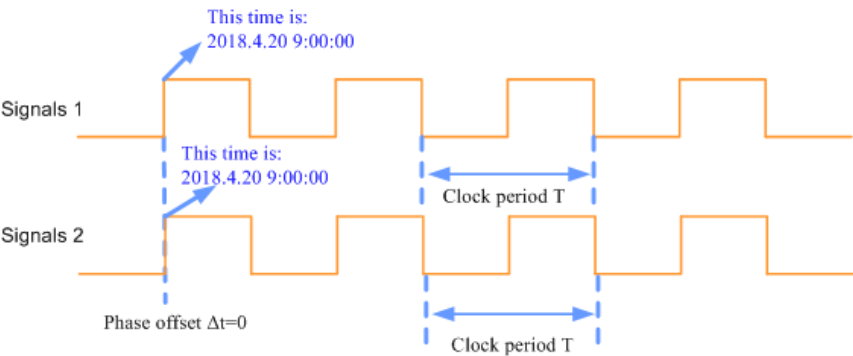
Time Synchronization

Time synchronization, also called phase synchronization, means that signals have the same frequency and phase. That is, there is no phase offset between signals.

Figure 14-2 shows two clocks that synchronize their phases to each other. The relationship between the two clocks is summarized as follows:

- The two clocks have the same clock frequency (their clock periods T_s are the same).
- Clock pulses of the two clocks have the same phase (the phase difference is 0).

Figure 14-2 Phase synchronization



14.2.3 Clock Synchronization

Table 14-2 Comparison between clock synchronization solutions

Clock Source	Description	Remarks
2 MHz or 2 Mbit/s BITS clock	Traces a BITS input clock source and supports 2.048 Mbit/s bitstream (HDB3) or 2.048 MHz clock signal input.	This solution features high deployment costs because each CO requires a BITS device.

Clock Source	Description	Remarks
Synchronous Ethernet	Synchronous Ethernet uses Ethernet bitstreams to recover clock signals for Ethernet clock synchronization. The implementation mode is similar to that on an SDH or PDH network. The device uses high-precision clock signals as the transit reference in the transmit direction. It recovers and extracts the clock signals at the receive end. The physical layer transmits and receives the clock signals and is compatible with traditional networks. The OLT traces the clock source recovered from GE or 10GE lines. It can also use the clock recovered from line bitstreams as the system clock source.	This solution requires bearer networks to support synchronous Ethernet.
1588v2	The IEEE organization proposed the IEEE1588 V2 precision time synchronization protocol, which supports system-wide synchronization accuracy within the sub-microsecond range. In contrast to the GPS solution, the IEEE1588 V2 solution achieves the same time precision but has advantages in terms of cost, maintenance, and security. It has become the most popular time synchronization protocol in the industry.	This solution requires bearer networks to support IEEE1588 V2 at each hop and applies in mobile bearing scenarios that require time synchronization, such as CDMA2000, TD-SCDMA, and LTE.

Clock Source	Description	Remarks
1588 adaptive clock recovery (ACR)	In 1588 ACR, a master device supporting IEEE1588 V2 encapsulates the local system clock data into 1588 V2 packets. The PSN network transparently transmits the 1588 V2 packets to a peer slave device. The slave device obtains timestamps from the received 1588 V2 packets and recovers the clock data to synchronize its frequency with the master device. In the 1588 ACR solution, the PSN network does not need to support clock synchronization or the clock of the PSN network can be a third-party clock, and clock packets are transparently transmitted as service packets.	- Provides E2E clock synchronization and is simple in deployment, meeting clock frequency requirements of MSAN and wireless networks. - Promotes packet delay variation (PDV) requirements on intermediate networks.
PON line clock	Traces the clock source recovered from PON lines and can also use the clock recovered from line bitstreams as the system clock source.	None

14.2.4 Time Synchronization

Figure 14-3 Time synchronization solutions

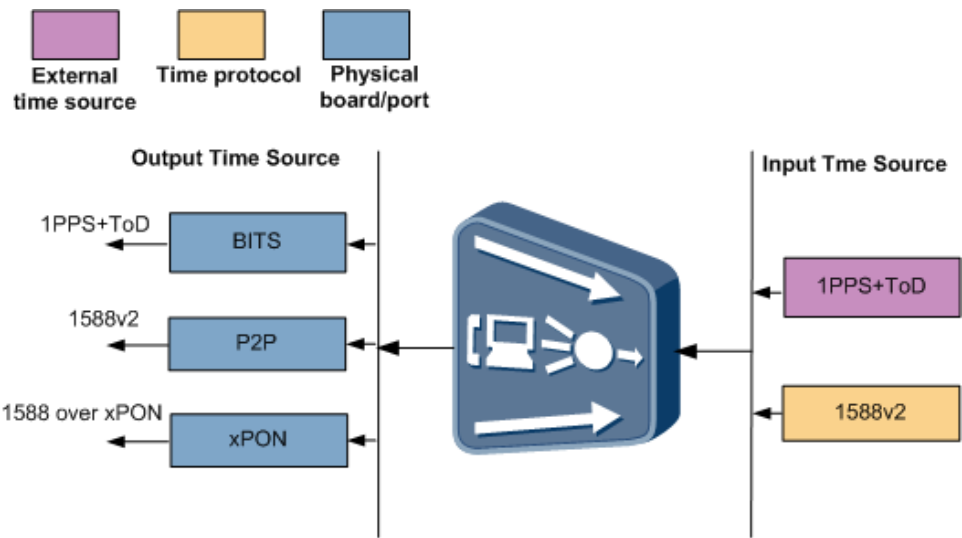


Table 14-3 Comparison between time synchronization solutions

Time Source	Description	Remarks	Time Input	Time Output
1 PPS +TOD	Traces the input time source and supports 1 PPS+TOD time synchronization.	In some mobile bearing scenarios, some intermediate devices do not support time transfer. Therefore, the 1 PPS+TOD time must be sent to the OLT/MDU and the device uses the 1 PPS+TOD time as the system time source. This solution features high deployment costs because each CO requires BITS and GPS devices.	Yes	Yes
1588v2 (based on IEEE)	The IEEE organization proposed the IEEE1588 V2 precision time synchronization protocol, which supports system-wide synchronization accuracy within the sub-microsecond range. In contrast to the GPS solution, the IEEE1588 V2 solution achieves the same time precision but has advantages in terms of cost, maintenance, and security. It has become the most popular time synchronization protocol in the industry.	This solution requires bearer networks to support 1588v2 at each hop and applies in mobile bearing scenarios that require time synchronization, such as CDMA2000, TD-SCDMA, and LTE.	Yes	• 1588v2 over PON • 1588v2 over GE

Time Source	Description	Remarks	Time Input	Time Output
1588v2 (based on G.8275.1)	G.8275.1 defines precision time protocol telecom profile for phase/time synchronization with full timing support from the network based on the IEEE 1588v2 precision time synchronization protocol.	This solution requires bearer networks to support G.8275.1 hop by hop and applies in mobile bearing scenarios that require time synchronization, such as CDMA2000, TD-SCDMA, and LTE.	Y	1588v2 over PON 1588v2 over GE/10GE

14.3 Physical Layer Clock/Time Synchronization

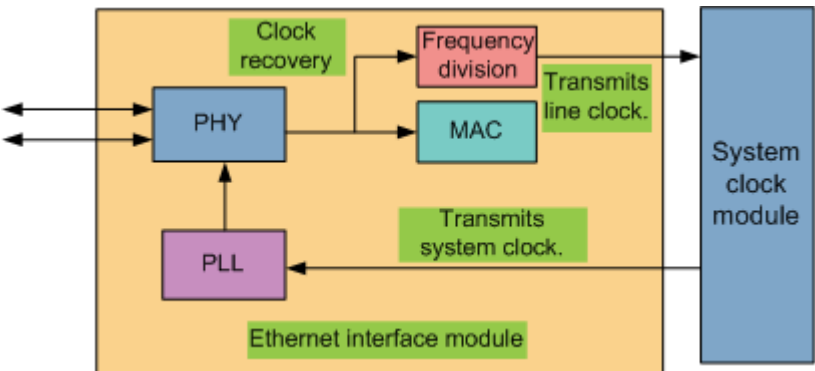
This section describes the definition and principle of the physical clock and time system of the Access devices, and describes the specific applications of physical clock and time synchronization.

14.3.1 Physical Layer Clock/Time Synchronization Principles

14.3.1.1 Synchronous Ethernet

Synchronous Ethernet, similar to traditional SDH synchronization, is a synchronization technology that uses physical-layer bitstreams to carry frequency information and recovers frequency information also from physical-layer bitstreams. Synchronous Ethernet enables the device to extract clock signals from serial bitstreams on an Ethernet line, select a better clock source, and finally send the clock signals (line clock) to a system clock phase-locked loop (PLL). The PLL then traces the clock signals and generates a system clock and uses the system clock as the transmit clock at the Ethernet physical layer to transmit clock data to lower-layer devices.

Figure 14-4 Synchronous Ethernet clock signal processing



- Ethernet interface receive clock:
 - The PHY chip in the Ethernet interface module recovers a clock from Ethernet line bitstreams, divides the frequency of the clock, and sends the clock to the system clock module.
 - The system clock module selects the clock source with the highest precision based on clock source priorities and sends the clock source to the system PLL as the system reference clock. Then, the PLL traces the reference clock and outputs a high-precision clock for each interface.
- Ethernet interface transmit clock:
 - The system clock module sends a high-precision clock to Ethernet interfaces on NEs.
 - The PLL of the Ethernet interface module traces the high-precision clock sent from the system clock module, generates a reference clock for the Ethernet link bitstreams, and sends the reference clock out using Ethernet link bitstreams.

Performance and Deployment Limitations

A synchronous Ethernet clock is simple to implement. The mechanism for transferring the clock in synchronous Ethernet is simple to implement and the recovered clock is reliable in compliance with ITU-T G.823 with respect to the synchronization interface specifications.

Similar to an SDH network, a synchronous Ethernet network has limitations on deployment. For the synchronous Ethernet network, the clock is transferred over links. All nodes on the clock trail must have the synchronous Ethernet feature to achieve clock synchronization (only frequency synchronization) of the entire network.

Synchronous Ethernet can work with IEEE 1588v2 clocks for time synchronization.

14.3.1.2 External Time Source

A time source is a signal source containing reference timing information. Each NE synchronizes its local clock phase to the reference timing using its phase-locked loop (PLL). In this manner, time synchronization is implemented on the entire network.

A time source can be from an external time source or a line time source.

In some mobile carrying scenarios, 1PPS+TOD time signals must be injected to an OLT or an MDU because intermediate devices do not support transmission of these signals. Then the signals are used as the system time source.

The 1PPS+TOD protocol receives signals using a solution similar to time signal reception using a GPS satellite. This protocol transmits two types of signals: 1PPS and TOD signals. Frame headers and time information are transmitted over dual lines.

1PPS+TOD time signals consist of 1PPS signals and TOD time information.

- 1PPS
1PPS is short for one pulse per second. 1PPS signals are used for time scaling and work at the RS-422 levels. The pulse frequency of 1PPS is 1 Hz. That is,

one pulse is transmitted per second. The 1PPS signal pulse width ranges from 20 ms to 200 ms. On the rising edge of the pulse, UTC time signals are aligned.

- **TOD**
TOD is short for time of day. TOD messages provide time in ASCII format. TOD signals also work at the RS-422 or RS-232 levels and provide a baud rate of 9600 bit/s. A TOD message contains information such as current date/time, time standard ID, 1PPS status flag, date/time adjusted based on UTC leap seconds, leap second adjustment directive, and GPS time.

TOD can be in UBX or NMEA format.

Table 14-4 TOD Format

TOD Format	Description
can be in UBX	a private format of the Ublox company. The UBX format is in binary code and identified by a length domain because it does not contain a start or end character.
NMEA	a set of communication protocol formulated by the National Marine Electronics Association to standardize various global positioning system (GPS) navigators. The NMEA protocol is in ASCII format and identified by start and end characters. A comma (,) is used to separate domains.

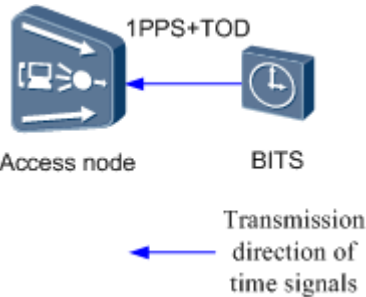
 NOTE

The OLT supports only the UBX format.

As shown in [Figure 14-5](#), the OLT or MDU can function as an access node to receive 1PPS+TOD clock signals.

- When the OLT functions as the access node, it receives 1PPS+TOD clock signals using the BITS/TOD port as the clock source.
- When the MDU functions as the access node, it receives 1PPS+TOD clock signals using the clock/time output port BITS/TOD port as the clock source.

Figure 14-5 External time source synchronization



14.3.1.3 Clock Mode

This topic describes the three clock modes supported: Locked mode, Holdover mode and Free-run mode.

Locked Mode

In this mode, the system clock source is synchronized with the input clock source. The phases of the system clock source and the input clock source are in a constant relationship. The device traces the BITS clock source, upstream Ethernet synchronous clock, line clock source, Auto-adaptation recovery clock, or IEEE1588 V2 message recovered clock source. The ideal clock source can meet the 50 ppb requirements of mobile backhaul.

Holdover Mode

The device records the clock data of the trace mode. If the clock source is lost, the system builds a system clock by using the recorded clock data, and maintains the clock properties as consistent as possible with the clock properties in the trace mode. As such, the system enters and remains in the holdover mode. The precision of the holdover mode meets the G.813 or G.8262 requirements.

NOTE

The system supports the holdover mode only when configured with the stratum-3 clock daughter board.

Free-Run Mode

In this mode, the device works based on the inherent frequency of the internal crystal oscillator inside the device.

14.3.1.4 Clock Source Selection

The device uses a clock source selection algorithm to select a clock source as its reference clock. It supports the clock source selection algorithm based on clock source priorities or synchronization status messages (SSMs).

Clock Source Priority-based Clock Source Selection

If uses the clock source priority-based clock source selection algorithm to select a clock source, users need to configure the external clock sources with different priorities. The OLT/MDU then automatically selects the clock source that has the highest priority and is running properly as its reference clock. When the traced clock source becomes faulty, the device automatically selects the clock source that has the second highest priority and is running properly as its reference clock.

SSM-based Clock Source Selection

SSM messages are used for transporting clock signal quality levels over clock links. By reading data carried in the SSM messages, the node clocks on SDH and synchronization networks obtain the information of the upper-layer clocks, perform operations based on instructions carried in the SSM messages, such as

tracing a clock, switching a clock source, or entering the holdover state, and send the clock synchronization information of the node clocks to lower-layer clocks.

The following table lists ITU-T G.781-compliant SSM quality levels.

Quality Level	SSM Code	Code Value	Description
QL-PRC	0010	0x02	Indicates that the timing quality generated by a primary reference clock defined in Recommendation G.811 is transported.
QL-SSU-A	0100	0x04	Indicates that the timing quality generated by a type I or V (transit exchange) slave clock defined in Recommendation G.812 is transported.
QL-SSU-B	1000	0x08	Indicates that the timing quality generated by a type VI (local exchange) slave clock defined in Recommendation G.812 is transported.
QL-SEC	1011	0x0b	Indicates that the timing quality generated by an SDH equipment clock (SEC) defined in Recommendation G.813 is transported.
QL-DNU	1111	0x0f	Indicates that the clock source is not used for synchronization.

If the SSM-based clock source selection algorithm is used, the device extracts the quality level from clock source input signals. If the clock source does not support SSM information extraction, users must manually configure the quality level. The device automatically selects the clock source that has the highest quality level and is running properly as its reference clock. Ensure that the quality level is higher than or equal to the lowest SSM level of the clock source.

- If there are two external clock sources with the same highest quality level, the device selects the one that has a higher clock source priority.
- If the clock source traced by the OLT/MDU becomes faulty, the OLT/MDU automatically selects the clock source that has the second highest quality level and is running properly as its reference clock.

In SSM-based clock source selection mode, SSM quality levels of clock sources are used for selecting a clock source. The SSM quality levels of clock sources can be obtained in either of the following modes:

- Users configure the SSM quality levels of clock sources. In this mode, all clock source ports support SSM quality level configurations. For the clock source ports that support the extraction of SSM quality levels, users can also

configure SSM quality levels for the clock source ports as the SSM quality levels of these clock sources.

- The device extracts SSM information, from lines. Not all boards support the extraction of SSM information from lines. For details, see section **Feature Dependencies and Limitations**.

The device uses Ethernet (SSM), E1, , or PON ports to transport clock quality levels to lower-layer devices.

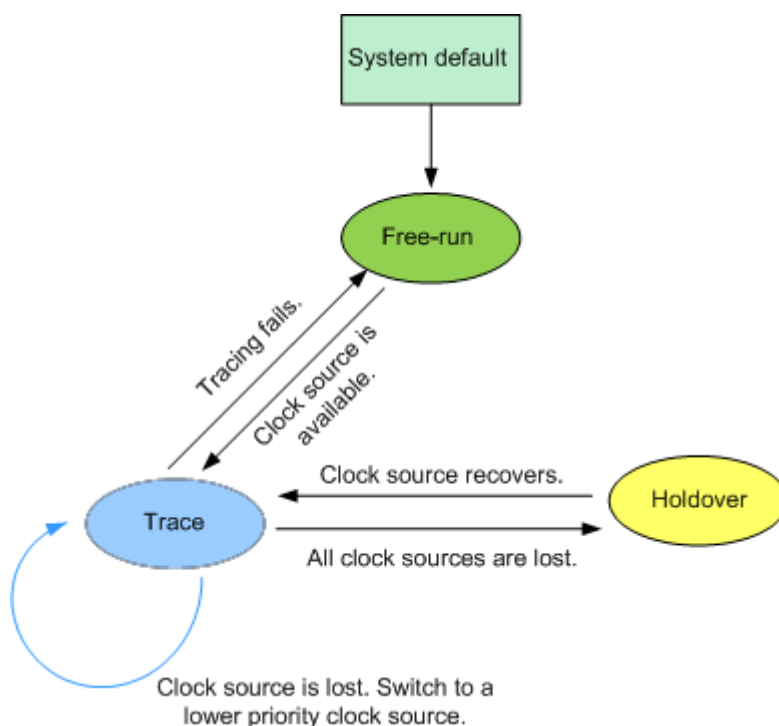
- E1 (2 Mbit/s) ports use four idle bits in the TS0 timeslot to transport quality levels.
- Ethernet clock synchronization ports use ESMC packets to transport quality levels.

The device enters holdover if no clock source is available, regardless of whether the clock source selection algorithm is based on clock source priorities or SSM messages. In holdover mode, the device uses the data recorded in tracing mode to control the clock unit so that the clock unit generates clock properties similar to those of the clock in tracing mode.

- If clock recovery is enabled, the device returns to the tracing mode from the holdover mode when a clock source recovers.
- If the clock recovery mode is disabled, the device does not return to the tracing mode no matter whether a clock source recovers in the holdover period.
- If the device restarts during the holdover period, the system enters the free-run mode.

Figure 14-6 shows the clock source status transition.

Figure 14-6 Clock source status transition

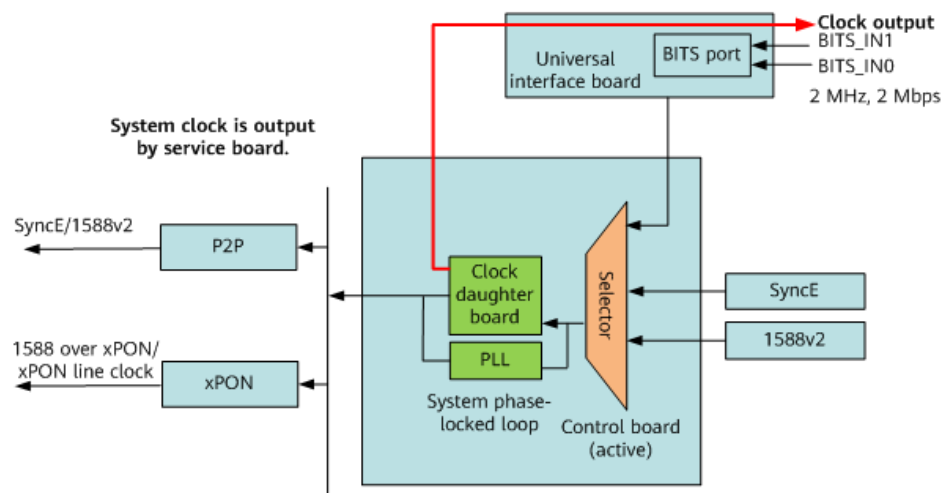


14.3.2 Physical Layer Clock/Time Synchronization Usage Scenarios

14.3.2.1 Applications of Clock Output

By specific configuration, the OLT can select a system clock output. The output clock can serve as the clock source for other devices, as shown in [Figure 14-7](#).

Figure 14-7 Clock output



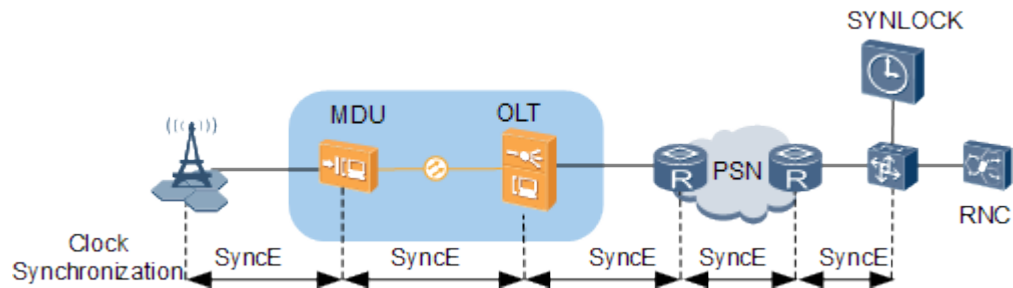
When the system clock is selected as the output clock, the clock output through the universal interface board port is the system clock phase-locked by the MA5800.

The following clock sources can serve as the system clock:

- BITS clock source: including 2 Mb/s and 2 MHz signals.
- Synchronous Ethernet line clock
- IEEE1588 V2 clock source
- Free-running internal clock source

14.3.2.2 Clock Synchronization of the Synchronous Ethernet Service

Traditional Ethernet application does not consider the synchronization requirement. The Ethernet ports adopt the ± 100 ppm local oscillator as the transmit clock, and the transmit clocks of the NEs are independent of each other. As such, the clocks are not precise enough. Synchronous Ethernet is a technology that recovers the clock from the bit streams on the Ethernet link and implements synchronization between Ethernet networks. The implementation mode is similar to the synchronization mode on the SDH/PDH network. In the transmit direction, the high-precision system clock is adopted as the transmit clock, which is recovered and obtained at the receive end. The transmission and reception are performed by the physical layer independently, which in terms of function is compatible with traditional Ethernet.

Figure 14-8 Clock synchronization for the synchronous Ethernet service

14.3.3 Configuring the Physical Clock

On a digital network comprising the access device and other devices, the primary problem to be solved is clock synchronization for carrying the traditional TDM service. To ensure the system clock synchronization of each device in the digital network, a system clock source must be specified.

Context

IP-based solution is the trend of future network and service development, so is the trend of the bearer network. Difficulties, however, currently exist in the transition from the SDH-based traditional network to the IP-based Ethernet bearer network. One key technology involved is how to carry traditional TDM service on the new network. Traditional TDM service has two major applications: voice service and clock synchronization service. In a traditional communications network architecture, the TDM service of the fixed network is mainly voice service. Cumulative inconsistency between the clocks at both ends of the bearer network over a long time causes frame slip. On a communications network, the wireless application has the most rigorous requirements on the clock frequency. The frequencies of different base stations must be synchronized within a specified precision. Otherwise, re-sync occurs during the base station switching.

To ensure clock synchronization among devices, relevant clock synchronization methods are adopted based on the clock source solution provided by an upper-layer device.

14.3.3.1 Configuring the System Clock Based on the Priority

If a device has multiple clock sources and the precision of the clock sources is provided, you need to configure the priorities of the clock sources. Generally, the higher the precision is, the higher the priority is.

Context

A clock source can be an external BITS clock or a line clock from the upper-layer node. The clock module automatically judges the types of the specified clock sources (BITS, TDM), and sends them according to their priorities to the clock module, serving as clock sources for phase lock.

Procedure

Step 1 Run the **clock source sourceid** command to configure the system clock source.

Specify the clock signals extracted from a certain port as the system clock source.

- The system supports 10 clock sources in total.
- Only the external clock sources on the physical entities are added by running this command and the external clock sources are numbered. To enable the relevant external clock source, you need to run the **clock priority system** command to determine whether the relevant clock source is available.
- The system clock cannot serve as the system clock source.

Step 2 Run the **clock priority system** command to configure the priority of the system clock source.

- The system supports 10 clock source priorities. The highest priority is p0 and the lowest priority is p9.
- When the clock source is selected based on the priority, the system does not check the quality of the clock source. Therefore, you must configure the clock source of high quality with a high priority.
- After the priority of the clock source is configured, the system selects the clock source with the highest priority and in the normal state as the system clock source.
- When the clock source with the highest priority is faulty, the system automatically switches to the clock source with the second highest priority.
- When the clock source with the highest priority recovers, the system switches back to this clock source.

----End

Example

Assume the following configurations: The device obtains three clock sources from a BITS port on the universal interface board and ports 0/2/0 and 0/2/1 on the upstream interface board as clock source 0, clock source 1, and clock source 2 of the system. Configure clock source 0 with the highest priority and configure clock source 2 with the lowest priority. To perform the preceding configurations, do as follows:

```
huawei(config)#clock source 0 0/0/0 2MHz 120ohm
huawei(config)#clock source 1 0/2/0
huawei(config)#clock source 2 0/2/1
huawei(config)#clock priority system 0/1/2
```

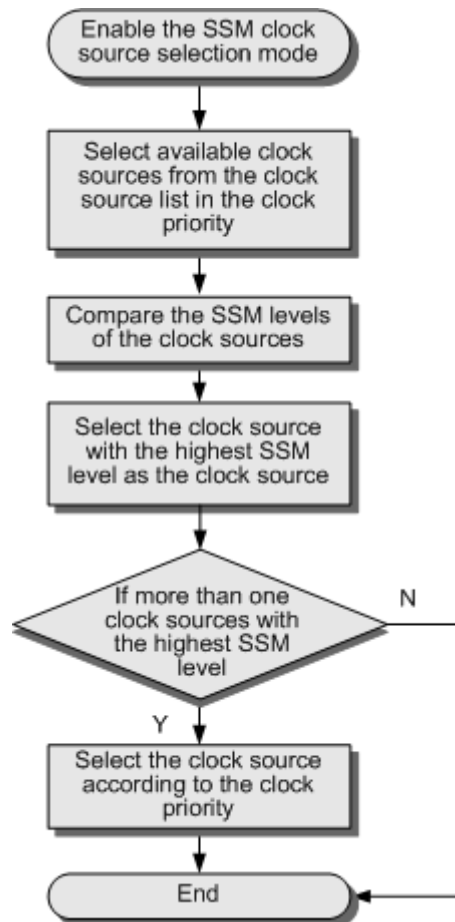
14.3.3.2 Configuring the System Clock Based on the SSM Clock Source Selection Mode

If the clock transmitted from an upper-layer device contains a synchronization status message (SSM) and all clock sources are selected based on the SSM, you need to configure the system clock based on the SSM clock source selection mode.

Context

By default, the SSM clock source selection mode is disabled. That is, the system selects the clock source based on the priority. The system enables the SSM clock source selection mode only after the system determines that the clock source contains an SSM and the entire system are based on the SSM clock source selection mode.

For the detailed SSM clock source selection process, see the following flowchart.



Procedure

- Step 1** Enable the SSM clock source selection mode.
Run the **clock ql-mode enable** command to enable the SSM clock source selection mode.
- Step 2** Run the **clock source** command to configure the system clock source.
- Step 3** Run the **clock priority** command to configure the clock source range based on the SSM clock source selection mode and the priority sequence of the corresponding clock sources if the SSM quality levels are the same.
- Step 4** (Optional) Run the **clock ql sourceid clock-ql** command to configure the SSM quality level for the clock source. If the SSM clock source selection mode is enabled, but a clock source does not support the output of an SSM, you need to

manually configure the SSM quality level for the clock source. After the SSM quality level is configured, the device no longer matches the received SSM.

 NOTE

- When the SSM clock source selection mode of the system is disabled, the SSM quality level of the clock source cannot be set.
- When the system selects the clock source based on the SSM quality level, the system selects the clock sources based on the priority and then compares the SSM of the clock sources. Finally, the system selects the clock source with the highest SSM quality level as the system clock source. If there are multiple clock sources with the same SSM quality level, the system selects the clock source based on the priority.

Step 5 (Optional) Run the **clock ql input lower-limit** command to configure the lowest synchronization status message (SSM) quality level threshold of the clock source. When the SSM quality level of the clock source of the upper-layer device is greater than or equal to that of the device, the clock of the upper-layer device is traced. Otherwise, the clock of the device is in the holdover state and switched to the free-run state after 24 hours elapses.

Step 6 (Optional) Run the **clock ql output** command to configure whether the specified port sends the SSM quality level.

----End

Example

Example 1:

Configure the SSM clock source selection mode as the system clock source selection mode. Configure the three clock sources obtained from upstream ports **0/9/0** and **0/9/1** on the control board and port **0/2/0** on the upstream board as clock source 0, clock source 1, and clock source 2 with SSM respectively. Configure clock source 0 with the highest priority and clock source 2 with the lowest priority and set the lower threshold to QL-SSU-B for received clock sources. To perform the preceding configurations, do as follows:

```
huawei(config)#clock ql-mode enable
huawei(config)#clock source 0 0/9/0
huawei(config)#clock source 1 0/9/1
huawei(config)#clock source 2 0/2/0
huawei(config)#clock priority system 0/1/2
huawei(config)#clock ql input lower-limit QL-SSU-B
```

Example 2:

Configure the SSM clock source selection mode as the system clock source selection mode. Configure the clock sources obtained from upstream ports **0/9/0** and **0/9/1** on the control board as clock source 0 and clock source 1 with SSM respectively; and the clock source obtained from port **0/0/0** (that does not support SSM) on the universal interface board as clock source 2. Configure clock source 0 with the highest priority and clock source 2 with the lowest priority.

Manually set the SSM quality level to QL-SSU-A for clock source 2 (port **0/0/0**) that does not support SSM and set the lowest threshold for the received clock source to QL-SSU-B.

Send SSM from port **0/3/1**. To perform the preceding configurations, do as follows:

```
huawei(config)#clock ql-mode enable
huawei(config)#clock source 0 0/9/0
```

```
huawei(config)#clock source 1 0/9/1
huawei(config)#clock source 2 0/0/0 2MHz 120ohm
huawei(config)#clock ql 2 QL-SSU-A
huawei(config)#clock priority system 0/1/2
huawei(config)#clock ql input lower-limit QL-SSU-B
huawei(config)#clock ql output 0/3/1 enable
```

14.3.3.3 Configuring External Clock

The device can select a system clock output or export the line clock as the clock source of another device.

Context

The external clock output supports the selection of the following two benchmark clocks.

- Select the system clock as the output benchmark clock.
- Select the line clock as the output benchmark clock.

Procedure

Step 1 Run the **clock external bits-type** command to set the signal type of the BITS port.

NOTE

The system defaults to 2 Mbit/s.

Step 2 Configuring the clock source of the external clock

1. Run the **clock source sourceid** command to configure the clock sources of the external clock.

Step 3 Run the **clock priority systemian** command to configure the priority of the system clock source.

- The system supports 10 clock source priorities. The highest priority is p0 and the lowest priority is p9.
- When the clock source is selected based on the priority, the system does not check the quality of the clock source. Therefore, you must configure the clock source of high quality with a high priority.
- After the priority of the clock source is configured, the system selects the clock source with the highest priority and in the normal state as the system clock source.
- When the clock source with the highest priority is faulty, the system automatically switches to the clock source with the second highest priority.
- When the clock source with the highest priority recovers, the system switches back to this clock source.

----End

Example

Assume the following configurations: Configure the SyncE clock sources obtained from port 0 on the control board in slot **0/9** and port 0 on the upstream interface board in slot 0/2 as clock source 1 and clock source 2 of the system respectively. Configure clock source 1 with a higher priority than clock source 2, and configure

the system clock as the output clock. To perform the preceding configurations, do as follows:

```
huawei(config)#clock source 1 0/9/0
huawei(config)#clock source 2 0/2/0
huawei(config)#clock priority system 1/2
```

14.3.4 Physical Layer Clock/Time Synchronization Standards and Protocols Compliance

The following lists the reference standards and protocols of this feature:

- ITU-T G.823 (the control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy)
The ITU-T G.823 describes the jitter and wander of the PDH interface in the 2048 kbit/s synchronous system. Here, the E1 port is mainly referred to, which meets the G.824 requirements for the 1544 kbit/s system. G.823 defines the requirements on the traffic interface and the synchronization interface. The traffic interface performance is the basic requirement for service transmission. To transmit synchronous clock signals, the E1 port must meet the requirements of the synchronization interface. The synchronization interface has stricter requirements on jitter and wander than the traffic interface does.
 - The G.823 defines the following items for the traffic interface and the synchronization interface:
 - Jitter output
 - Output wander
 - Input jitter and wander tolerance
- ITU-T G.825, The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)
The ITU-T G.825 defines the jitter and wander characteristics of SDH devices.
 - The ITU-T G.825 defines the following items for the STM port:
 - Jitter output
 - Output wander
 - Input wander tolerance
 - Input jitter tolerance
 - Jitter and wander generation
 - Jitter and wander transfer
- ITU-T G.8261, Timing and Synchronization Aspects in Packet Networks
The ITU-T G.8261 defines the wander budget of CES and synchronous Ethernet for packet networks. The ITU-T G.8261 requirements are similar to the requirements of the ITU-T G.823 on the TDM network. The CESoP service and synchronous Ethernet clock feature of the MA5800 need to meet the ITU-T G.8261 requirements.
- ITU-T G.8262, Timing characteristics of synchronous Ethernet equipment slave clock (EEC)

The ITU-T G.8262 defines the requirements on the synchronous Ethernet clock system, which are equal to the G.813 and G.812 requirements on the TDM network. To meet the ITU-T G.8262 specifications, the MA5800 must be configured with the stratum-3 clock daughter board.

- ITU-T G.8264, Distribution of timing through packet networks

The ITU-T Recommendation G.8264 defines the SSM protocol and message format for the synchronous Ethernet to ensure clock synchronization between Ethernet devices.

14.4 1588v2 (based on IEEE)

The IEEE organization proposed the IEEE 1588v2 precision time synchronization protocol, which supports system-wide synchronization accuracy within the sub-microsecond range. In contrast to the GPS solution, the IEEE 1588v2 solution achieves the same time precision but has advantages in terms of cost, maintenance, and security. It has become the most popular time synchronization protocol in the industry.

14.4.1 Why Is 1588v2 Required

Background

1. Traditionally, time synchronization chains use the NTP, which can only ensure time precision within milliseconds. This precision is far below the time synchronization precision of microseconds required by wireless base stations.
2. On the base station side, GPS can be used to solve frequency and time synchronization problems. However, GPS has many problems, such as difficult site selection, high fault rate, difficult maintenance, difficult feeder routing, high security risks, and high costs.
3. To meet the high time precision requirement of wireless synchronization base stations and solve the disadvantages of the existing GPS solution, a high precision time synchronization solution for terrestrial transmission is urgently needed.

IEEE 1588v2 high-precision Time Transfer Protocol

Based on the synchronization requirements for different wireless systems and time synchronization condition, IEEE defines IEEE 1588v2 high-precision time protocol (full name: Precision Clock Synchronization Protocol for Networked Measurement and Control Systems and abbreviation: PTP). The protocol supports time synchronization precision in the sub-microsecond range.

In contrast to the GPS solution, IEEE 1588v2 solution achieves the same time precision but has advantages in terms of cost, maintenance, and security. It has become the most popular time transfer protocol in the industry because of the following advantages:

1. Space localization: The IEEE 1588v2 protocol is applicable to local area networks supporting multicast messaging including but not limited to Ethernet.

2. Low cost: The IEEE 1588v2 protocol helps minimize the demand for network resources and CPU resources and therefore enables low-cost applications.
3. Network transformation trend: IP networks are transformed to future—oriented convergence networks.

14.4.2 1588v2 Basic Concepts

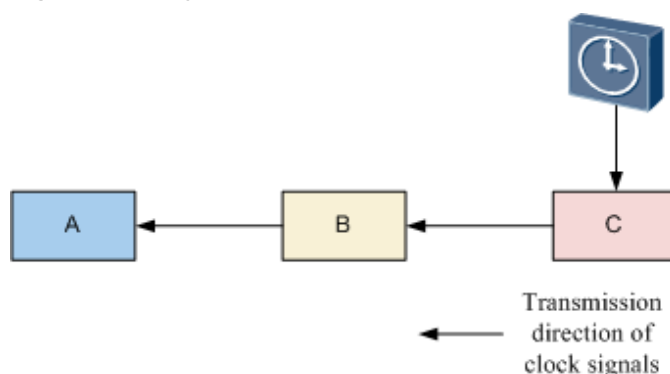
14.4.2.1 Device Model

When a pair of nodes performs time synchronization, the upstream node distributing the reference time signals is the master node and the downstream node receiving the reference time signals is the slave node. As shown in [Figure 14-9](#), B is the master node, and A is the slave node.

In the subnet system, grand master is the master clock. Each system has only one grandmaster clock (GMC), and each subnet has only one master clock. Slave clocks are kept synchronized with the master clock.

As shown in [Figure 14-9](#), C is the grand master, and nodes A and B must be synchronized with C.

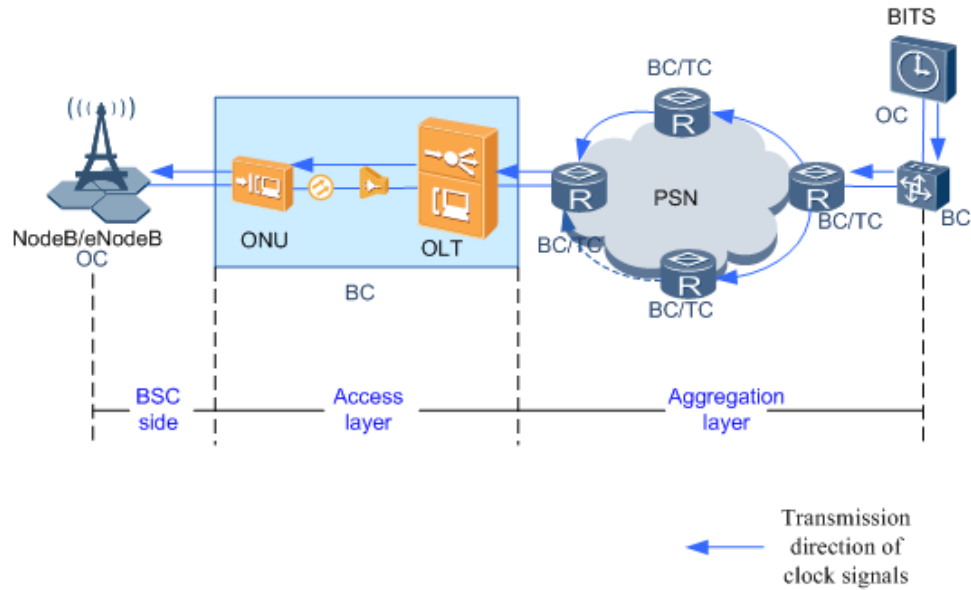
Figure 14-9 Synchronization on devices



1588v2 Device Model

The IEEE 1588v2 standard defines five network node models: ordinary clock (OC), boundary clock (BC), end-to-end transparent clock (E2E TC), peer-to-peer transparent clock (P2P TC), and management node.

Figure 14-10 Device model



OC

An OC has only one 1588v2 clock interface (a clock interface enabled with 1588v2) through which the OC synchronizes with an upstream node or distributes time signals to downstream nodes. An OC has only one physical port. Therefore, in practice, an OC can either be a grandmaster (GM) clock or a slave lock.

As shown in [Figure 14-10](#), BITS is generally configured as an OC, functioning as the GM clock in the entire network; a basic station, as a slave device, is also configured as an OC.

BC

A BC has several physical ports for network communication. Each port is similar to the port of an OC, which is used to connect multiple domains. One of the ports is used to synchronize with an upstream node. The other ports can be used to distribute time signals to downstream nodes.

In practice, a BC synchronizes its time with the upstream device and issues the synchronized time to the downstream devices.

As shown in [Figure 14-10](#), BC contains the access network devices at the access layer.

E2E TC

An E2E TC provides several physical ports, forwards all PTP messages, and measures and corrects the residence time of PTP event messages traversing the E2E TC.

P2P TC

A P2P TC has multiple ports. In addition to functions of an E2E TC, a P2P TC is also able to compute and correct the link delay between each port and similarly equipped port on another node sharing the link, that is, the link peer.

Difference between a TC and BC/OC: BC/OC must be synchronized with the clock on other devices, and TC does not restore the clock from IEEE 1588 packets but processes and forwards IEEE 1588 packets.

As shown in [Figure 14-10](#), a TC can function as a device at the aggregation layer.

Management node

A management node has multiple ports and serves as a management interface to PTP management messages. The management node is only used to manage the synchronization nodes and does not provide the synchronization function.

14.4.2.2 Clock Domain and Clock ID

Clock Domain

Logically, a physical network can be divided into multiple clock domains. Each clock domain has a reference time with which all devices in the domain are synchronized. Each clock domain has its own reference time and these times are independent of one another.

A device can join only one clock domain and can synchronize only with the synchronization time of that clock domain.

Clock ID

A clock ID identifies a clock in an IEEE 1588v2 clock subnet. In an IEEE 1588v2 packet, a clock source ID occupies eight bytes. It consists of two parts: The first three bytes are OUI code, and the other five bytes are extended ID.

Organizational Unique Identifier (OUI): an organization identifier uniformly assigned by the IEEE standard.

Extended ID: an identifier uniformly assigned by the organization represented by the OUI to ensure that the clock ID in each IEEE 1588v2 packet is unique.

14.4.2.3 1588v2 Messages

Message Type

As shown in [Table 14-5](#), there are two types of IEEE 1588v2 messages: event message and general message.

Table 14-5 Message Type

Message Type	Message	Description
Event message	• Sync • Delay_Req • Pdelay_Req • Pdelay_Resp	Event messages are timed messages in that an accurate timestamp is generated both at the device ingress and egress. Timestamps need to be processed in a timely manner at the time of message transmission and reception.
General Message	• Announce • Follow_Up • Delay_Resp • Pdelay_Resp_Follow_Up	General messages are not timed messages and do not require accurate timestamps. Timestamps do not need to be processed in a timely manner at the time of message transmission and reception.

- The Sync, Delay_Req, Follow_Up, and Delay_Resp messages are used to generate and communicate the timing information needed to synchronize OCs and BCs using the delay request-response mechanism.
- The Pdelay_Req, Pdelay_Resp, and Pdelay_Resp_Follow_Up messages are used to measure the link delay between two clock ports implementing the Pdelay mechanism. The link delay is used to correct timing information in Sync and Follow_Up messages in systems composed of P2P TCs. OCs and BCs that implement the Pdelay mechanism can synchronize using the measured link delays and the information in the Sync and Follow_Up messages.
- The Announce message is used to establish the synchronization hierarchy. That is, information related to the best master clock (BMC) algorithm is carried in the Announce messages.

Message Format

An IEEE 1588v2 message must have a header, body, and suffix. The suffix length may be 0.

An IEEE 1588v2 message may be encapsulated in Ethernet or IP format.

IEEE 1588v2 message encapsulated in Ethernet format

Messages encapsulated in Ethernet format are classified into IEEE 1588v2 over Ethernet messages without VLAN tags and IEEE 1588v2 over Ethernet messages with VLAN tags.

Figure 14-11 Format of an IEEE 1588v2 over Ethernet message

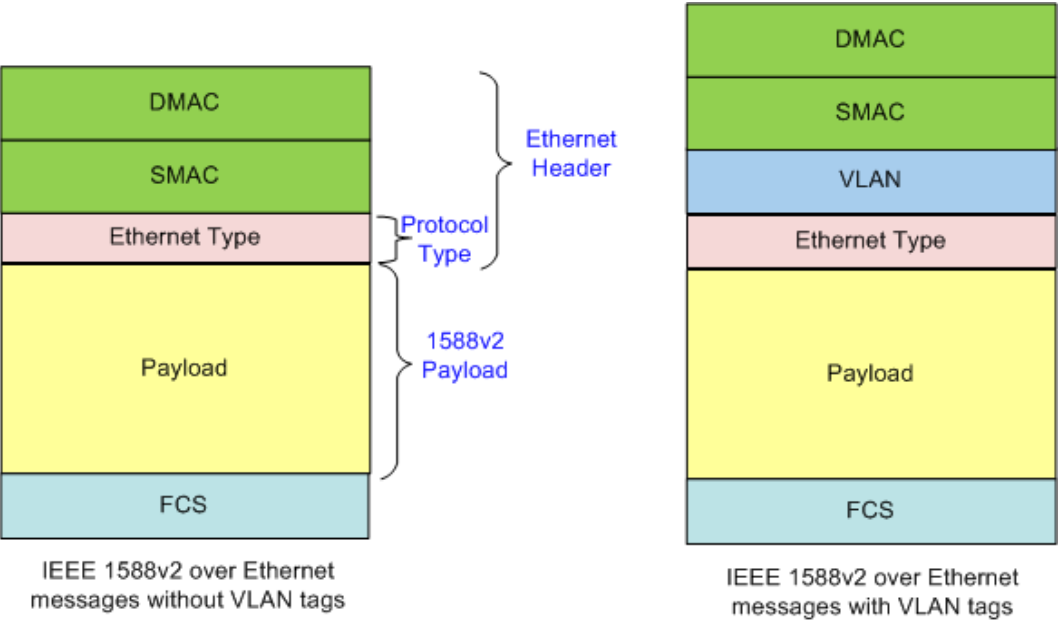


Table 14-6 describes the fields in an IEEE 1588v2 over Ethernet message.

Table 14-6 Fields in an IEEE 1588v2 over Ethernet message

Field Name	Bit Width (Unit: Bit)	Description
DMAC	6 x 8 = 48	Destination MAC address. It is configured by a user. - When the destination MAC address is not configured, the multicast encapsulation mode is used. This field is filled with 01-80-C2-00-00-0E for Pdelay packets and filled with 01-1B-19-00-00-00 for other packets. - When the destination MAC address is configured, the unicast encapsulation mode is used. This field is filled with the configured destination MAC address or with the SMAC of received packets.
SMAC	6 x 8 = 48	Source MAC address. It is configured by a user. It is the MAC address of an NE's control board.
VLAN	4 x 8 = 32	VLAN tag. It is configured by a user. At most one VLAN tag is supported, and TPID can only be 0x8100.
Ethernet Type	2 x 8 = 16	Ethernet type. It is configured by the system. This field has a fixed value of 88F7, which indicates an IEEE 1588v2 over Ethernet message.

Field Name	Bit Width (Unit: Bit)	Description
Payload	N = (A value ranging from 44 to 64) x 8	Payload of an IEEE 1588v2 over Ethernet message.
FCS	4 x 8 = 32	CRC32 check value.

IEEE 1588v2 message encapsulated in IP format

Messages in encapsulated in IP format are classified into IEEE 1588v2 over IPv4 messages without VLAN tags and IEEE 1588v2 over IPv4 messages with VLAN tags.

Figure 14-12 Format of an IEEE 1588v2 over IPv4 message

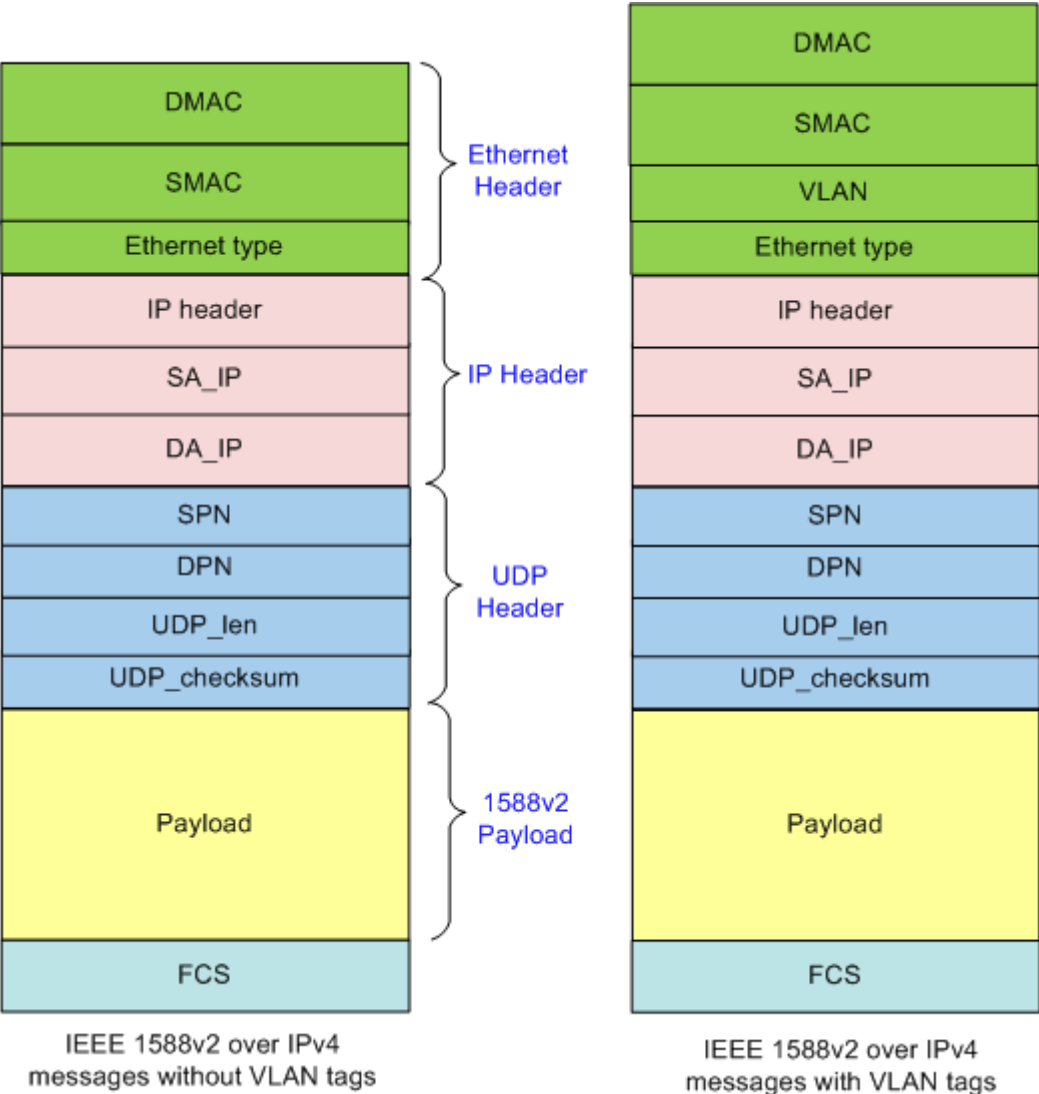


Table 14-7 lists the fields in an IEEE 1588v2 over IPv4 message.

Table 14-7 Fields in an IEEE 1588v2 over IPv4 message

Field Name	Bit Width (Unit: Bit)	Description
DMAC	6 x 8 = 48	-
SMAC	6 x 8 = 48	-
Ethernet Type	2 x 8 = 16	-

Field Name	Bit Width (Unit: Bit)	Description
VLAN	4 x 8 = 32	At most one VLAN tag is supported, and TPID can only be 0x8100.
IP header	12 x 8 = 96	An IP header consists of: IP version (4 bits) Header length (4 bits) Service type (8 bits) Total length (16 bits) Identifier (16 bits) Flag (3 bits) Fragment offset (13 bits) Lifetime (8 bits) Protocol (8 bits) Header checksum (16 bits)
SA_IP	4 x 8 = 32	Source IP Address. If an NE port is configured with an IP address, this field is filled with this IP address. If an NE port is not configured with an IP address, this field is filled with the NE's IP address.
DA_IP	4 x 8 = 32	Destination IP Address. When the destination IP address is not configured, the multicast encapsulation mode is used. This field is automatically filled with the destination IP address. It is filled with 224.0.0.107 for Pdelay packets and filled with 224.0.1.129 for other packets. When the destination IP address is configured, the unicast encapsulation mode is used. This field is filled with the configured destination IP address or with the SA_IP of received packets.
SPN	2 x 8 = 16	Source port ID. It is filled by the system with the ID of the NE port that transmits the packet.
DPN	2 x 8 = 16	Destination port ID, which is used to identify whether the packet is a 1588 packet. It is filled by the system.
UDP_Len	2 x 8 = 16	Data packet length. It is calculated by the system automatically using the following formula: UDP header length + 1588v2 payload length.

Field Name	Bit Width (Unit: Bit)	Description
UDP_checksum	2 x 8 = 16	Header checksum. The value is 0 if the check is not required.
Payload	N = (A value ranging from 44 to 64) x 8	-
FCS	4 x 8 = 32	-

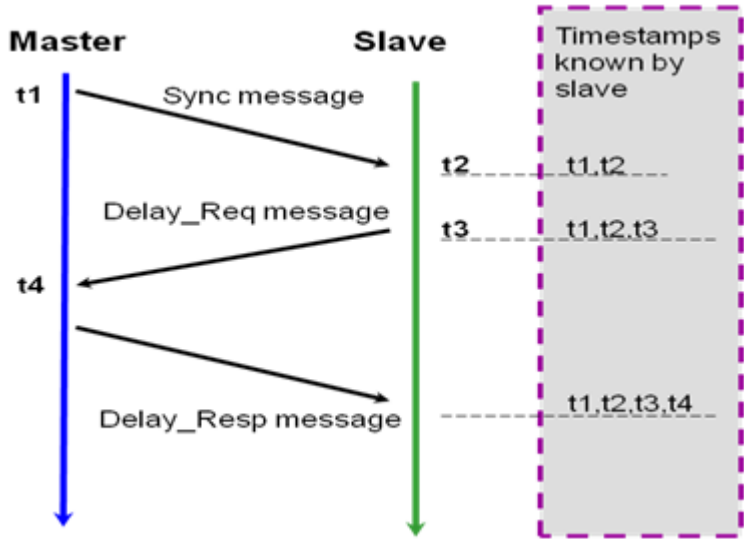
14.4.3 1588v2 Principle

14.4.3.1 Clock Synchronization Mechanism

Time Synchronization Principle

The master and slave exchanges IEEE 1588v2 messages in the following procedure:

Figure 14-13 IEEE 1588v2 time synchronization principle



1. The master sends a Sync message at t1 and carries the t1 timestamp in the Sync message.
2. The slave receives the Sync message at t2, locally generates the t2 timestamp, and extracts the t1 timestamp from the Sync message.

3. The slave sends a Delay_Req message at t3 and locally generates the t3 timestamp.
4. The master receives the Delay_Req message at t4, locally generates the t4 timestamp, and sends the Delay_Req message with the t4 timestamp back to the slave.
5. The slave extracts the t4 timestamp from the Delay_Res message after receiving it.

"Delaysm" is the path delay in the direction from the master to the slave,
"Delaysm" is the path delay in the direction from the slave to the master, and
"Offset" is the time offset between the slave and master. All of them are variables.

$$t2 - t1 = \text{Delaysm} + \text{Offset}$$

$$t4 - t3 = \text{Delaysm} - \text{Offset}$$

When Delaysm = Delaysm, that is, when the transmit and receive links between the master and slave are symmetric, the following formula is satisfied:

$$\text{Offset} = [(t2 - t1) - (t4 - t3)] / 2$$

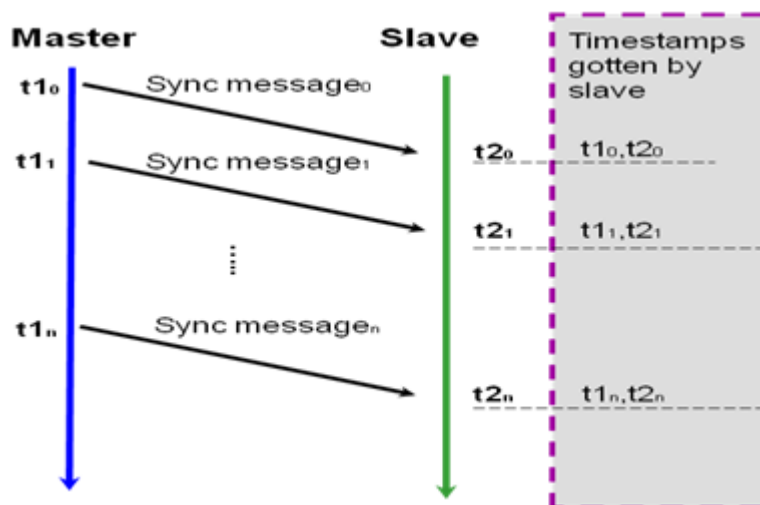
The slave can calculate the time offset between itself and the master based on the t1, t2, t3, and t4 timestamps and then corrects its own time to get synchronized with the master.

The preceding principle shows that IEEE 1588v2 time synchronization is based on the link symmetry between the master and slave. If the transmit and receive links are asymmetric, synchronization errors will occur and it will be half of the link delay asymmetry.

Frequency Synchronization Principle

The IEEE 1588v2 protocol implements frequency synchronization by exchanging Sync messages between the master and slave.

Figure 14-14 IEEE 1588v2 frequency synchronization principle



The master periodically sends Sync messages to the slave. If the slave frequency is synchronized to the master frequency, then the accumulative time errors within

the same time periods are the same, as long as the path delay changes are neglected.

In other words, $t_{2_1}-t_{2_0}=t_{1_1}-t_{1_0}$, $t_{2_2}-t_{2_1}=t_{1_2}-t_{1_1}$, $t_{2_3}-t_{2_2}=t_{1_3}-t_{1_2}, \dots, t_{2_n}-t_{2_0}=t_{1_n}-t_{1_0}$.

If $t_{2_n}-t_{2_0}$ is greater than $t_{1_n}-t_{1_0}$, then the slave frequency is higher than the master frequency, which means the slave frequency must be decreased. Conversely, the slave frequency must be increased.

14.4.3.2 BMC Algorithm

Background

The 1588v2 synchronization process involves two phases:

1. Establish the master/slave hierarchy.
In a clock domain, ordinary clock (OC) nodes and boundary clock (BC) nodes run the best master clock (BMC) algorithm based on the information carried in Announce packets received from each port to determine the reference clock source of each OC node and BC node and the status of each port, and set up the master-slave hierarchy and tracing path of the entire synchronization network.
2. Frequency/time synchronization
After the master/slave hierarchy and tracing paths are established, the master and slave exchange event messages such as Sync, Delay_Req, and Delay_Resp to implement frequency or time synchronization.

This section describes the BMC algorithm principles.

Overview

The BMC algorithm, defined in the 1588v2 protocol, is used to determine the master-slave relationship among clocks in a network. With this algorithm, clocks in the network are classified into master clock and slave clock. Slave clocks lock the frequency or time of the master clock. In the event of changes in the network or clock source attributes, the best master clock is re-selected using the BMC algorithm so that the time and clock in the entire network are synchronized.

- From the network aspect, the BMC algorithm helps form a tree structured (Grandmaster as the root and best clock source) master-slave synchronization hierarchy for clocks in the entire network.
- From the node aspect, the BMC algorithm helps determine the master clock in each clock node. All Announce messages received on the ports of a given clock node and the local clock are compared to determine which clock is the best.

If the best clock is an external clock, the external clock is determined as the master clock, that is, the clock is traced. If the best clock is the local clock, the local clock is the Grandmaster clock.

Algorithm Implementation

The BMC algorithm involves data set comparison, status decision, state machine, and data set update. The data set members include priority, clock quality (level,

precision, and offset), and stepRemoved (distance to the Grandmaster). These members are contained in ANNOUNCE packets defined by the protocol. An NE obtains the information about these members from the ANNOUNCE packets received on its ports. The NE uses the data set comparison algorithm to select the best external clock source (Ebest). Then the NE uses the status decision and state machine to determine the master/slave state of each port based on the Ebest, local clock D0, and data sets on the ports (Erbest). If the NE's clock is the master clock on the entire network, the NE's all ports transmit clock signals to other NEs. If the NE's clock is the slave clock, a port on the NE must be the slave port for tracing the master clock. The NE transmits the obtained master clock data to lower-layer NEs in ANNOUNCE packets through its master port.

Data set comparison algorithm

The algorithm compares two groups of data that represent two clock ports. One group of data represents the default features of the local clock, and the other group of data represents the information contained in the synchronization packet received from an external port. The algorithm compares the following attributes in the data sets in order to obtain the best ANNOUNCE packet:

- priority1: indicates the priority configured by a user. It identifies a clock's relative priority in the master clock set.
- clockClass: indicates the clock source's level.
- clockAccuracy: indicates the clock's precision.
- OffsetScaledLogVariance: indicates the clock's stability. It is the quality of clock signals that are received by an NE. The NE obtains the value using Allan deviation.
- priority2: indicates the priority configured by a user. It is used to select a better clock source when other attributes of clock sources are the same.
- Clock Identity: indicates the clock ID on a device.

After the preceding priority-based sorting is complete, when two interfaces on the same NE receive two Announce messages indicating the same external master clock and the comparison results are the same, distance between the local clock and the external master clock (indicated by the stepsRemoved field in the Announce message) is used to determine the clock based on the number of hops on the link. (The clock received by the port with fewer hops to the Grandmaster clock source is selected.) This situation usually occurs in a PTP system with a loop.

Status decision algorithm

The status decision algorithm involves the data sets D0, Erbest, and Ebest. The algorithm determines the status decision code and recommended status for each port based on the data set comparison results. The recommended status is a factor for triggering the state machine. The state machine obtains a port's next status based on the triggering factor and current status. The status decision code is used to select a data set to update the global date set of the NE.

State machine

The state machine obtains a port's next status based on the triggering factor and current status. The trigger condition may be the recommended status of the port or some external events that may cause the status change, such as port enabling/disabling (DISABLE/ENABLE), port going online/offline (PORT LINKUP/DOWN), and timeout (TIMEOUT) interruption.

Data set update

An NE uses the status decision code of each port to determine whether to use Ebest or D0 to update the global data set. The updated global data set is used as the tracing data set of the NE and is transmitted by the NE's master port to lower-layer NEs.

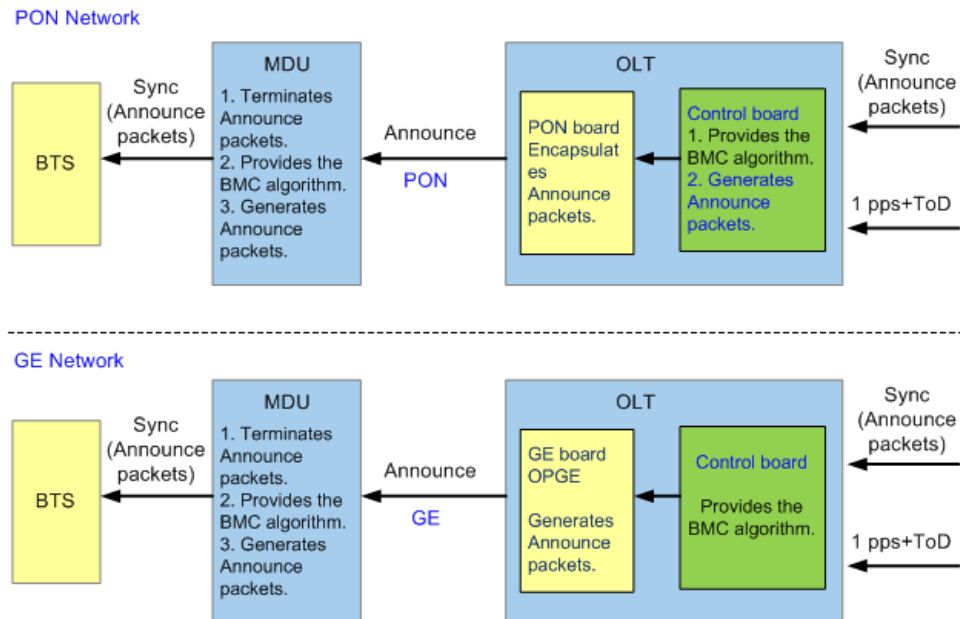
In the LTE carrying scenario, the BMC uses only the data set comparison algorithm. The algorithm is implemented as follows: Each port uses the algorithm to compare the ANNOUNCE packets that contain clock information and select the best clock source (Erbest) received on the port.

BMC Implementation in an FTTM LTE Scenario

As shown in [Figure 14-15](#), in the PON networking scenario carried by FTTM LTE base stations, the overall BMC solution is as follows:

1. An OLT obtains ANNOUNCE packets from an uplink Ethernet port.
2. The control board of the OLT obtains the time source information from the Announce message, compares the time source with other synchronization sources in the system through the BMC algorithm, and selects the best clock as the system time source.
3. The OLT constructs Announce packets and broadcasts the packets to downstream MDUs through the GEM ports.
4. The MDU obtains the Announce message from the PON line, obtains the time source information from the Announce message, compares the time source with other synchronization sources in the system through the BMC algorithm, and selects the best clock as the system time source.
5. An MDU constructs ANNOUNCE packets and transmits them to lower-layer base stations using user-side ports.

The difference between the GE networking scenario and the PON networking scenario is as follows: The OLT constructs the Announce packets and then issues the PTP packets to the downstream MDU through the GE.

Figure 14-15 BMC implementation in an FTTM LTE scenario

14.4.3.3 Delay Compensation Mechanism

Context

Based on the principles described, 1588v2 time synchronization is based on delay symmetry on transmit and receive links between the master and slave. If the link delay between the master and slave is asymmetric, synchronization values will be inaccurate, and the error will be half of the asymmetric link delay.

The transmission delay on a one-meter fiber is about 5 ns, so asymmetry on a one-meter fiber causes a 2.5 ns time synchronization error, and asymmetry on a 400-meter fiber causes a 1 us error. On a practical network, it is difficult to accurately control the E2E fiber asymmetry on the entire network within 400 m. For TD-SCDMA and LTE-TDD which require a synchronization precision of ± 1.5 us, a 1 us error is obviously intolerable. Therefore, in deployment of the 1588v2 time synchronous network, fiber asymmetry in the network must be seriously considered.

Solution

Currently, three solutions to fiber asymmetry are used in the industry:

- **Point-by-point measurement by instrument:** During deployment and maintenance, a device's 1588 time synchronization precision is measured by an 1588v2 instrument point by point. Fiber asymmetry is calculated based on the measured precision, and compensation is made accordingly. Alternatively, an OTDR can be used to measure asymmetry of each pair of fibers, and compensation can be made. The OTDR test interrupts services and the 1588v2 synchronization result cannot be viewed directly. Therefore, the 1588v2 meter is recommended for the test.
- **Bidirectional transmission over a single fiber:** A device uses a bidirectional single-fiber optical module to support signal transmission and reception on a

single fiber. This solution substantially resolves the asymmetry issue on dual-fiber links, and no measurement or compensation is required. In this solution, bidirectional link delay due to different wavelengths used for transmitting and receiving signals is generally small and can be automatically calculated and compensated by devices. According to G.652, the time error introduced by FE single-fiber bidirectional transmission is about 1.06 ns per kilometer, and the time error introduced by GE single-fiber bidirectional transmission is about 0.544 ns per kilometer, which is far less than the time error of 2.5 ns per meter for common dual-fiber transmission. After the single-fiber bidirectional optical module is used, you do not need to perform measurement onsite during deployment or maintenance.

- Automatic ring network measurement: A device uses a common dual-fiber optical module. During deployment, an instrument measures and compensates for asymmetry. During maintenance, asymmetry can be automatically measured on the ring network to avoid the necessity for onsite measurement upon fiber disconnection. This solution reduces the workload for repairing fiber disconnection. This solution utilizes the BMC algorithm in 1588v2. When fiber disconnection occurs on a ring network, services are automatically switched to the standby link, and the time synchronization precision of the nodes on the ring network stays in the usable range. When the faulty fiber is re-connected, the devices first automatically calculate and report asymmetry on the new fiber link and then compensate for asymmetry on the NMS. After that, services are switched back to the active link.

Delay Compensation Mode

Delay compensation can be length compensation or time compensation.

The relationship between the length compensation and time compensation is as follows: the delay compensated for each 1 m twisted pair is 8 ns, and the delay compensated for each 1 m coaxial cable is 4.5 ns.

14.4.4 1588v2 Network Application

14.4.4.1 Recommended: Synchronization Application (Network-wide 1588v2 and Synchronous Ethernet Deployment)

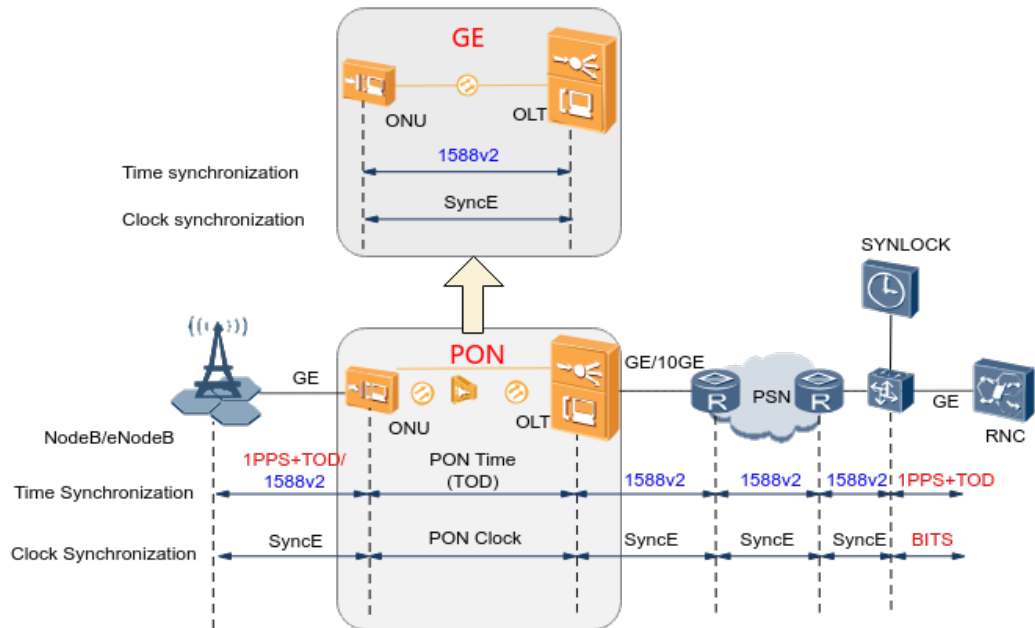
When bearer network devices support 1588v2 synchronization, time signals are injected from the bearer network.

- Time is synchronized in 1588v2 mode.
- When devices on the entire network support synchronous Ethernet (SyncE), SyncE is recommended for clock synchronization, as follows.

NOTE

SyncE uses Ethernet bit streams to recover clock signals for Ethernet clock synchronization. The implementation mode is similar to that on an SDH/PDH network. SyncE uses high-precision clock signals as the transit reference in the transmit direction. It restores and extracts the clock signals at the receive end. The physical layer transmits and receives the clock signals and is compatible with traditional networks.

Figure 14-16 Synchronization application (network-wide 1588v2 and SyncE deployment)



Time Synchronization

- Bearer network devices are used as an Ordinary Clock (OC) device. A bearer network device receives time signals through a 1PPS+TOD port and uses 1588v2 to synchronize time signals with other bearer network devices.
- Access devices are regarded as a boundary clock (BC) device as a whole. An OLT transmits 1588v2 time signals through a GE or 10GE upstream link to ONUs, and the ONUs output 1588v2 time to downstream devices through user-side GE links. Between the OLT and an ONU, time is transmitted using PON links in ONT Management and Control Interface (OMCI) mode or using GE links in PTP packet mode.
- Base stations are used as an Ordinary Clock (OC) device.
 - If a base station does not support 1588v2 synchronization, the base station uses a 1PPS+TOD port to receive time signals.
 - If a base station supports 1588v2 synchronization, the base station uses 1588v2 to synchronize time signals.

Clock Synchronization

- Bearer network devices use SyncE to synchronize clock signals with each other.
- An OLT transmits SyncE through a GE or 10GE upstream link to ONUs, and the ONUs output SyncE to downstream devices through user-side GE links. Between the OLT and an ONU, time is transmitted using PON or GE links.
- The base stations use SyncE to synchronize clock signals.

14.4.4.2 Synchronization Application (Network-wide 1588v2 Deployment)

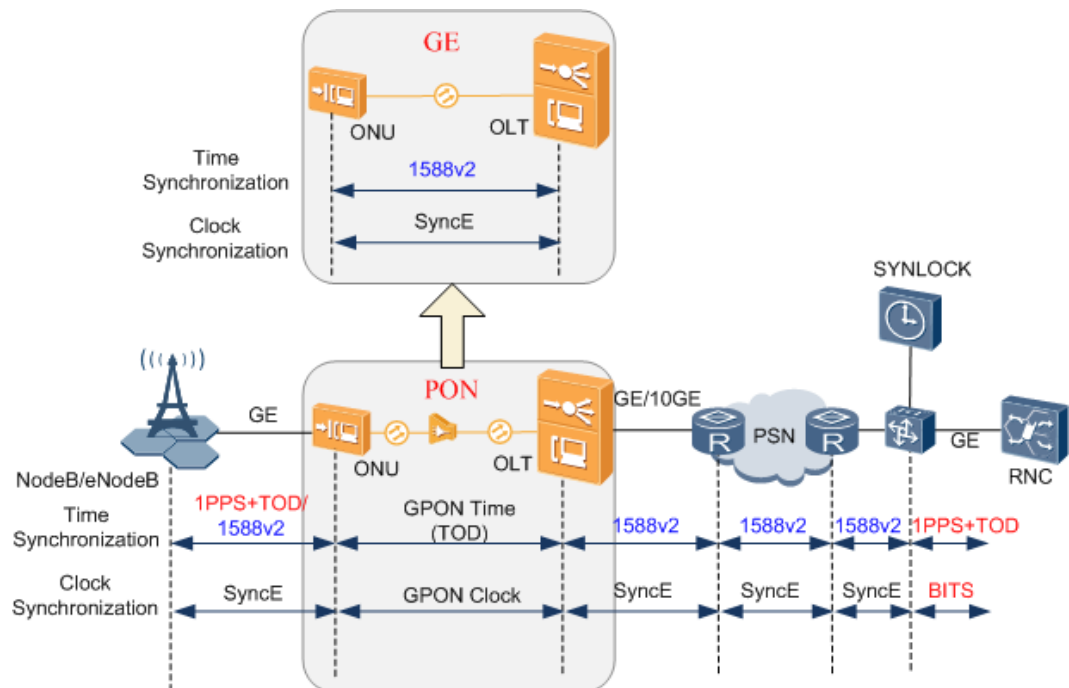
If devices at the bearer network support 1588v2 synchronization, time source is injected from the devices, and time synchronization is implemented using 1588v2.

If devices at the entire network do not support Synchronous Ethernet (SyncE), clock synchronization is implemented using 1588v2.

Time synchronization must be implemented on 3G, 4G, or Long Term Evolution (LTE) base stations and can be provided by the bearer network. When bearer network devices support 1588v2 synchronization, time signals are injected to a bearer network device and be synchronized, as shown in [Figure 14-17](#).

- Bearer network devices are used as an Ordinary Clock (OC) device to inject the synchronization time source using the 1PPS+TOD port. A bearer network device receives time signals through a 1PPS+TOD port and uses 1588v2 to synchronize time and clock signals with other bearer network devices.
- OLTs and ONUs are regarded as a boundary clock (BC) device as a whole. An OLT transmits 1588v2 time signals through a GE or 10GE upstream link to ONUs, and the ONUs output 1588v2 time to downstream devices through user-side GE links. Between the OLT and an ONU, time and clock signals are transmitted using PON links in ONT Management and Control Interface (OMCI) mode or using GE links in PTP packet mode.
- Base stations are used as an Ordinary Clock (OC) device.
 - If a base station does not support 1588v2 synchronization, the base station uses a 1PPS+TOD port to receive time signals, and use SyncE to synchronize clock signals.
 - If a base station supports 1588v2 synchronization, the base station uses 1588v2 to synchronize time and clock signals.

Figure 14-17 Synchronization application (network-wide 1588v2 deployment)



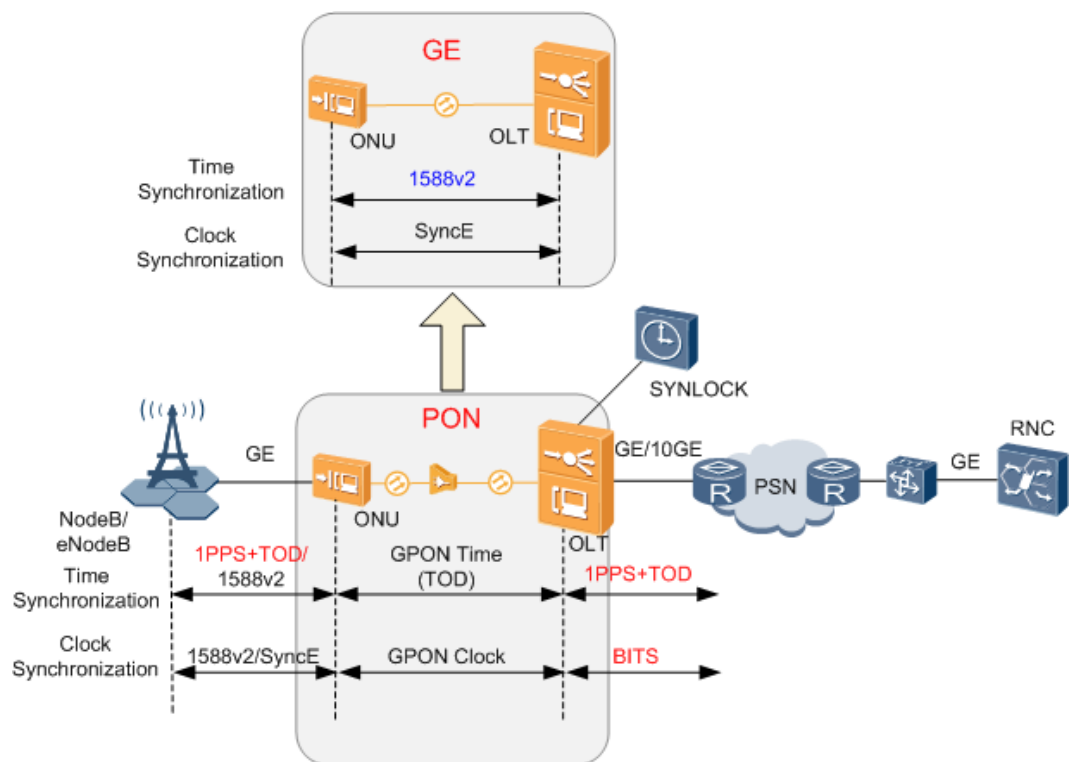
14.4.4.3 Synchronization Application (Clock or Time Signal Injection from an OLT)

Devices at the bearer network do not support 1588v2 synchronization, and time source and clock source are injected from an OLT.

3G and 4G long term evolution (LTE) base stations require time synchronization. When devices on the bearer network do not support 1588v2 synchronization, time signals can be injected from an OLT, as shown in [Figure 14-18](#).

- Time signals are injected from an OLT using a 1PPS+TOD port. The BITS synchronization clock source is injected into the building integrated timing supply (BITS) port.
- OLTs and ONUs are regarded as a boundary clock (BC) device as a whole. ONUs output 1588v2 time to downstream devices through user-side GE links. Between the OLT and an ONU, time and clock signals are transmitted using PON links in ONT Management and Control Interface (OMCI) mode or using GE links in PTP packet mode.
- Base stations are used as an Ordinary Clock (OC) device.
 - If a base station does not support 1588v2 synchronization, the base station uses a 1PPS+TOD port to receive time signals, and use SyncE to synchronize clock signals.
 - If a base station supports 1588v2 synchronization, the base station uses 1588v2 to synchronize time and clock signals.

Figure 14-18 Synchronization application (1588v2 clock or time signal injection from an OLT)



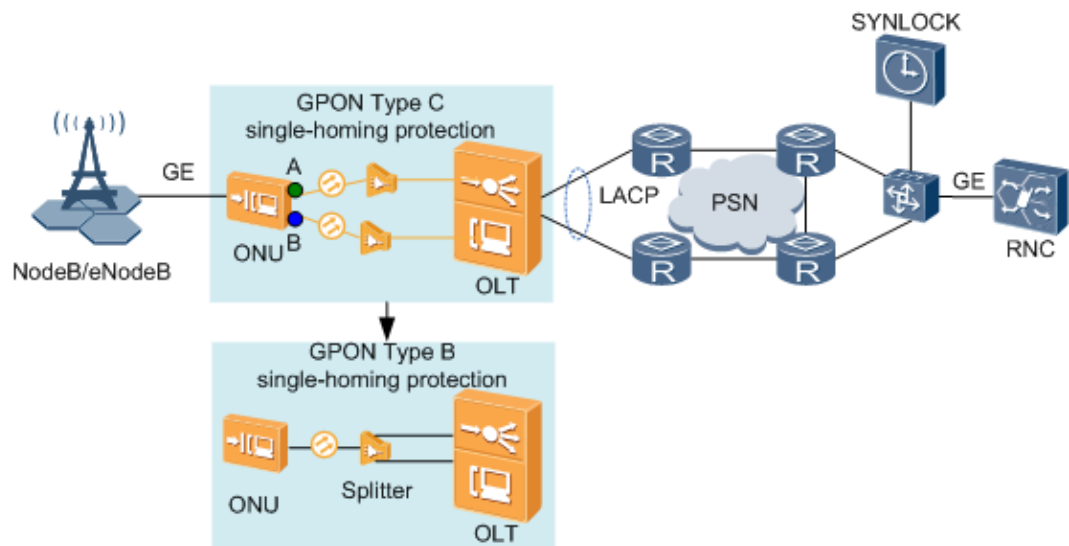
14.4.4.4 Time and Clock Synchronization Protection Application

A protection solution is provided on the bearer network and multiple time sources and clock sources are available. The time and clock synchronization protection feature improves network security.

As shown in [Figure 14-19](#), GPON Type C/Type B single-homing protection is configured between the ONU and two OLTs, and LACP is configured between the OLTs and bearer network devices.

- When the working link becomes faulty, protection switching is triggered and data is switched to the standby link. This protection mechanism ensures uninterrupted data transmission.
- As shown in [Figure 14-19](#), port A is assumed to be a master port and port B is a slave port. If the active link is faulty, the clock source must also be switched to the standby link. That is, the link is switched from port A to port B. This prevents signals from being lost.
- After the faulty link restores, the system will not immediately switch the clock source back to the original active link and the clock source of port B is preferentially traced.

Figure 14-19 GPON Type C dual-homing protection



NOTE

Other protection features can be deployed between the OLT and ONUs, or between the OLT and the bearer network. For details about the protection features, see feature description.

Table 14-8 Time and clock source selection modes on an ONU/OLT

Synchronizati on Type	Time and Clock Source Selection Modes on an ONU/OLT
Time synchronizatio n	• Static selection based on priorities configured on an ONU/OLT Users must configure a unique priority for each external time source. The system selects the time source that has the highest priority and is in the normal state as the reference time. • Automatic selection based on best master clock (BMC) The BMC algorithm classifies clocks on a network into a master clock and slave clocks. Slave clocks trace the frequency or time of the master clock. When the network topology or the attribute of a clock source changes, the algorithm selects a new grandmaster clock so that clocks and times are synchronized on the entire network. For details, see 14.4.3.2 BMC Algorithm.
Clock synchronizatio n	• Static selection based on priorities configured on an ONU/OLT Users must configure a unique priority for each external clock source. The system selects the clock source that has the highest priority and is in the normal state as the reference clock. • Automatic selection based on Synchronization Status Message (SSM) levels The system obtains the clock quality level from received clock source signals (users must manually configure the quality level for a clock source whose SSM level cannot be obtained). Then the system automatically selects a clock source as the reference clock when the source meets the following three conditions: has the highest level; the level is not smaller than the lower SSM level; is in the normal state. If the two external clock sources have the highest SSM quality level, the system selects a clock source with the highest priority as the system reference clock.

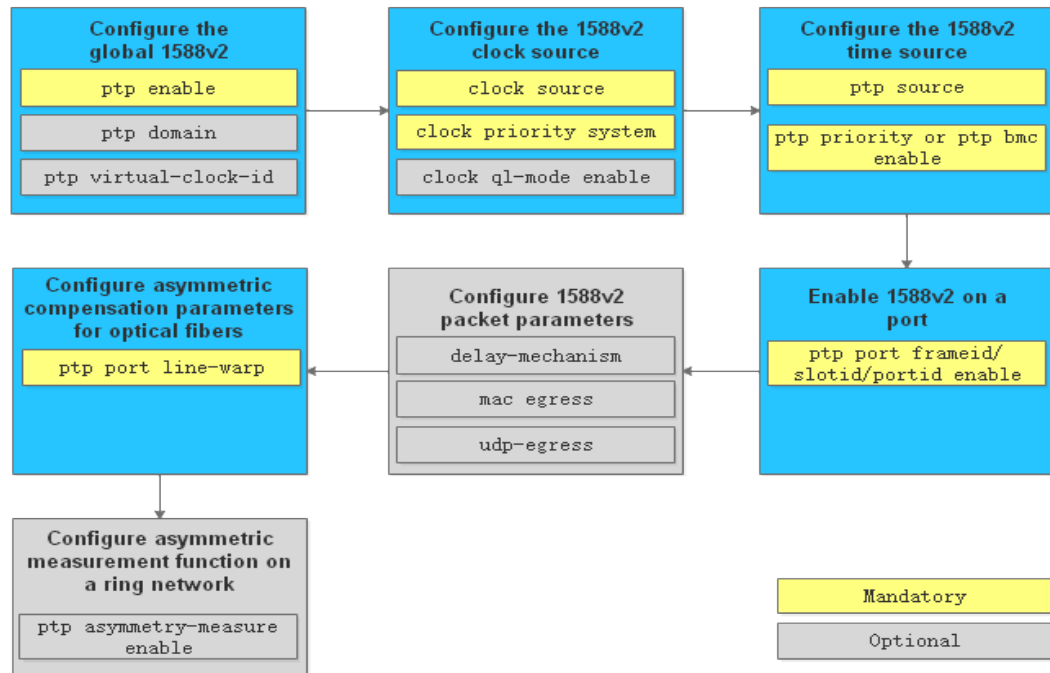
14.4.5 Configuring the 1588v2 Function

3G and 4G long term evolution (LTE) base stations require frequency (clock) and phase (time) synchronization. This section describes how to configure 1588v2 to implement clock synchronization and sub-microsecond-level time synchronization.

Configuration Process

[Figure 14-20](#) shows the process of configuring the 1588v2 function.

Figure 14-20 Process of configuring the 1588v2 function



Procedure

Step 1 Configure the global 1588v2 function.

1. Run the **ptp enable** command to enable the 1588v2 function on a device.
2. **Optional:** Run the **ptp domain** command to specify a 1588v2 time domain.

After the configuration, a time domain has a clock source. All devices in the time domain use the clock source. Ensure that the MDU time domain is the same as that of the OLT and upper-layer bearer network device.

3. **Optional:** Run the **ptp virtual-clock-id** command to configure the 1588v2 virtual clock ID of a device.

The clock ID uniquely identifies a clock node in a 1588v2 domain.

If this parameter is not configured, its value consists of the organizational unique identifier (OUI)+product ID+last four bytes of the MAC address. The OUI is 00-25-9e, and the product ID is 40. For example, if the MAC address of the system is 00e0-fc00-a025, the corresponding default clock ID is 00259e405898a025.

Step 2 Configure a 1588v2 clock source. After the configuration, device clocks on the network are synchronized.

1. Run the **clock source** command to configure a 1588v2 clock source.

The clock source can be the synchronous Ethernet clock or 1588v2 clock recovered from a GE or 10GE line on the network side or the BITS clock.

If the network supports the synchronous Ethernet clock, the clock source preferentially uses the synchronous Ethernet clock.

2. Run the **clock priority system** command to set the priority of the clock source. A device may trace multiple clock sources for synchronizing the clock. It selects the clock source with the highest priority as the clock source.

p0 indicates the highest priority, and p9 indicates the lowest priority.

3. **Optional:** Configure the clock source selection mode when the protection mechanism is configured.

A clock source can be statically or dynamically selected.

- To statically select a clock source based on the local priority, perform [Step 2.2](#) to set a local priority for a clock source. The device selects the clock source with the highest priority as the clock source.
- To automatically select a clock source using the Synchronization Status Message (SSM):
 - i. Run the **clock ql-mode enable** command to configure the status of the SSM source selection function.
 - ii. Run **clock ql** command to configure the SSM quality level of the clock source. The device selects a clock source as the clock source when the clock source has the optimal quality level that is greater than or equal to the lowest SSM level of the clock input source and is running properly.

Step 3 Configure a 1588v2 time source. After the configuration, device time on the network is synchronized.

1. Run the **ptp source** command to configure a 1588v2 time source.

The time source can be the 1588v2 time recovered from a GE or 10 GE line on the network side or BITS time. If the network does not support 1588v2 time synchronization, the time source can use the BITS time.

2. **Optional:** When the BITS time is used, run the **ptp bits** command to configure the attributes of a BITS clock source, such as the precision and class of the clock source, and the priority of the clock signal.
3. Select a time source when the protection mechanism is used.

A time source can be statically or dynamically selected.

- To statically select a time source based on the local priority, run the **ptp priority** command to set the priority of the time source.
- To dynamically select a time source based on the best master clock (BMC), run the **ptp bmc enable** command to enable the automatic BMC source selection function.

Step 4 Enable 1588v2 on a port to transmit 1588v2 packets.

Run the **ptp port** to enable 1588v2 on an Ethernet port.

Enable 1588v2 on all Ethernet ports that need to transmit 1588v2 packets.

Step 5 Optional: (Optional) Configure 1588v2 parameters.

Set the timestamp mode of the 1588v2 packets, MAC encapsulation mode, and UDP encapsulation mode.

1. Run the **ptp port delay-mechanism** command to configure the delay measurement mode for 1588v2 ports. The default mode is delay.

The delay measurement mode on ports of all the devices in a 1588v2 synchronization network must be the same.

2. Run the **ptp port frameid/slotid/portid clock-step { one-step | two-step }** command to configure the step mode for 1588v2 ports.

By default, 1588v2 packets carry timestamps in one-step mode. The 1588v2 ports identify Follow_Up packets in two-step mode in the Rx direction for communicating with other products.

3. Run the **ptp port frameid/slotid/portid interval { announce value | req value | sync value }** command to configure the interval at which 1588v2 packets are sent.
 - 1588v2 frequency synchronization:
The peer-end master device must send Sync packets at an interval longer than or equal to 32 packets per second.
 - 1588v2 time synchronization:
 - The peer-end master device must send Sync packets at an interval longer than or equal to 1 packet per second.
 - The local-end device must send Delay_request or Pdelay_request packets at an interval longer than or equal to 1 packet per second.
4. **Optional:** Configure the encapsulation mode for 1588v2 packets.
 - Run the **ptp port mac-egress** command to configure the MAC encapsulation mode for 1588v2 packets to be forwarded by the port. The packets are forwarded in Layer 2 mode.
 - When you specify **destination-mac**, the 1588v2 packets are forwarded in Layer 2 unicast mode.
 - When you do not specify **destination-mac** *destination-mac-value*, the 1588v2 packets are forwarded in Layer 2 multicast mode.
 - Run the **ptp port frameid/slotid/portid udp-egress { [destination-mac destination-mac-value] | [source-ip source-ip-addr [destination-ip destination-ip-addr] [dscp dscp-value] [vlan vlan-id [priority priority-value]] }** command to configure the UDP encapsulation mode for 1588v2 packets to be forwarded on the port. The packets are forwarded in Layer 3 mode.
 - When you specify **destination-ip** *destination-ip-addr*, the 1588v2 packets are forwarded in Layer 3 unicast mode.
 - When you do not specify **destination-ip** *destination-ip-addr*, the 1588v2 packets are forwarded in Layer 3 multicast mode.

Step 6 Configure asymmetric compensation parameters for optical fibers.

Run the **ptp port frameid/slotid/portid line-warp linewarptype linewarptype linewarpvalue** command to configure asymmetric compensation parameters for optical fibers.

Asymmetric optical fibers between two devices result in time difference for data transmission and reception. During site deployment, measure and calculate the time differences in the two directions and compensate the time on the devices by configuring cable transmission deviations.

Step 7 **Optional:** Configure the asymmetric measurement function on a ring network.

Run the **ptp asymmetry-measure enable** command to configure the asymmetric measurement function on a ring network.

This function utilizes the BMC algorithm in IEEE 1588v2. When fiber disconnection occurs on the ring network, services are automatically switched to the standby link, and the time synchronization precision of the nodes on the ring network stays in the usable range. When the faulty fiber is re-connected, the devices first automatically calculate and report asymmetry on the new fiber link and then compensate for asymmetry on the NMS. After that, services are switched back to the active link.

----End

Result

- Run the **display clock source** command to check whether the clock source in the system is 1588v2 and whether it is running properly. In normal cases, **State** is **successful**.
- Run the **display ptp source** command to check whether the clock source in the system is 1588v2 and whether it is running properly. In normal cases, **Lock state** is **successful**.

When clock tracing is abnormal, rectify the fault based on the handing suggestions in the reported alarm or event.

Example

An MDU connects to a 4G LTM eNodeB using a GE port. The MDU connects to the OLT using the GPON uplink port and then to the radio network controller (RNC) over the upper-layer network to carry 4G services over the access network. The 4G LTE eNodeB requires high precision time synchronization and the 1588v2 time is deployed on the network.

The parameters planned on the OLT are as follows:

- Time domain: 1
- Clock or time source input: GE uplink port 0/8/0
- Clock or time source output: GPON service port 0/3/1
- Packet encapsulation mode: MAC (default mode) (packets are forwarded in Layer 2 multicast mode)

The parameters planned on the MDU are as follows:

- Time domain: 1
- Clock or time source input: GPON uplink port 0/0/0
- Clock or time source output: GE service port 0/1/1
- Packet encapsulation mode: MAC (default mode) (packets are forwarded in Layer 2 multicast mode)

Configurations on the OLT side

```
huawei(config)#ptp enable
huawei(config)#ptp domain 1
huawei(config)#clock source 0 1588
huawei(config)#clock priority system 0
huawei(config)#ptp source 0 0/8/0
huawei(config)#ptp bmc enable
```

Configurations on the MDU

```
huawei(config)#ptp enable
huawei(config)#ptp domain 1
huawei(config)#clock source 0 0/0/0
huawei(config)#clock priority system 0
huawei(config)#ptp source 0 0/0/0
huawei(config)#ptp port 0/1/1 enable
huawei(config)#ptp bmc enable
```

14.4.6 Configuring 1588v2-related Delay Compensation for Asymmetric Fibers

Prerequisites

A global positioning system (GPS) and clock signal tester, such as a Paragon tester, are available.

The 1588v2 precision of the upper-layer device meets usage requirements.

1588v2-related Delay Compensation Rules for Asymmetric Fibers

- After the first compensation on a network, if the 1588v2 precision meets clock precision requirements (1 us) of a base station, no more compensation is required for this base station.
- If the 1588v2 precision is required to improve (to be within 500 ns) for a base station, or the 1588v2 precision of some base stations fails to meet clock precision requirements after the compensation on the entire network, a second compensation is required for such base stations.
- If the capacity of a network needs to be expanded (for example, a ring is added), and the compensation on new base stations or sites must not change the original compensation data, separate compensation is performed on the new base stations or sites.

Context

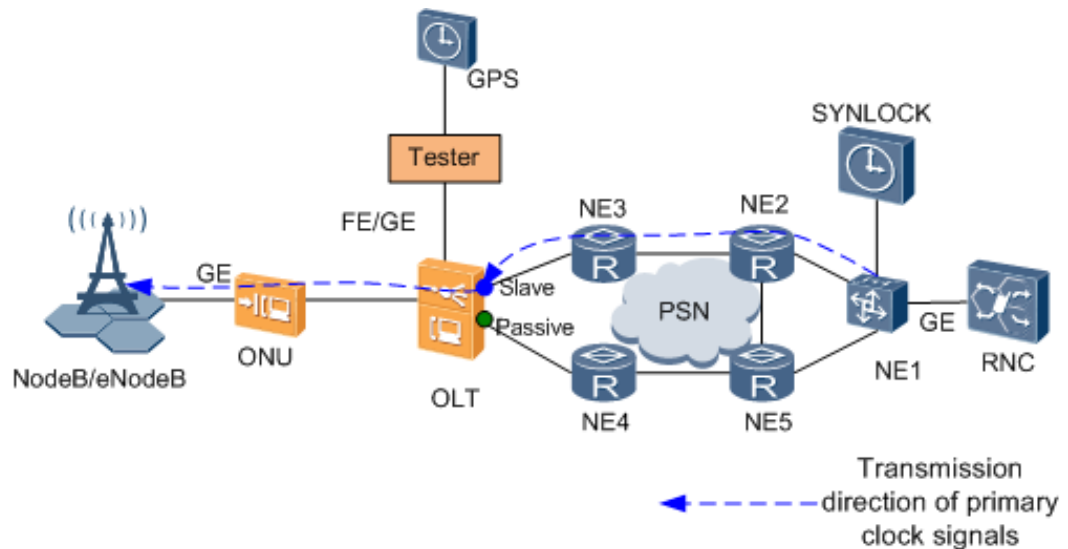
An OLT can connect to ONUs in PON or GE mode:

- In PON connections, the optical fibers between the OLT and ONUs are symmetric. Therefore, no asymmetric delay compensation is required for the optical fibers. In this case, you only need to measure the OLT and implement delay compensation on the optical fibers between the OLT and its upper-layer device.
- In GE connections, the optical fibers between the OLT and ONUs may be asymmetric. In this case, you need to measure the ONUs and implement delay compensation on the optical fibers not only between the OLT and its upper-layer device but also between the OLT and ONUs.

As shown in the following figure, the OLT is used as a test node.

- The OLT connects to a tester using an FE/GE/10GE port.
- The slave port on the OLT connects to NE 3 for receiving primary clock signals.
- The passive port on the OLT connects to NE 4 for receiving standby clock signals.

Figure 14-21 Delay compensation networking



Procedure

Step 1 Perform delay compensation on the slave port of the OLT.

1. Calculate the difference between the data output by the FE or GE port after the OLT traces the 1588v2 clock and the data measured by the GPS. Record the difference as D1.
2. Check whether D1 is within ± 20 ns. If it does, go to [Step 2.1](#). If it does not, go to [Step 1.3](#).
3. Run the **ptp port frameid/slotid/portid line-warp linewarptype linewarpdirection linewarpvalue** command to set the compensation value of the slave port to d, which is equal to D1.
4. Calculate the difference between the output 1 PPS data after the OLT traces the 1588v2 clock and the data measured by the GPS. Record the difference as D2.
5. Check whether D2 is within ± 20 ns. If it does, go to [Step 2.1](#). If it does not, go to [Step 1.3](#).

Step 2 Perform delay compensation on the passive port of the OLT.

1. Check whether the OLT provides a passive port. If it does, go to [Step 3](#). If it does not, go to [Step 2.2](#).
2. Run the **ptp port frameid/slotid/portid disable** command to disable 1588v2 on the original slave port.
3. Check whether the passive port has been switched to the slave port. If it does, go to [Step 2.4](#).
4. Calculate the difference between the output 1 PPS data after the OLT traces the 1588v2 clock and the data measured by the GPS. Record the difference as D3.
5. Check whether D3 is within ± 20 ns. If it does, go to [Step 3](#). If it does not, go to [Step 2.6](#).
6. Run the **ptp port frameid/slotid/portid line-warp linewarptype linewarpdirection linewarpvalue** command to set the compensation value of the slave port to d, which is equal to D3.

7. Calculate the difference between the output 1 PPS data after the OLT traces the 1588v2 clock and the data measured by the GPS. Record the difference as D4.
8. Check whether D4 is within ± 20 ns. If it does, go to [Step 2.9](#). If it does not, go to [Step 2.6](#).
9. Enable 1588v2 on the original slave port and check whether this port has been switched to the status queried in [Step 2.1](#).

Step 3 Perform delay compensation on the uplink port of an ONU.

Connect a tester to the ONU and perform delay compensation on the optical fiber between the OLT and this ONU. For details, see [Step 1](#).

----End

14.4.7 1588v2 Maintenance and Diagnosis

This describes how to query the status of common alarms and how to handle the alarms.

The 1588v2 clock or time source tracing status can be verified by running the following command:

- **display clock source:** used to check whether the system reference clock source is a 1588v2 clock source and whether the clock source is functional.
- **display ptp source:** used to check whether the system reference time source is a 1588v2 time source and whether the time source is functional.
- **display ptp info:** used to check whether the time locking status and 1588v2 running data are correct.
- **display ptp timestamps:** used to query the timestamp information about the 1588v2 clock source.
- **display ptp packet-discard-reason port:** used to query the historical records of 1588v2 packet abnormality causes for a 1588v2 device port to know the abnormalities of 1588v2 packets on this port.

If any alarm or event is reported, rectify the fault according to the "Alarm and Event Reference".

14.4.8 1588v2 (based on IEEE) Reference Standards and Protocols

Document	Description
IEEE 1588-2008	Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
ITU-T G.813	Timing requirements of SDH equipment slave clocks (SEC)
ITU-T G.823	The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

Document	Description
ITU-T G.8260	Definitions and terminology for synchronization in packet networks
ITU-T G.8261	Timing and Synchronization aspects in Packet Networks
ITU-T G.8262	Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC)
G.987.3	XG-PON TC Layer Specification
G.988	ONU management and control interface specification (OMCI)

14.5 1588v2 (Based on G.8275.1)

G.8275.1 defines precision time protocol telecom profile for phase/time synchronization with full timing support from the network based on the IEEE 1588v2 precision time synchronization protocol.

1588v2 (based on G.8275.1) and 1588v2 (based on IEEE) have the same network applications. For details, see [14.4.4 1588v2 Network Application](#).

14.5.1 Basic Concept

Packet Type

G.8275.1 supports packets of types Sync, Follow_Up, Announce, Delay_Req, and Delay_Resp.

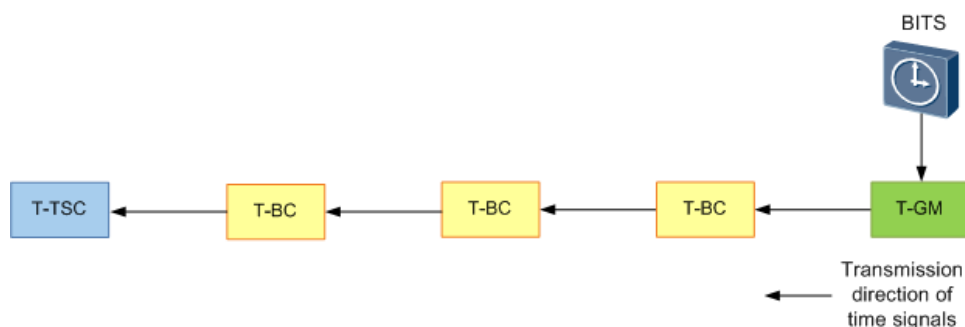
- Packets Sync, Delay_Req, Follow_Up, and Delay_Resp are used to generate and exchange timing packets that are required when the delay mechanism is used for the synchronization between the ordinary clock (OC) and boundary clock (BC).
- Message Announce is used to set up a synchronization system, that is, the information related to best master clock algorithm (BMCA) is carried in the message Announce.

Device Model

The G.8275.1-supported devices are as follows:

- Telecom grandmaster (T-GM): The clock that can only be the master one supports one or more precision time protocol (PTP) ports, but cannot trace other PTP clocks.
- Telecom boundary clock (T-BC): The boundary clock that can be the master clock and it can trace other PTP clocks.
- Telecom time slave clock (T-TSC): The clock that can only be the slave clock.

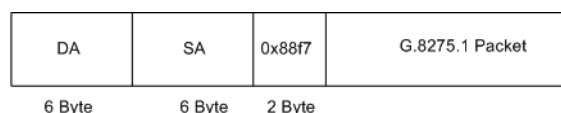
The OLT or MA5694S can serve as a T-BC device.



Packet Encapsulation Mode

G.8275.1-defined packets are encapsulated in Layer 2 multicast mode (without tags), as shown in the following figure.

In the figure, EtherType is 0x88f7. There are two types of destination multicast MAC addresses: unforwardable multicast MAC address and forwardable multicast MAC address.



14.5.2 BMCA Algorithm

The G.8275.1 profile uses best master clock algorithm (BMCA) that is different from the clock source algorithm defined in 1588v2. Differences are:

1. BMCA defines the Boolean attribute of every port as notSlave.
 - If the port attribute is notSlave, the port is in the Master state and cannot be the Slave state.
 - If the port attribute is not notSlave, the port can be in the Slave state.
2. BMCA supports multiple Grandmaster clocks and one PTP domain traces one Grandmaster clock.
3. The port supports attribute LocalPriority to set the datasets Erbest and Ebest for port status determination.
 - Message Announce sent by every clock source carries the quality parameters clock-class and clock-accuracy required for clock source selection. Attribute LocalPriority is configured and is not transmitted over a packet.
 - If several-channel time sources have the same quality parameters, such as clock-class, clock-accuracy, and priority2, attribute LocalPriority can be used to compare the time source quality.
4. Clock attribute priority2 is configurable. It is 128 by default for a T-BC device.

Other clock attributes: clockAccuracy and offsetScaledLogVariance.

- clockAccuracy: indicates the clock's precision.
- offsetScaledLogVariance: indicates the clock's stability. It is the quality of clock signals that are received by an NE. The NE obtains the value using Allan deviation.

14.5.3 Configuring 1588v2 (Based on G.8275.1)

Prerequisites

Time synchronization can be performed only after the clock has been synchronized. For example, synchronous Ethernet clock is used to implement clock synchronization.

1588v2 (based on G.8275.1) cannot be interconnected with 1588v2 (based on IEEE).

Procedure

Step 1 Run the **ptp device-type t-bc** command to set the device type to T-BC.

By default, the BC mode is used. That is, the device complies with the IEEE 1588v2 standard by default and implements 1588v2 based on the default profile. In this case, you need to manually switch the mode to T-BC to implement 1588v2 based on the ITUT G.8275.1 standard.

Step 2 Configure the global precision time protocol (PTP) function.

1. Run the **ptp t-bc** command to enter T-BC mode.
2. Run the **ptp enable** command to enable the PTP function on a device.
3. **Optional:** Run the **ptp domain** command to specify a time domain.

After the configuration, a time domain has a clock source. All devices in the time domain use the clock source.

4. **Optional:** Run the **ptp virtual-clock-id** command to configure the virtual clock ID of a device.

The clock ID uniquely identifies a clock node in a time domain.

If this parameter is not configured, its value consists of the organizational unique identifier (OUI)+product ID+last four bytes of the MAC address. The OUI is 00-25-9e, and the product ID is 40. For example, if the MAC address of the system is 00e0-fc00-a025, the corresponding default clock ID is 00259e405898a025.

Step 3 Enable PTP on a port to transmit PTP packets.

1. Run the **ptp port frameid/slotid/portid enable** command to enable PTP on an Ethernet port.

Enable 1588v2 on the ports that are required to transmit 1588v2 packets, for example, the uplink port on an OLT, user-side port on an MDU and GE port connecting the OLT and MDU.

You are not required to enable the function on the GPON port connecting the OLT and MDU.

2. Run the **ptp port frameid/slotid/portid notslave disable** command to set the port to slave state. Then, you can trace the time source of the upper-layer device through this port.

When the GE/10GE upstream port serves as the port for tracking the time source of the upper-layer device, it needs to be set to the slave state.

However, this state does not need to be set for the GE port on the user side of the OLT and MDU and for the PON port between the OLT and MDU.

Step 4 Configure the T-BC time source for time synchronization on the device.

1. Run the **ptp source** command to configure the T-BC time source.

The time source can be the T-BC time or BITS time recovered from the network-side GE/10GE/PON line. If the network does not support T-BC time synchronization, you can use the BITS time.

2. **Optional:** When the BITS time is used, run the **ptp bits** command to configure the attributes of a BITS clock source, such as the precision and class of the clock source, and the priority of the clock signal.
3. **Optional:** Configure the local priority of the time source.

Time source selection supports best master clock algorithm (BMCA) for automatic selection. You can run the **ptp port frameid/slotid/portid local-priority** command to configure the local priority of the time clock source. If several-channel time sources have the same time attributes, you can configure the local priority to compare time source quality. The smaller the **local-priority**, the higher the priority.

Step 5 Optional: Configure PTP packet parameters.

Configure parameters carried in the PTP packet, including the timestamp mode and MAC mode.

1. Run the **ptp port frameid/slotid/portid clock-step { one-step | two-step }** command to configure the step mode for PTP ports.

By default, 1588v2 packets carry timestamps in one-step mode. The 1588v2 ports identify Follow_Up packets in two-step mode in the Rx direction for communicating with other products.

2. **Optional:** Configure the encapsulation mode for PTP packets.

Run the **ptp port frameid/slotid/portid mac-egress destination-mac destination-mac-value** command to configure the MAC encapsulation mode for PTP packets to be forwarded by the port. The packets are forwarded in Layer 2 mode.

There are two types of destination multicast MAC addresses: unforwardable multicast MAC address and forwardable multicast MAC address.

Step 6 Configure asymmetric compensation parameters for optical fibers.

Run the **ptp port frameid/slotid/portid line-warp linewarptype linewarpdire linewarpvalue** command to configure asymmetric compensation parameters for optical fibers.

Asymmetric optical fibers between two devices result in time difference for data transmission and reception. During site deployment, measure and calculate the time differences in the two directions and compensate the time on the devices by configuring cable transmission deviations.

Step 7 Optional: Configure the asymmetric measurement function on a ring network.

Run the **ptp asymmetry-measure enable** command to configure the asymmetric measurement function on a ring network.

This function utilizes the BMCA algorithm in G.8275.1. When fiber disconnection occurs on the ring network, services are automatically switched to the standby link, and the time synchronization precision of the nodes on the ring network stays in the usable range. When the faulty fiber is re-connected, the devices first automatically calculate and report asymmetry on the new fiber link and then compensate for asymmetry on the NMS. After that, services are switched back to the active link.

----End

Example

An MDU connects to a 4G LTM eNodeB using a GE port. The MDU connects to the OLT using the GPON uplink port and then to the radio network controller (RNC) over the upper-layer network to carry 4G services over the access network. The 4G LTE eNodeB requires high precision time synchronization and the 1588v2 time is deployed on the network.

The parameters planned on the OLT are as follows:

- Time domain: 24
- Clock or time source input: GE uplink port 0/8/0
- Clock or time source output: GPON service port 0/3/1
- Packet encapsulation mode: MAC (default mode) (packets are forwarded in Layer 2 multicast mode)

The parameters planned on the MDU are as follows:

- Time domain: 24
- Clock or time source input: GPON uplink port 0/0/0
- Clock or time source output: GE service port 0/1/1
- Packet encapsulation mode: MAC (default mode) (packets are forwarded in Layer 2 multicast mode)

Configurations on the OLT

```
huawei(config)#ptp device-type t-bc
huawei(config)#ptp t-bc
huawei(config-t-bc)#ptp enable
huawei(config-t-bc)#ptp port 0/8/0 enable
huawei(config-t-bc)#ptp port 0/8/0 notslave disable
huawei(config-t-bc)#ptp source 0 0/8/0
```

Configurations on the MDU

```
huawei(config)#ptp device-type t-bc
huawei(config)#ptp t-bc
huawei(config-t-bc)#ptp enable
huawei(config-t-bc)#ptp port 0/1/1 enable
huawei(config-t-bc)#ptp source 0 0/0/0
```

14.5.4 1588v2 (Based on G.8275.1) Reference Standards and Protocols

Document	Description
G.8275.1	Precision time protocol telecom profile for phase/time synchronization with full timing support from the network.
G.8273.2	Timing characteristics of telecom boundary clocks and telecom time slave clocks. NOTE For details, see <i>Feature Specifications and Limitations</i> .
ITU-T G.813	Timing requirements of SDH equipment slave clocks (SEC)
ITU-T G.823	The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy
ITU-T G.8260	Definitions and terminology for synchronization in packet networks
ITU-T G.8261	Timing and Synchronization aspects in Packet Networks
ITU-T G.8262	Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC)
G.987.3	XG-PON TC Layer Specification
G.988	ONU management and control interface specification (OMCI)

14.6 1588 ACR

1588 Adaptive Clock Recover (ACR) enables a master device that supports IEEE 1588v2 to encapsulate the local system clock information into 1588v2 packets and transparently send them to peer slave devices through a third-party network. The slave devices obtain the timestamp from the 1588v2 packets and restore the clock to implement frequency synchronization between devices at both ends of a packet switched network (PSN).

14.6.1 Why Is 1588 ACR Required

Benefits

On the current 3G and 4G LTE networks, the frequency recovery modes of devices at the convergence layer are synchronous Ethernet and 1588v2. In addition, the frequency recovery is performed hop by hop. Therefore, the hardware of the entire network must support synchronous Ethernet or 1588v2, which has high requirements on the hardware of the network.

However, in the 2G mobile bearer network, enterprise private line, and narrowband service network reconstruction scenarios, the MAN cannot be

reconstructed to provide hop-by-hop clock synchronization. Therefore, it is difficult to introduce accurate clock synchronization.

How to achieve high clock synchronization accuracy with low network deployment costs?

The IEEE proposes the 1588 ACR solution, that is, the adaptive clock recovery solution. In this solution, frequency information is carried in 1588v2 packets and transparently transmitted over an intermediate network. Devices at both ends recover frequency information using 1588v2 packets to implement frequency synchronization.

Function

1588 ACR synchronizes the frequencies of the devices at the two ends of a packet switched network (PSN). Specifically, a master device supporting 1588v2 encapsulates the local system clock data into 1588v2 packets. The PSN network transparently transmits the 1588v2 packets to a slave device. The slave device obtains timestamps from the received 1588v2 packets and recovers the clock data of the master device. The PSN network does not need to support clock synchronization, or the clock of the PSN network can be a third-party clock.

1588 ACR implements frequency synchronization but not time synchronization.

14.6.2 1588 ACR Basic Concepts

The basic concepts involved in the 1588 adaptive clock recovery (ACR) feature are the same as those of 1588v2. For details, see [14.4.2 1588v2 Basic Concepts](#) of the 1588v2 feature.

14.6.2.1 1588 ACR Messages

ITU-T G.8265.1 defines seven types of 1588 adaptive clock recovery (ACR) messages. The [Table 14-9](#) describes each type of 1588 ACR messages.

Table 14-9 1588 ACR messages

Type	Classification	Message Transmit Rate (pps)	Function
Sync	Event message	1/16-128	Sync, Delay_Req, Follow_Up, and Delay_Resp messages carry timestamps for recovering clock frequencies.
Delay_Req			
Follow_Up	General message	1/16-128	
Delay_Resp			

Type	Classification	Message Transmit Rate (pps)	Function
Announce		1/16-8 Default: 1/2	Announce messages carry best master clock adaptive (BMCA) information, such as priorities and quality levels (QLs). The Announce messages are used by slave devices to select a clock source and by master devices to implement clock protection switchovers.
Signaling		None	Signaling messages are used for unicast negotiations. A slave device sends a master device a signaling message to request Sync or Announce messages. Then the master device sends a signaling message to respond to the slave device. The master and slave devices exchange Sync or Announce messages only after the negotiation between them is successful.
Management		N/A	Management messages are used for device management. ITU-T G.8265.1 has not defined how to use the management messages.

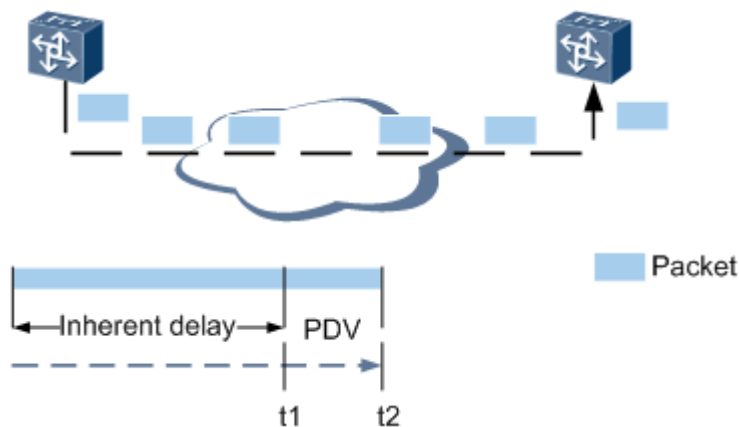
ITU-T G.8265.1 defines only transmit rate ranges for 1588v2 messages. Select a message transmit rate based on device hardware capability (crystal oscillation) and clock performance requirements (usage scenario and customer's requirements). A higher message transmit rate results in better clock recovery performance. The message transmit rate is configured on a slave device. After the configuration, the slave device sends the message transmit rate to the master device through a signaling request. Then the master device sends Sync or Announce messages to the slave device at the message transmit rate.

14.6.2.2 PDV

1588 adaptive clock recovery (ACR) is related to packet delay variation (PDV), which indicates the delay variation of the packet transmitted over a network. As shown in [Figure 14-22](#), the packet forwarding delay is calculated using the following formula: Delay = Inherent delay + PDV.

- Inherent delay: the minimum delay when packets pass through a network. The inherent delay has a fixed value, which is the sum of the physical link (for example, optical fiber) delay and the fixed circuit delay inside a device.
- PDV: Because of queue scheduling by priority and clock domain translation, a device has to store packets in buffer registers, such as first in first out (FIFO) and random access memory (RAM), for a period of time (for example, several milliseconds) before sending them. As a result, the packets arrive at a destination after a delay, at any time from t_1 to t_2 in [Figure 14-22](#). The delay is called PDV.

Figure 14-22 PDV diagram



14.6.2.3 1588 ACR Modes

Device Model

For the concept of device model, see [14.4.2.1 Device Model](#).

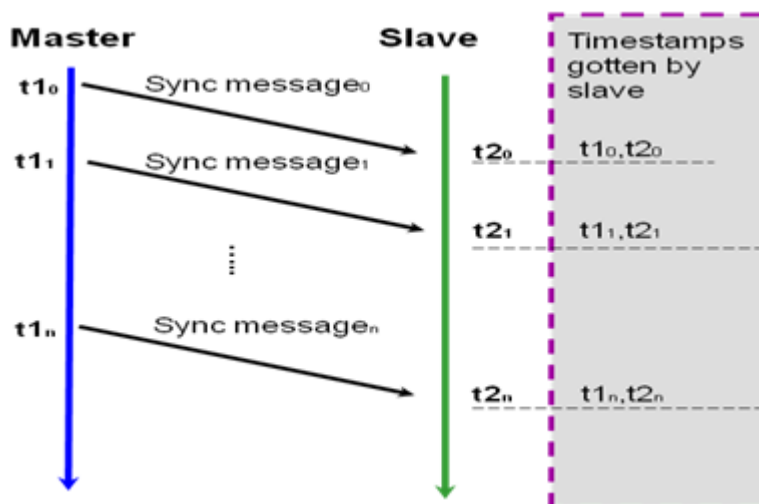
According to ITU-T G.8265.1, a slave device supporting 1588 adaptive clock recovery (ACR) supports only the slave-only ordinary clock (SOOC) model.

The 1588 ACR feature applies in end-to-end (E2E) deployment scenarios. A slave device needs to synchronize its clock frequency only with that of a master device. Therefore, the slave device does not need to support the boundary clock (BC) model.

One-way and Two-way

In one-way mode, the master device sends Sync messages to the slave device and the slave device does not send Delay_Req messages to the master device. The slave device recovers the frequency according to the timestamp contained in the Sync messages. For details, see [Figure 14-23](#).

Figure 14-23 One-way mode



The master periodically sends Sync messages to the slave. If the slave frequency is synchronized to the master frequency, then the accumulative time errors within the same time periods are the same, as long as the path delay changes are neglected.

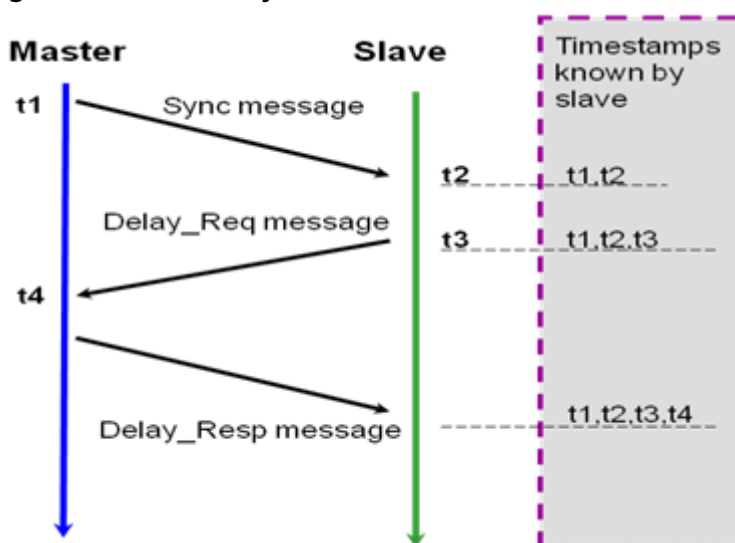
In other words, $t2_1 - t2_0 = t1_1 - t1_0$, $t2_2 - t2_1 = t1_2 - t1_1$, $t2_3 - t2_2 = t1_3 - t1_2$..., $t2_n - t2_0 = t1_n - t1_0$.

If $t2_n - t2_0$ is greater than $t1_n - t1_0$, then the slave frequency is higher than the master frequency, which means the slave frequency must be decreased. Reversely, the slave frequency must be increased.

One-way is the basic principle of 1588 ACR frequency synchronization, and can meet the synchronization requirements of 1588 ACR.

In two-way mode, packets are transmitted bidirectionally between the master and slave. The master sends Sync packets to the slave, and the slave sends Delay_Req packets to the master. The master and slave exchange 1588v2 packets to implement frequency synchronization. For details, see [Figure 14-24](#).

Figure 14-24 Two-way



1. The master sends a Sync message at t1 and carries the t1 timestamp in the Sync message.
2. The slave receives the Sync message at t2, locally generates the t2 timestamp, and extracts the t1 timestamp from the Sync message.
3. The slave sends a Delay_Req message at t3 and locally generates the t3 timestamp.
4. The master receives the Delay_Req message at t4, locally generates the t4 timestamp, and sends the Delay_Req message with the t4 timestamp back to the slave.
5. The slave extracts the t4 timestamp from the Delay_Resp message after receiving it.

"Delaysm" is the path delay in the direction from the master to the slave,
"Delaysm" is the path delay in the direction from the slave to the master, and
"Offset" is the time offset between the slave and master. All of them are variables.

$$t2-t1=Delaysm+Offset$$

$$t4-t3=Delaysm-Offset$$

When Delaysm = Delaysm, that is, when the transmit and receive links between the master and slave are symmetric, the following formula is satisfied:

$$Offset=[(t2-t1)-(t4-t3)]/2$$

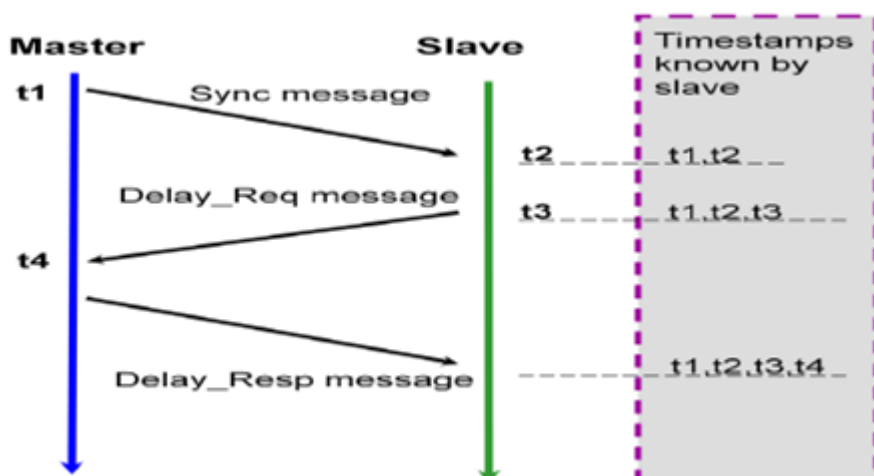
The slave can calculate the time offset between itself and the master based on the t1, t2, t3, and t4 timestamps and then corrects its own time to get synchronized with the master.

Both the one-way and two-way modes implement frequency synchronization and the one-way mode uses fewer bandwidths. According to ITU-T G.8265.1, the master must support both one-way and two-way modes. A slave is required to support either the one-way or two-way mode. The master can be connected to slaves that support the one-way or two-way mode.

One-step and Two-step

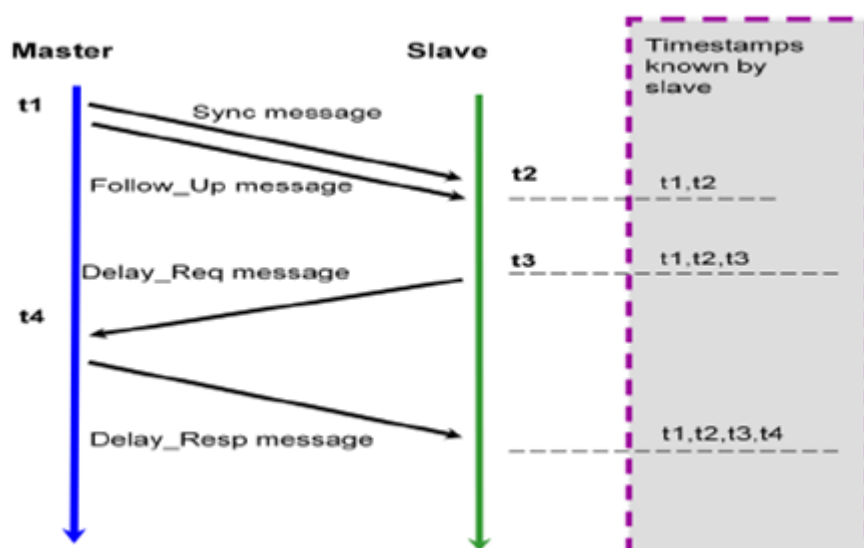
In One-step mode, there is no follow-up packet, and the Sync packet directly carries the timestamp t1, as shown in [Figure 14-25](#).

Figure 14-25 One-step mode



In two-step mode, each time a Sync packet is sent, a follow_up packet is generated to carry the timestamp t1 generated when the Sync packet is sent, as shown in [Figure 14-26](#).

Figure 14-26 Two-step mode



The two-step mode is defined by IEEE 1588v2. In this mode, a Sync message corresponds to a Follow_Up message. When a Sync message passes the timestamp point, the master device hardware generates timestamp t1. The master device does not insert timestamp t1 into the Sync message, but inserts it into the Follow_Up message. The slave device extracts timestamp t1 from the received Follow_Up message. This reduces real-time requirements for the master and slave devices.

According to ITU-T G.8265.1, a 1588 ACR master device supports either or both of the one-step and two-step modes, and a 1588 ACR slave device automatically

adapts to the mode carried in a Sync message sent from the master device. If the slave device connects to two master devices that use different 1588 ACR modes, the slave device must support the two modes.

Packet Encapsulation

According to ITU-T G.8265.1, 1588 ACR messages are encapsulated in UDP over IPv4 mode. This meets the requirements of appendix D *Transport of PTP over User Datagram Protocol over Internet Protocol Version 4* in the IEEE 1588v2 protocol.

1588 ACR messages are unicast UDP over IPv4 packets.

14.6.2.4 1588 ACR Clock Source Selection Algorithm

BMCA Algorithm

Based on the best master clock (BMC) algorithm of IEEE 1588v2, ITU-T G.8265.1 defines the best master clock adaptive (BMCA) algorithm for 1588 adaptive clock recovery (ACR). BMCA is simpler than BMC.

Table 14-10 lists BMCA parameters involved in 1588 ACR clock source selection.

Table 14-10 BMCA parameters involved in 1588 ACR clock source selection

Parameter	Description
Packet timing signal fail (PTSF)	Indicates that a Sync message is lost, an Announce message is lost, or a clock source is unavailable. The possible cause of an unavailable clock source is as follows: The packet delay variation (PDV) or the clock jitter of the master device is so large that the slave device cannot tolerate.
Quality level (QL)	Each master device carries its QL through an Announce message. The slave device preferentially traces the clock of the master device with the highest QL.
Priority	A slave device configures a local priority for each master device. If multiple master devices have the same QL, the slave device traces the clock of the master device with the highest priority.

If a slave device connects to multiple master devices and links are set up between the slave device and the master devices through unicast negotiations, the slave device receives the Announce and Sync messages sent from each master device. Then the slave device determines the best clock source as follows:

1. The slave device checks the PTSF of the clock of each master device. If PTSF occurs on a master device, the slave device does not trace the clock of the master device.

2. The slave device compares the QL of each master device and traces the clock of the master device with the highest QL.
3. If multiple master devices have the same QL, the slave device traces the clock of the master device with the highest priority.

Relationship Between 1588 ACR Clock Synchronization and Physical-Layer Clock Synchronization

The relationships between the 1588v2 clock synchronization and the physical-layer clock synchronization, including SDH synchronization and synchronous Ethernet, are as follows:

- The clock source of a 1588 ACR master device may be from an SDH or a synchronous Ethernet network.
In this scenario, the master device must convert the synchronization status message (SSM) QL of the SDH or synchronous Ethernet network to the 1588 ACR clock class. In this manner, the clock sources of the master devices can be switched over for protection. In addition, a master device sends its clock QL to the slave device through Announce messages.
- The clock output from a 1588 ACR slave device can be used as the clock input to an SDH or synchronous Ethernet network.
In this scenario, the 1588 ACR slave device recovers the clock frequency from 1588v2 messages and synchronizes the clock frequency with that of the master device. In addition, the slave device provides the recovered clock frequency to the downstream network or base station through the SDH or synchronous Ethernet network. In this case, the slave device must convert the 1588 ACR clock class to the SSM QL of the SDH and synchronous Ethernet network. In this manner, the clock sources of the slave devices can be switched over for protection.

ITU-T G.8265.1 defines the mapping between the 1588 ACR clock class and the SSM QL of the SDH or synchronous Ethernet network, as shown in the [Table 14-11](#).

Table 14-11 Mapping between the 1588v2 clock class and the SSM QL

SSM QL	ITU-T G.781 Option Synchronization layer functions	1588v2 Clock Class
0010	QL-PRC	84
0100	QL-SSU-A	90
1000	QL-SSU-B	96
1011	QL-SEC	104
1111	QL-DNU	110

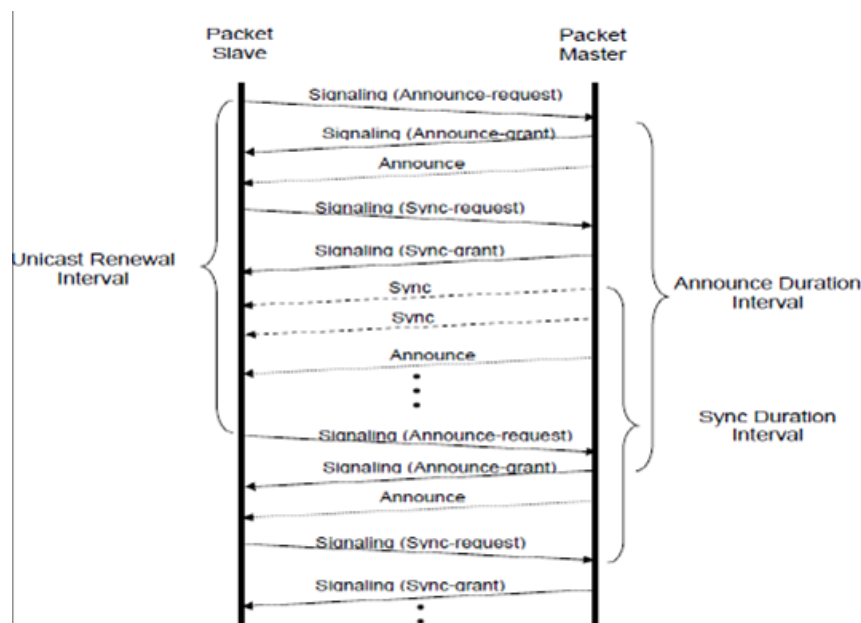
14.6.3 1588 ACR Principles

14.6.3.1 1588 ACR Unicast Negotiation

ITU-T G.8265.1 defines that a slave device communicates with a master device through a unicast negotiation. Specifically, the slave device initiates a request to the master device. The master device sends 1588v2 packets to the slave device only after authenticating the slave device.

A unicast negotiation is performed through signaling messages that carry request data. The request data includes the requested message type, message transmit rate, and duration. The duration defines the valid period of a request. The master device sends the messages requested by the slave device only within the duration. After the duration elapses, the master device stops sending the messages to the slave device. The master device will start sending messages again only after the slave device initiates a new request. [Figure 14-27](#) shows the process of a 1588 adaptive clock request (ACR) unicast negotiation.

Figure 14-27 Process of a 1588 ACR unicast negotiation



1. The slave device sends the master device a signaling message to request Announce messages. The signaling message contains the type, message transmit rate, and duration of the requested Announce messages.
2. The master device sends a signaling message to respond to the slave device, notifying the slave device that the request is permitted or rejected.
 - If the request is permitted, the master device sends Announce messages to the slave device at the message transmit rate requested by the slave device.
 - If the request is rejected, the master device does not send Announce messages to the slave device.

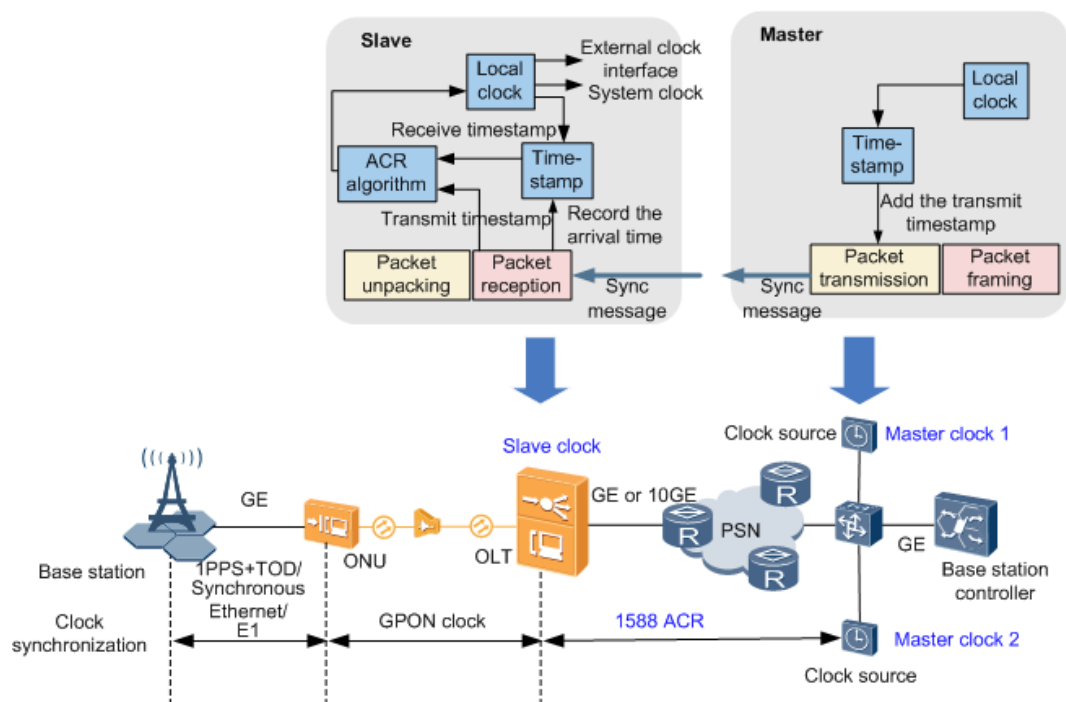
3. The slave device sends the master device a signaling message to request Sync messages. The signaling message contains the type, message transmit rate, and duration of the requested Sync messages.
4. The master device sends a signaling message to respond to the slave device, notifying the slave device that the request is permitted or rejected.
 - If the request is permitted, the master device sends Sync messages to the slave device at the message transmit rate requested by the slave device.
 - If the request is rejected, the master device does not send Sync messages to the slave device.

ITU-T G.8265.1 defines that the duration of each message can be configured on the slave device. The duration ranges from 60s to 1000s, with 300s by default. Before duration elapses, the slave device determines whether to initiate a new request. To ensure message continuity, the slave device initiates a new request after the duration elapses and before the master device stops sending messages.

14.6.3.2 1588 ACR Principles

1588 adaptive clock recovery (ACR) uses the ACR algorithm to recover the clock frequency of the transmit end from the transmit and receive timestamps carried in 1588v2 packets.

Figure 14-28 1588 ACR principles



The 1588 ACR process is as follows:

1. The slave device uses the 1588 ACR clock source selection algorithm to determine the best master clock from master devices 1 and 2 for tracing.

2. The master device providing the best master clock adds a transmit timestamp that contains the local system time to a 1588v2 packet.
3. The packet switched network (PSN) transparently transmits the 1588v2 packet to the slave device.
4. The slave device extracts the transmit timestamp from the received 1588v2 packet and adds the receive timestamp to the 1588v2 packet.
5. The slave device uses the ACR algorithm to process the transmit and receive timestamps contained in the 1588v2 packets that are received within the specified duration. Then the slave device recovers the clock frequency of the master device.

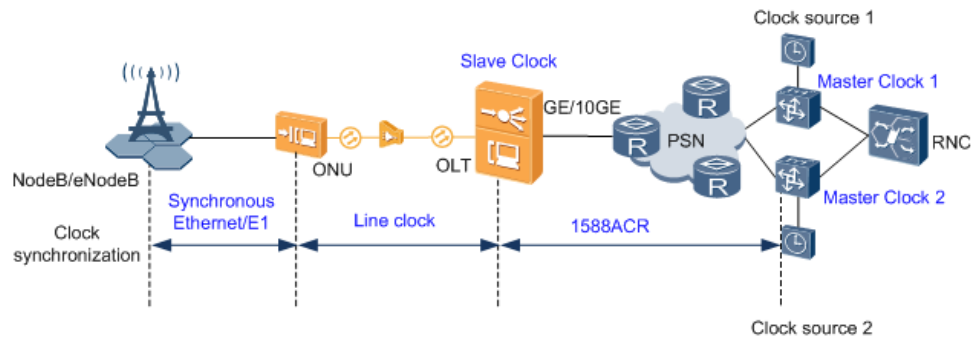
14.6.4 1588 ACR Deployment Requirements

When planning and deploying 1588 adaptive clock recovery (ACR), minimize the packet delay variation (PDV) for a stable running environment.

- Clock source protection: Deploy at least two master devices to implement clock source protection switchover.
- Locations of master and slave devices: Deploy the master and slave devices on the edge nodes connected to the intermediate network. This reduces the PDV caused by the intermediate network.
- Scale of an intermediate network: Adjust the routes of 1588 ACR messages and the locations of master and slave devices to minimize the number of forwarding hops for the 1588 ACR messages.
- Type of an intermediate network: Test and collect the PDV data on the live network to check whether 1588 ACR can be deployed on the network.
- Network traffic: Ensure that the long-term average traffic of the network is less than 80% of the maximum traffic that can be afforded by the network. Short-term network congestion and service interruptions are allowed according to G.8261.
- Quality of service (QoS) priority: Configure a high priority for 1588 ACR messages to reduce the PDV caused by packet forwarding.
- Packet loss ratio: Ensure that the packet loss ratio is not greater than 0.5%. This prevents timing signal failure.
- Message transmit rate:
 - A higher transmit rate of Sync messages results in better clock recovery performance.
 - A higher transmit rate of Announce messages results in faster fault detection and protection switchover.
 - If there are many slave devices, a higher message transmit rate results in a higher bandwidth. In this case, the one-step mode is recommended. If the bandwidth is still high after the one-step mode is used, decrease the message transmit rate.

14.6.5 1588 ACR Networking

[Figure 14-29](#) shows the 1588 adaptive clock recovery (ACR) networking.

Figure 14-29 1588 ACR networking

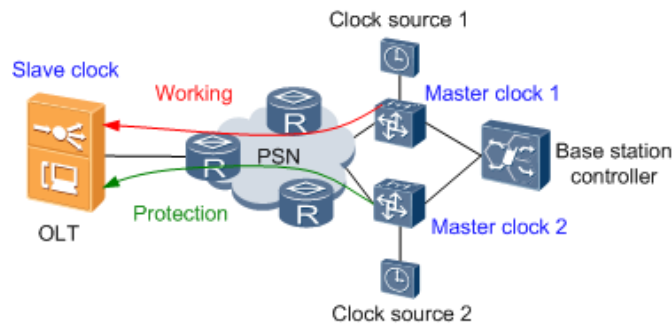
- Clock sources 1 and 2 inject clock signals to the primary and secondary master devices, respectively. The clock signals are transmitted through 1588v2 or synchronous Ethernet. The convergence layer is a third-party packet switched network (PSN) or an intermediate network that does not support 1588v2 or synchronous Ethernet. 1588 ACR is deployed on the convergence layer to ensure clock precision.
- The optical line terminal (OLT), a slave device, supports the negotiation with two master devices. According to the 1588 ACR clock source selection algorithm, the OLT traces the clock of the master device that provides better clock signals.
- The master devices convert 1588v2 or synchronous Ethernet clock packets to timestamps and encapsulate the timestamps into 1588 ACR messages. The convergence layer transparently transmits the 1588 ACR messages to the OLT. The OLT recovers the clock frequency from the received 1588 ACR messages and sends the clock frequency to the optical network unit (ONU) through line clock synchronization.
- The ONU sends the clock frequency to the base station through synchronous Ethernet, or E1 line clock synchronization.

The OLT is located at the end of a mobile bearer network or an access network. If 1588 ACR is enabled, the OLT can be used only as a slave device.

1588 ACR Protection Networking

If a clock source is faulty, services are interrupted. Therefore, the clock source must be protected. For the 1588 ACR feature, deploy a secondary master device to provide a secondary clock source. [Figure 14-30](#) shows the 1588 ACR protection networking.

Figure 14-30 1588 ACR protection networking



In the preceding networking, if the primary master device is faulty, the slave device automatically traces the clock of the secondary master device. After the primary master device recovers, the slave device automatically traces the clock of the primary master device.

14.6.6 Configuring 1588 ACR

This section describes how to configure 1588 adaptive clock recovery (ACR) to implement the end to end (E2E) frequency synchronization across a third-party network.

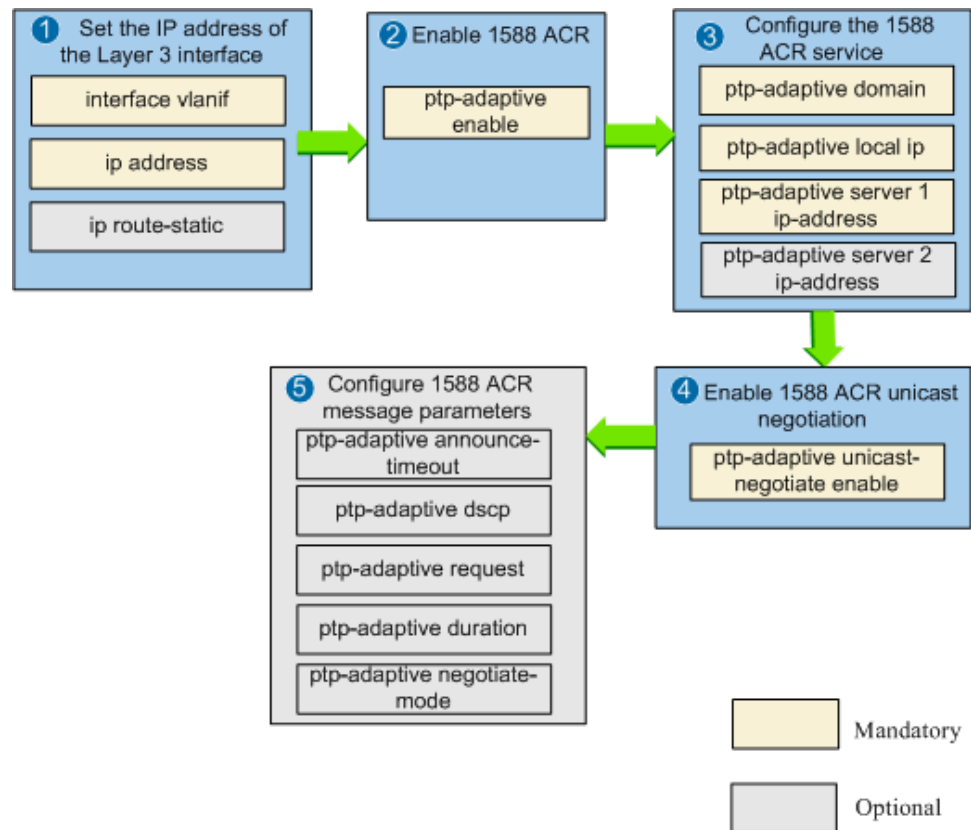
Prerequisites

- The optical line terminal (OLT) has been installed and deployed.
- The master device is functional.
- The route on the third-party network is reachable.

Configuration Process

[Figure 14-31](#) shows the 1588 ACR configuration process.

Figure 14-31 1588 ACR configuration process



Procedure

Step 1 Set the IP address of the Layer 3 interface.

1. Run the **interface vlanif** command to create a VLANIF interface and enter the VLANIF mode.
2. Run the **ip address** command to set the IP address of the VLAN interface.

NOTE

Ensure that the IP address of the VLAN interface and that of the master device port are in the same network segment.

3. **Optional:** Run the **ip route-static** command to configure a route from the local IP address of the master device to the IP address of the VLAN Layer 3 interface on the slave device.

Perform this step if the local IP address of the master device port and that of the VLAN Layer 3 interface on the slave device are in different network segments.

Step 2 Run the **ptp-adaptive enable** command to enable 1588 ACR.

Step 3 Configure the 1588 ACR service.

1. Run the **ptp-adaptive domain** command to configure the time domain for the 1588 ACR devices.

 NOTE

Clock synchronization can be performed on the slave device only if the master and slave devices are in the same time domain.

2. Run the **ptp-adaptive local-ip** command to configure the local IP address of the 1588 ACR slave device.

1588 ACR messages are Layer 3 unicast IP packets. Therefore, a fixed IP address is required between the master and slave devices. This IP address is generally a loopback address or the IP address of an outbound port. In this step, the local IP address is the IP address of the VLAN interface set in [Step 1.2](#).

3. Run the **ptp-adaptive server 1 ip-address** command to set the IP address of 1588 ACR master device server 1.

 NOTE

In this step, the IP address is the local IP address of the master device.

4. **Optional:** Run the **ptp-adaptive server 2 ip-address** command to set the IP address of master device 2.

Perform this step if a protection switchover is required for master devices.

 NOTE

If a slave device connects to two master devices, the slave device traces the clock of the master device with a higher quality level and priority based on the 1588 ACR clock source selection algorithm. If the primary master device is faulty, the slave device automatically traces the clock of the secondary master device based on the 1588 ACR clock source selection algorithm.

Step 4 Run the **ptp-adaptive unicast-negotiate enable** command to enable 1588 ACR unicast negotiation.

Step 5 Optional: Configure 1588 ACR message parameters.

- Run the **ptp-adaptive announce-timeout** command to configure the maximum number of times that Announce messages are not received within a packet transmit period. The default number is 3.
- Run the **ptp-adaptive dscp** command to configure the priority for processing forwarded 1588 ACR messages. The default priority is 56.

 NOTE

This parameter determines the 1588 ACR message forwarding priority. A higher priority results in a smaller network jitter for the 1588 ACR messages. Accordingly, the recovered clock performance is better. Otherwise, the recovered clock performance is not so good.

- Run the **ptp-adaptive request interval** command to configure the interval requested by the slave device at which the master device sends 1588 ACR Announce, Sync, or Delay_Req messages to the slave device.

 NOTE

- Default interval for Announce messages: 11
- Default interval for Sync messages: 3
- Default interval for Delay_Req messages: 3

The minimum message transmit rate required by the frequency recovered through 1588 ACR varies according to network condition. A larger packet transmit rate results in better recovered frequency performance. However, this requires more system resources and bandwidths. Therefore, configure a proper value to balance the frequency performance, network resources, and bandwidths.

- Run the **ptp-adaptive duration** command to configure the interval at which a re-negotiation is performed between the master and slave devices. The default time is 300s.

 NOTE

The duration for each type of packet is separately configured. Therefore, before a duration elapses, the slave device determines whether to initiate a new request based on site requirements. To ensure message continuity, the slave device initiates a new request after the duration elapses and before the master device stops sending messages.

- Run the **ptp-adaptive negotiate-mode** command to configure the 1588 ACR negotiation mode to one-way or two-way. The default mode is one-way.

 NOTE

The frequency recovered in two-way mode is better than that recovered in one-way mode, but this mode requires more bandwidths.

----End

Result

After the **display ptp-adaptive all** command is executed, **Ptp adaptive state** is **Enable**, **Current state** is **Slave**, and **Nego-state** is **Success**.

If an error occurs in clock tracing, rectify the fault based on the reported clock alarm or event.

Example

The following configurations are used as an example to configure 1588 ACR: An OLT connects to a third-party network through GE upstream transmission and then to a radio network controller (RNC). This implements wireless service carried over a base station network. The third-party network does not support 1588v2. Therefore, 1588 ACR is deployed on the network.

Data plan on the OLT:

- Time domain: 1
- VLAN ID: 2
- IP address of the VLAN interface: 10.10.11.2
- IP address of 1588 ACR master device server 1: 10.10.11.10

OLT configuration

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.11.2 24
```

```
huawei(config-if-vlanif2)#quit
huawei(config)#ptp-adaptive enable
huawei(config)#ptp-adaptive domain 1
huawei(config)#ptp-adaptive local-ip 10.10.11.2
huawei(config)#ptp-adaptive server 1 ip-address 10.10.11.10
huawei(config)#ptp-adaptive unicast-negotiate enable
```

14.6.7 1588 ACR Maintenance and Diagnosis

1. If any alarms or events is reported, rectify faults using the alarm or event troubleshooting methods.
2. Run the **display ptp-adaptive all** command to query the 1588 ACR running status. Rectify faults, if any.
3. Run the **display ptp-adaptive server** command to query the statistics of the collected transmit and receive 1588 ACR messages. Rectify faults, if any.
4. Run the **display ptp-adaptive all** command to query 1588 ACR configurations. Ensure that 1588 ACR is enabled, the IP address of the 1588 ACR server is correct, and 1588 ACR attributes are correct.
5. Check clock hardware status. Ensure that the upstream interface board, physical ports and links, and the clock daughter board are functional. Specifically, no board or port alarm is reported. A clock daughter board fault can be queried through alarms or commands.
6. Run the **display ptp-adaptive all** command to check the status and configuration of the Layer 3 interface.
7. Run the **display ip routing-table** command to check whether the master and slave routes are reachable.

14.6.8 1588 ACR Standard and Protocol Compliance

Standard or Protocol	Description
IEEE 1588-2008	Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
ITU-T G.8260	Definitions and terminology for synchronization in packet networks
ITU-T G.8261	Timing and Synchronization aspects in Packet Networks
ITU-T G.8262	Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC)
ITU-T G.8265	Architecture and requirements for packet based frequency delivery
ITU-T G.8265.1	Precision time protocol telecom profile for frequency synchronization

14.6.9 Remote 1588 Packet Capture

If a failure occurs during 1588v2 protocol interconnection, remote 1588v2 packet capture facilitates fault locating so that customers can quickly rectify a fault. This feature supports capture of 1588v2 (IEEE-based), 1588v2 (G.8275.1-based), and 1588 ACR packets.

Context

The remotely captured 1588 packets are first buffered on the control board, and uploaded to the file server as files, and then opened by using the tool.

Procedure

- Step 1** Run the **capture 1588v2** command to enable 1588v2 packet capture.
If 1588 ACR packets are captured, run the **capture 1588acr** command to enable 1588 ACR packet capture.
- Step 2** Run the **file-server auto-backup debug** command to configure the backup server.
- Step 3** Run the **capture start** command to start packet capture.
- Step 4** During packet capture, run the **capture stop** command to stop it. Then, the device uploads packets to the server.
- Step 5** Once packet capture stops, run the **undo capture 1588v2** or **undo capture 1588acr** command to disable 1588 packet capture.

----End

Example

To capture 1588v2 (IEEE-based) packets, do as follows:

```
huawei(config)#diagnose
huawei(diagnose)%%capture 1588v2 0/2/0
huawei(diagnose)%%file-server auto-backup debug primary 192.168.1.20 sftp
huawei(diagnose)%%capture start -c 10000 //10000 indicates the number of captured packets.
huawei(diagnose)%%undo capture 1588v2 0/2/0
```

14.7 NTP

The Network Time Protocol (NTP) is used to synchronize the time between the distributed time server and the client.

NOTE

You are advised to enable NTP for accurate system time.

14.7.1 NTP Introduction

Definition

The Network Time Protocol (NTP) is an application layer protocol in the TCP/IP protocol suite. NTP is used to synchronize the time between the distributed time

server and the client. The implementation of NTP is based on IP and UDP. NTP involves the Time Protocol and the ICMP Timestamp Message, with special design on accuracy and robustness.

Purpose

NTP defines the accurate time in an entire network.

Because the network topology is complicated, the clock synchronization among all the devices in the entire network becomes more critical. The objective of NTP is to synchronize the clocks of all the devices on a network which have clocks. This helps to keep time consistency among all the devices in the network. Therefore, the device can offer various applications based on the clock synchronization. For example, before analyzing logs collected from different devices for network management, you must ensure that the time on the logs is from synchronized clocks.

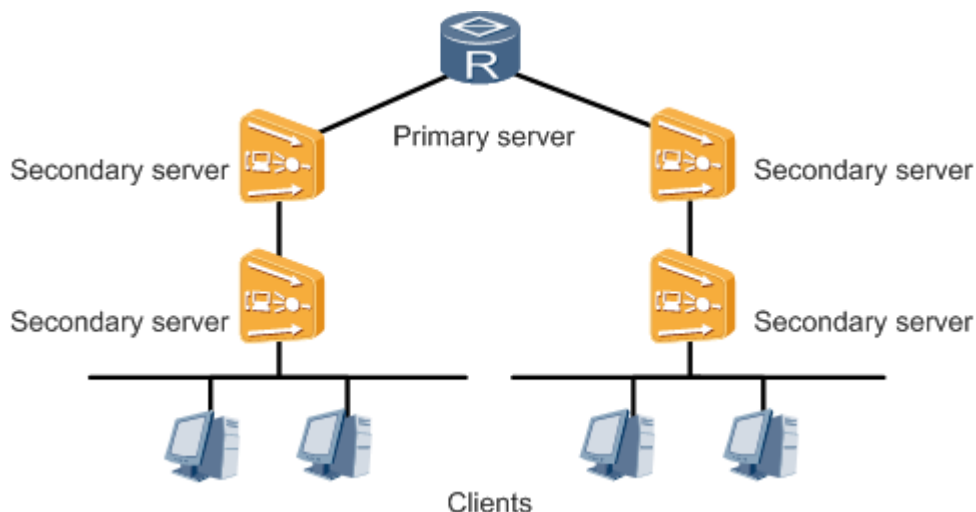
The MA5800 supports the NTP feature to guarantee that the clocks of all the devices in a network are consistent.

14.7.2 NTP Principle

14.7.2.1 NTP Network Architecture

As shown in the followed figure, the networking of NTP is composed of a primary time server, secondary time servers, clients, and interconnecting transmission paths.

Figure 14-32 NTP network architecture



- A primary time server directly synchronizes its clock with a primary reference source which is usually a radio clock or Global Positioning System (GPS).
- A secondary time server synchronizes its clock with the clock of the primary time server or other secondary time servers on the network, and transmits the time information to clients on the network through NTP.

Under normal circumstances, primary and secondary time servers in a synchronization subnet assume a hierarchical-master-slave structure, with the primary server at the top and the secondary servers at successive stratum levels near leaf nodes. Secondary time servers at stratum levels further from the master time server will get less accurate clock information.

14.7.2.2 NTP Operating Mode

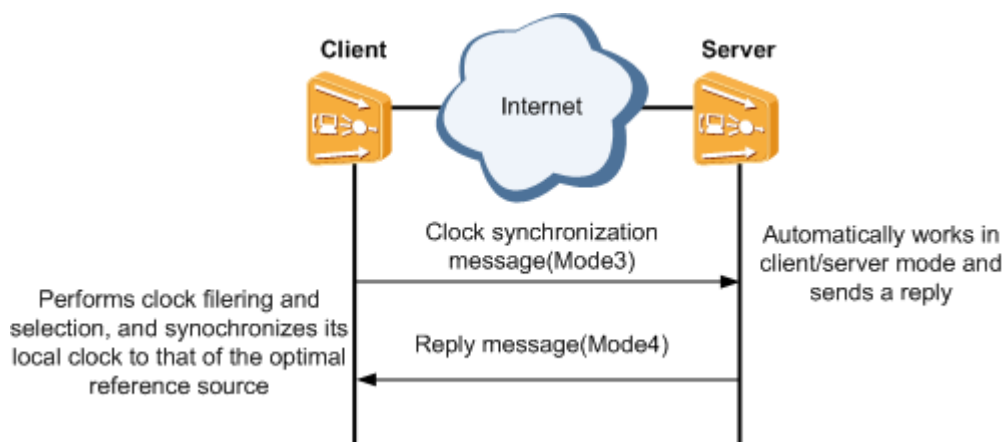
In actual application, you need to select a proper NTP operating mode based on the network deployment to meet various clock synchronization requirements. The operating modes of NTP are classified into Unicast Client/Server Mode, peer mode, broadcast mode, multicast mode and anycast mode.

Unicast Client/Server Mode

- The host that functions as a client sends packets to the server periodically. The value of the Mode field in a packet is set to 3. This indicates that the packet is sent by a client, without considering whether the server is reachable and which stratum the server is on. Usually, the host operating in client mode is a workstation on a specified network, which synchronizes its clocks with the clock on the server but does not alter the clock of the server.
- The host that functions as a server receives the packets from the client and sends response packets. The value of the Mode field in a response packet is set to 4. This indicates that the packet is sent by a server. Usually, the host operating in server mode is a time server on a network, which provides synchronization information for the clients but does not alter its own clock.

During and after the restart, the host operating in client mode periodically sends NTP request messages to the host operating in server mode. After receiving the NTP request message, the server swaps the position of destination IP address and source IP address, and the source port number and destination port number, fills in the necessary information, and sends the message to the client. The server does not need to retain state information when the client sends the request message. The client freely adjusts the interval for sending NTP request messages according to the local conditions.

Figure 14-33 Unicast Client/Server Mode



Peer Mode

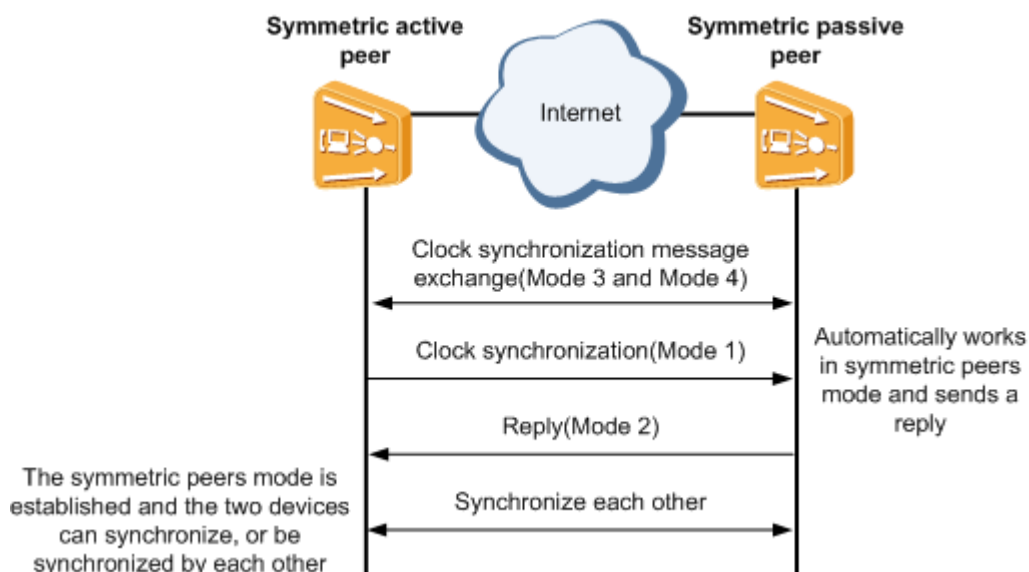
In this mode, the active peer and the passive peer can be synchronized with each other. To be specific, the higher stratum (lower level) peer is synchronized with the lower stratum (higher level) peer. The active and passive peers firstly exchange NTP packets whose values of Mode fields are 3 (sent by the client) and NTP packets whose values are 4 (sent by the server).

- **Active peer:** A host that functions as an active peer sends packets periodically. The value of the Mode field in a packet is set to 1. This indicates that the packet is sent by an active peer, without considering whether its peer is reachable and which stratum its peer is on. The active peer can provide time information about the local clock for its peer, or synchronize the time information about the local clock based on that of the peer clock.
- **Passive peer:** A host that functions as a passive peer receives packets from the active peer and sends response packets. The value of the Mode field in a response packet is set to 2. This indicates that the packet is sent by a passive peer. The passive peer can provide time information about the local clock for its peer, or synchronize the time information about the local clock based on that of the peer clock.
- **Prerequisites for a host to function as a passive peer:** The packets received by the local host are sent by an active peer. The number of the stratum that the active peer is on must be less than or equal to the number of the stratum that the local host is on. In addition, the routes between the local host and the active peer must be reachable.

NOTE

The host operating in passive mode is at the lower stratum in the synchronization subnet. You do not need to obtain information about the peer in advance because the connection between peers is not set up and status variables are not configured unless the passive host receives NTP messages from the peer.

Figure 14-34 Peer mode

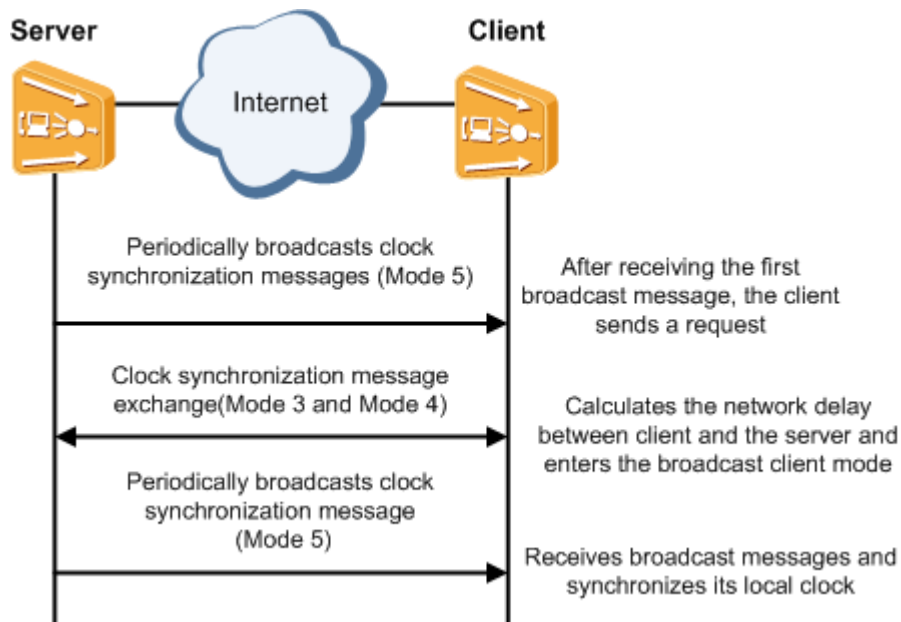


Broadcast Mode

- A host that runs in broadcast mode sends clock synchronization packets to the broadcast address 255.255.255.255 periodically. The value of the Mode field in a packet is set to 5. This indicates that the packet is sent by a host that runs in broadcast mode, without considering whether its peer is reachable and which stratum its peer is on. The host running in broadcast mode is usually a time server running high-speed broadcast media on the network, which provides synchronization information for all of its peers but does not alter the clock of its own.
- The client listens to the broadcast packets sent from the server. When the client receives the first broadcast packet, the client and server exchange NTP packets whose values of Mode fields are 3 (sent by the client) and the NTP packets whose values of Mode fields are 4 (sent by the server). In this process, the client enables the server/client mode for a short time to exchange information with the remote server. This allows the client to obtain the network delay between the client and the server. Then, the client returns the broadcast mode, and continues to sense the incoming broadcast packets to synchronize the local clock.

The broadcast mode is applied to the high speed network that has multiple workstations and does not require high accuracy. In a typical scenario, one or more time servers on the network periodically send broadcast packets to the workstations. The delay of packet transmission in a LAN is at the milliseconds level.

Figure 14-35 Broadcast mode



Multicast Mode

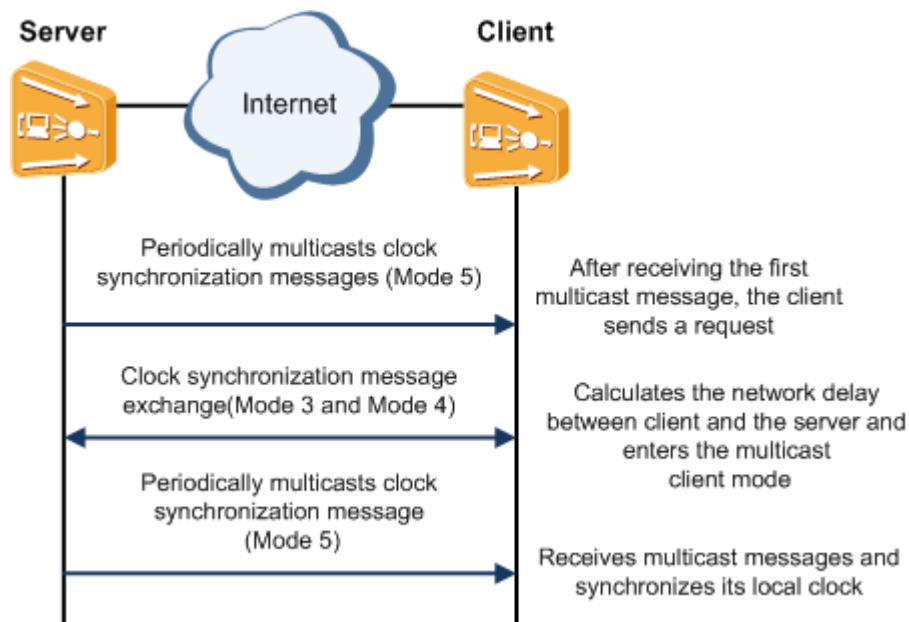
- A server running in multicast mode sends clock synchronization packets to a multicast address periodically. The value of the Mode field in a packet is set to 5. This indicates that the packet is sent by a host that runs in multicast mode.

The host running in multicast mode is usually a time server running high-speed broadcast media on the network, which provides synchronization information for all of its peers but does not alter the clock of its own.

- The client listens to the multicast packets from the server. When the client receives the first multicast packet, the client and the server exchange NTP packets whose values of Mode fields are 3 (sent by the client) and the NTP packets whose values of Mode fields are 4 (sent by the server). In this process, the client enables the server/client mode for a short time to exchange information with the remote server. This allows the client to obtain the network delay between the client and the server. Then, the client returns the multicast mode, and continues to sense the incoming multicast packets to synchronize the local clock.

Multicast mode is useful when there are large numbers of clients distributed in a network. This normally results in large number of NTP packets in the network. In the multicast mode, a single NTP multicast packet can potentially reach all the clients in the network and thus reduce the control traffic on the network.

Figure 14-36 Multicast mode

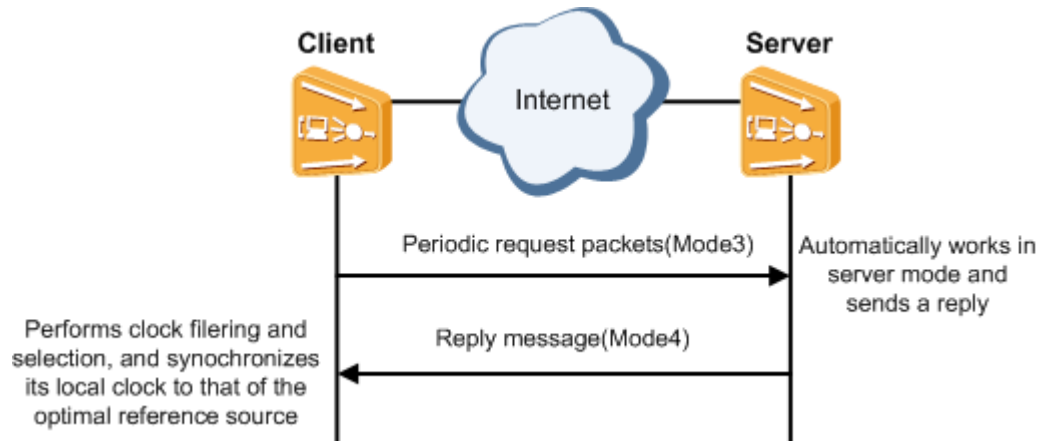


Manycast Mode

In multicast mode, the client first searches for a server by continuously sending NTP packets whose destination IP address is the specified IPv4/IPv6 multicast address. The Mode field in the packets is set to 3 (client mode), and the TTLs of the packets increases from 1. A designated NTP manycast server listens for packets with that address. If a server receives the packets from the client, it returns an ordinary server (mode 4) packet to the client. If client receives the packets from the server, temporary C/S connection between them is established. After a certain period of time, the client stops the search process and select the best NTP server among all connections. Other connections not selected will be aged out.

Manycast mode is applied to a small set of servers scattered over the network. Clients can discover and synchronize to the closest manycast server. Manycast can especially be used where the identity of the server is not fixed and a change of server does not require reconfiguration of all the clients in the network.

Figure 14-37 Manycast mode



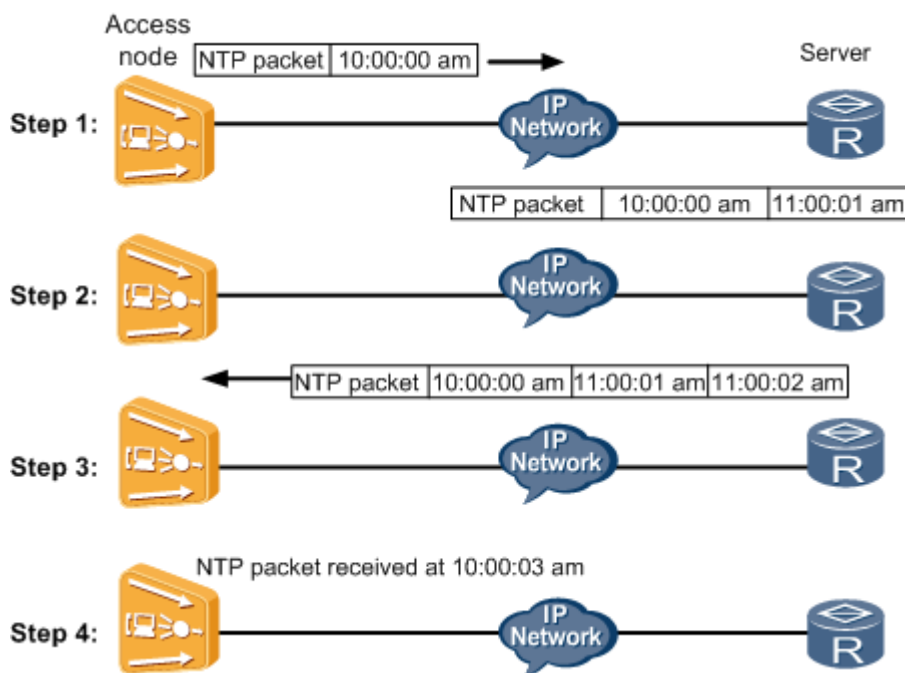
Kiss-o'-Death (KOD)

KOD packets provide useful information to a client and are used for status reporting and access control. When KOD is enabled at the server, the server may send packets with kiss codes DENY and RATE to the client.

- When the client receives packet with kiss code DENY, the client demobilizes any associations with that server and stops sending packets to that server.
- When the client receives packet with kiss code RATE, the client immediately reduces its polling interval to that server and continues to reduce it each time it receives a RATE kiss code.

14.7.2.3 NTP Working Principle

As shown in [Figure 14-38](#), the MA5800 serves as the NTP client and the router serves as the NTP server. The MA5800 uses the time of the router as the reference and synchronizes its time with the router through NTP.

Figure 14-38 Operating principle of NTP

1. The MA5800 sends an NTP packet to the router. This packet contains the timestamp when it leaves the MA5800. Assume that the timestamp is 10:00:00 am (T1).
2. When the NTP packet arrives at the router, the router adds its timestamp to the packet. Assume that the timestamp is 11:00:01 am (T2).
3. When the NTP packet leaves the router, the router adds another timestamp to the packet. Assume that the timestamp is 11:00:02 am (T3).
4. When the MA5800 receives the response packet, it adds a new timestamp to the packet. Assume that the timestamp is 10:00:03 am (T4).

Now, the MA5800 has sufficient information to calculate two important parameters:

- The delay for a round trip of the NTP packet = $(T4 - T1) - (T3 - T2)$.
- Offset between the MA5800 and the router = $((T2 - T1) - (T4 - T3)) / 2$

In this way, the MA5800 can set its clock according to the information and thus keeps its clock synchronized with that of the router.

14.7.2.4 NTP Security Mechanism

When a time server in the subnet is faulty or data is maliciously modified or destroyed, timekeeping on other time servers in the subnet should not be affected. To meet this requirement, NTP provides two security mechanisms: access right and NTP authentication to guarantee the network security.

Access Right Control

You can run the **ntp-service access** command to set the right to access the NTP service of the MA5800 so as to protect the NTP service.

The MA5800 supports five levels of access rights, as shown in the following table.

Table 14-12 NTP access rights supported by the MA5800.

Access Right	Description
peer	Indicates the minimum access right. The remote end can perform time requests and control queries for the local NTP service. The local clock can also be synchronized with the clock of the remote server.
server	Indicates that the remote end can perform time requests and control queries for the local NTP service. The local clock, however, cannot be synchronized with the clock of the remote server.
synchronization	Indicates that the remote end can perform time requests only for the local NTP service.
query	Indicates the maximum access right. The remote end can perform control queries only for the local NTP service.
limited	Controls the incoming packet rate and kiss code is sent when KoD is enabled.

NTP Authentication

The NTP authentication can be used on security-critical networks. If the NTP authentication is enabled, the MA5800 uses MD5-algorithm or HMAC-SHA256-algorithm keys to authenticate users who access the NTP service. You are recommended to use the HMAC-SHA256 algorithm to improve security. The NTP authentication must be configured on both the server and the client.

The key on the client must match the one on the server for the user to pass the NTP authentication.

The process for configuring the NTP authentication on the server and the client is as follows:

1. Enable the NTP authentication.
2. Configure the NTP authentication key.
3. Declare that the NTP authentication key is trustworthy.

 NOTE

- The client is synchronized to only the server that provides the reliable key. If the key provided by the server is unreliable, the client is not synchronized to the server.
- When the client is configured with the NTP authentication, if only the server is configured with same authentication key as the client, the client can pass the authentication. Here, the server does not need to enable the NTP authentication function or declare that the key is reliable.

14.7.3 Configuring the Network Time

Configure the NTP protocol to keep the time of all devices on the network synchronized, so that the MA5800 implements various service applications based on universal time, such as the network management system and the network accounting system.

Context

Introduction to the NTP Protocol:

- The Network Time Protocol (NTP) is an application layer protocol defined in RFC 1305, which is used to synchronize the times of the distributed time server and the client. The RFC defines the structures, arithmetics, entities and protocols used in the implementation of NTP.
- NTP is developed from the time protocol and the ICMP timestamp message protocol, with special design on the aspects of accuracy and robustness.
- NTP runs over UDP with port number as 123.
- Any local system that runs NTP can be time synchronized by other clock sources, and also act as a clock source to synchronize other clocks. In addition, mutual synchronization can be done through NTP packets exchanges.

NTP is applied to the following situations where all the clocks of hosts or routers in a network need to be consistent:

- In the network management, an analysis of log or debugging information collected from different routers needs time for reference.
- The charging system requires the clocks of all devices to be consistent.
- Completing certain functions, for example, timing restart of all the routers in a network requires the clocks of all the routers be consistent.
- When several systems work together on the same complicate event, they have to take the same clock for reference to ensure a correct implementation order.
- Incremental backup between the backup server and clients requires clocks on them be synchronized.

When all the devices on a network need to be synchronized, it is almost impossible for an administrator to manually change the system clock by using a command line. This is because the work load is heavy and clock accuracy cannot be ensured. NTP can quickly synchronize the clocks of network devices and ensure their precision.

There are four NTP modes: server/client, peer, broadcast and multicast modes. The MA5800 supports all these modes.

Default Configuration

Table 14-13 provides the default configuration for NTP.

Table 14-13 Default configuration for NTP

Parameter	Default Value
NTP-service authentication function	Disable
NTP-service authentication key	None
Maximum NTP sessions	100
Clock stratum	16

14.7.3.1 (Optional) Configuring NTP Authentication

This topic describes how to configure NTP authentication to improve the network security and prevent unauthorized users from modifying the clock.

Prerequisites

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the device are configured so that the server and the client are reachable to each other at the network layer.

Context

In certain networks that have strict requirements on security, enable NTP authentication when running the NTP protocol. Configuring NTP authentication is classified into configuring NTP authentication on the client and configuring NTP authentication on the server.

Precaution

- If NTP authentication is not enabled on the client, the client can synchronize with the server, regardless of whether NTP authentication is enabled on the server.
- If NTP authentication is enabled, a reliable key should be configured.
- The configuration of the server must be the same as that of the client.
- When NTP authentication is enabled on the client, the client can pass the authentication if the server is configured with the same key as that of the client. In this case, you do not need to enable NTP authentication on the server or declare that the key is reliable.
- The client is synchronized to only the server that provides the reliable key. If the key provided by the server is unreliable, the client is not synchronized to the server.

- The flow of configuring NTP authentication is as follows: start->enable NTP authentication->configure the reliable NTP authentication key->declare the reliable key->end.

Procedure

- Step 1** Run the **ntp-service authentication enable** command to enable NTP authentication.
- Step 2** Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
- Step 3** Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.

----End

Example

To enable NTP authentication, set the NTP authentication key as **aNiceKey** with the key number 42, and then define key 42 as a reliable key, do as follows:

```
huawei(config)#ntp-service authentication enable
huawei(config)#ntp-service authentication-keyid 42 authentication-mode md5 plain password123
huawei(config)#ntp-service reliable authentication-keyid 42
```

14.7.3.2 Configuring the NTP Broadcast Mode

This topic describes how to configure the MA5800 for clock synchronization in the NTP broadcast mode. After the configuration is completed, the server periodically broadcasts clock synchronization packets through a specified port, and the client listens to the broadcast packets sent from the server and synchronizes the local clock according to the received broadcast packets.

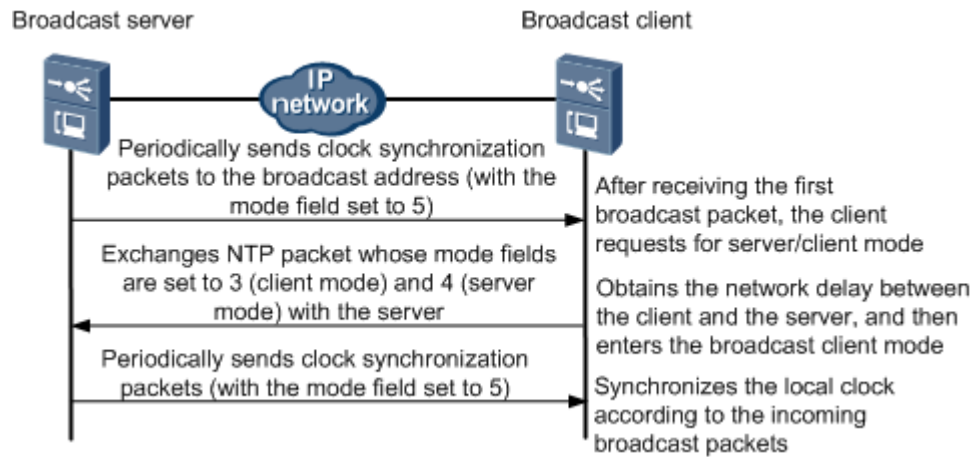
Prerequisites

Before configuring the NTP broadcast mode, make sure that the network interface and the routing protocol of the MA5800 are configured so that the server and the client are reachable to each other at the network layer.

Context

In the broadcast mode, the server periodically sends clock synchronization packets to the broadcast address, with the mode field set to 5 (indicating the broadcast mode). The client listens to the broadcast packets sent from the server. After receiving the first broadcast packet, the client exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server to estimate the network delay between the client and the server. The client then enters the broadcast client mode, continues to listen to the incoming broadcast packets, and synchronizes the local time according to the incoming broadcast packets, as shown in [Figure 14-39](#).

Figure 14-39 NTP broadcast mode



Precaution

1. In the broadcast mode, you should configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be higher than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- Configure the NTP broadcast server host.
 - a. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
 - b. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

- i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
- c. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.

- iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
- iv. Configure an IP address for the VLAN interface based on the actual requirement.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
- d. Run the **ntp-service broadcast-server** command to configure the NTP broadcast server mode of the host, and specify the key ID for the server to send packets to the client.
- e. Run the **display ntp-service status** command to verify the configuration result.
- Configure the NTP broadcast client host.
 - a. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

 - i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
 - b. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
 - iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
 - iv. Configure an IP address for the VLAN interface based on the actual requirement.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
 - c. Run the **ntp-service broadcast-client** command to configure a host as the NTP broadcast client.

----End

Example

(IPv4) Assume the following configurations: MA5800_S uses the local clock as the master NTP clock on stratum 2 and works in the NTP broadcast mode,

broadcasting clock synchronization packets periodically through IP address 10.10.10.10/24 of the Layer 3 interface of VLAN 2, and MA5800_C functions as the NTP client, listening to the broadcast packets sent from the server through IP address 10.10.10.20/24 of the Layer 3 interface of VLAN 2 and synchronizing with the clock on the broadcast server. To perform these configurations, do as follows:

1. On MA5800_S:

```
huawei(config)#undo ntp-service server disable
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service broadcast-server
huawei(config-if-vlanif2)#quit
```
2. On MA5800_C:

```
huawei(config)#undo ntp-service server disable
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service broadcast-client
huawei(config-if-vlanif2)#quit
```

14.7.3.3 Configuring the NTP Multicast Mode

This topic describes how to configure the MA5800 for clock synchronization in the NTP multicast mode. After the configuration is completed, the server periodically multicasts clock synchronization packets through a specified port, and the client listens to the multicast packets sent from the server and synchronizes the local clock according to the received multicast packets.

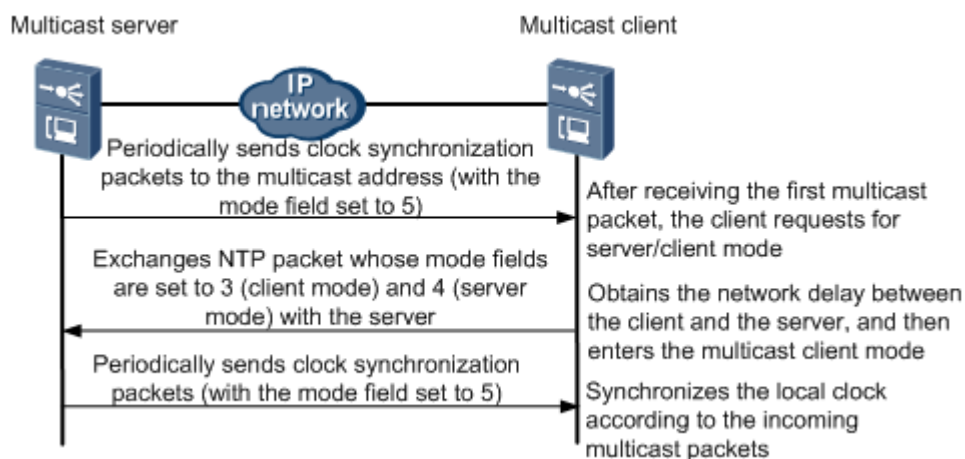
Prerequisites

Before configuring the NTP multicast mode, make sure that the network interface and the routing protocol of the MA5800 are configured so that the server and the client are reachable to each other at the network layer.

Context

In the multicast mode, the server periodically sends clock synchronization packets to the multicast address configured by the user. The default NTP multicast address 224.0.1.1 is used if the multicast address is not configured. The mode field of clock synchronization packet is set to 5 (multicast mode). The client listens to the multicast packets sent from the server. After receiving the first multicast packet, the client exchanges NTP packet whose mode fields are set to 3 (client mode) and 4 (server mode) with the server to estimate the network delay between the client and the server. The client then enters the multicast client mode, continues to listen to the incoming multicast packets, and synchronizes the local clock according to the incoming multicast packets, as shown in [Figure 14-40](#).

Figure 14-40 NTP multicast mode



Precaution

1. In the multicast mode, you should configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be higher than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- Configure the NTP multicast server host.
 - a. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
 - b. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

- i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
- c. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.

- iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
- iv. Configure the IP address of the VLAN interface.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
- d. Run the **ntp-service multicast-server** command to configure the NTP multicast server mode of the host, and specify the key ID for the server to send packets to the client.
- Configure the NTP multicast client host.
 - a. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

 - i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
 - b. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
 - iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
 - iv. Configure the IP address of the VLAN interface.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
 - c. Run the **ntp-service multicast-client** command to configure a host as the NTP multicast client.

----End

Example

(IPv4) Assume the following configurations: MA5800_S uses the local clock as the master NTP clock on stratum 2 and works in the NTP multicast mode, multicasting clock synchronization packets periodically through IP address 10.10.10.10/24 of the Layer 3 interface of VLAN 2, and MA5800_C functions as the NTP client, listening to the multicast packets sent from the server through IP address 10.10.10.20/24 of the Layer 3 interface of VLAN 2 and synchronizing with the clock on the multicast server. To perform these configurations, do as follows:

1. On MA5800_S:

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service multicast-server
huawei(config-if-vlanif2)#quit
```
2. On MA5800_C:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service multicast-client
huawei(config-if-vlanif2)#quit
```

14.7.3.4 Configuring the Unicast NTP Client

This topic describes how to configure the MA5800 as the NTP client to synchronize with the NTP server in the network.

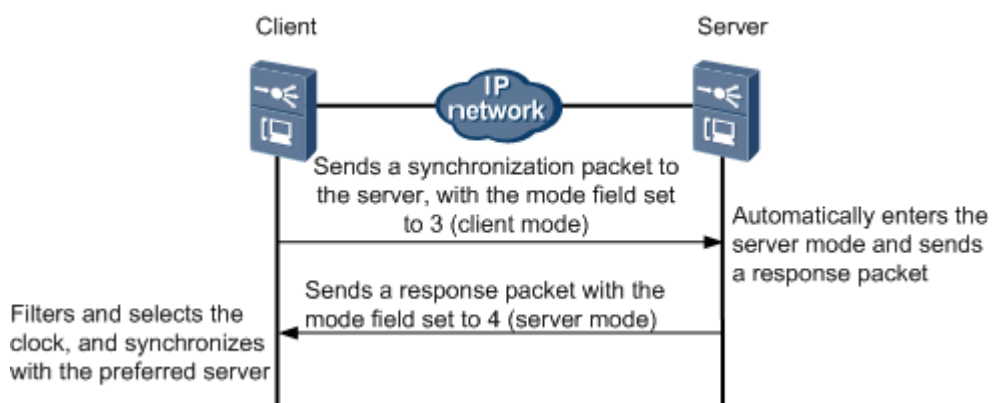
Prerequisites

Before configuring the NTP client/server mode, make sure that the network interface and the routing protocol of the MA5800 are configured so that the server and the client are reachable to each other at the network layer.

Context

In the client/server mode, the client sends a synchronization packet to the server, with the mode field set to 3 (client mode). After receiving the packet, the server automatically enters the server mode and sends a response packet with the mode field set to 4 (server mode). After receiving the response from the server, the client filters and selects the time, and synchronizes with the preferred server, as shown in [Figure 14-41](#).

Figure 14-41 NTP client/server mode



Precaution

1. In the client/server mode, you need to configure only the client, and do not need to configure the server.

2. The clock stratum of the synchronizing device must be lower than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

Step 1 Add a VLAN interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
3. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
4. Configure the IP address of the VLAN interface.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.

Step 2 Run the **ntp-service unicast-server** command on the client to configure the NTP unicast server mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

NOTE

- In this command, *ip-address* is a unicast address, which cannot be a broadcast address, a multicast address, or the IP address of a local clock.
- After the source interface of the NTP packets is specified by *source-interface*, the source IP address of the NTP packets is configured as the primary IP address of the specified interface.
- A server can function as a time server to synchronize other devices only after its clock is synchronized.
- When the clock stratum of the server is higher than or equal to that of the client, the client does not synchronize with the server.

You can run the **ntp-service unicast-server** command for multiple times to configure multiple servers. Then, the client selects the best server according to clock priorities or preemption.

For example, assuming that there are two servers A and B. A sets up a temporary NTP session, and then B sets up another. When the conditions (level and precision) of A and B are the same, [Table 14-14](#) shows the clock source selection results.

Table 14-14 Clock source selection results

Mode (A)	Mode (B)	Clock Source
None	None	A
None	Priority	B
None	Preemption	A
Priority	None	A

Mode (A)	Mode (B)	Clock Source
Priority	Priority	A
Priority	Preemption	A
Preemption	None	B
Preemption	Priority	B
Preemption	Preemption	A

Step 3 (Optional) Configure the ACL rules.

Filter the packets that pass through the Layer 3 interface. Only the IP packet from the clock server is allowed to access the Layer 3 interface. Other unauthorized packets are not allowed to access the Layer 3 interface. It is recommended to use the ACL rules for the system that has high requirements on security.

1. Run the **acl adv-acl-number** command to create an ACL for the IPv4 system.
2. Run the **rule** command to classify traffic according to the source IP address, destination IP address, type of the protocol over IP, and features or protocol of the packet, allowing or forbidding the data packets that meet related conditions to pass.
3. Run the **packet-filter** command to configure an ACL filtering rule for a specified port, and make the configuration take effect.

----End

Example

(IPv4) Assume the following configurations : One MA5800 functions as the NTP server (IP address: 10.20.20.20/24), the other MA5800 (IP address of the Layer 3 interface of VLAN 2: 10.10.10.10/24, gateway IP address: 10.10.10.1) functions as the NTP client, the NTP client sends the clock synchronization request packet through the VLAN interface to the NTP server, the NTP server responds to the request packet, and ACL rules are configured to allow only IP packets from the clock server to access the Layer 3 interface. To perform these configurations, do as follows:

```
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
huawei(config)#undo ntp-service server disable
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#acl 3010
huawei(config-acl-adv-3010)#rule deny ip source any destination 10.10.10.10
0.0.0.0
huawei(config-acl-adv-3010)#rule permit ip source 10.20.20.20 0.0.0.0 destination
10.10.10.10 0.0.0.0
huawei(config-acl-adv-3010)#quit
huawei(config)#packet-filter inbound ip-group 3010 port 0/9/1
```

14.7.3.5 Configuring the NTP Peer

This topic describes how to configure the MA5800 for clock synchronization in the NTP peer mode. In the peer mode, configure only the active peer, and the passive

peer does not need to be configured. In the peer mode, the active peer and the passive peer can synchronize with each other. The peer with a higher clock stratum is synchronized by the peer with a lower clock stratum.

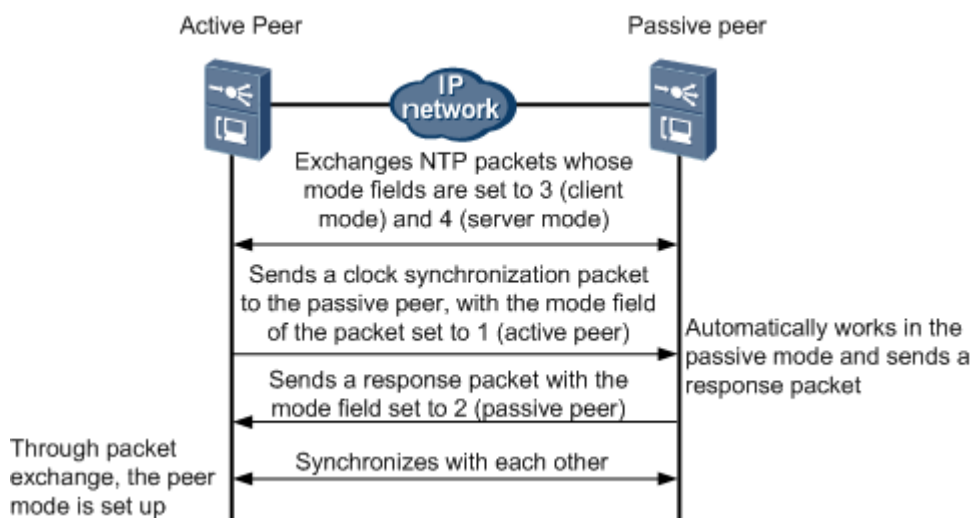
Prerequisites

Before configuring the NTP peer mode, make sure that the network interface and the routing protocol of the MA5800 are configured so that the server and the client are reachable to each other at the network layer.

Context

In the peer mode, the active peer and the passive peer exchange NTP packets whose mode fields are set to 3 (client mode) and 4 (server mode). Then, the active peer sends a clock synchronization packet to the passive peer, with the mode field of the packet set to 1 (active peer). After receiving the packet, the passive peer automatically works in the passive mode and sends a response packet with the mode field set to 2 (passive peer). Through packet exchange, the peer mode is set up. The active peer and the passive peer can synchronize with each other. If both the clock of the active peer and that of the passive peer are synchronized, the clock on a lower stratum is used, as shown in [Figure 14-42](#).

Figure 14-42 NTP peer mode



Precaution

1. In the peer mode, you need to configure the NTP mode only on the active peer.
2. The peers determine clock synchronization according to the clock stratum instead of according to whether the peer is an active peer.

Procedure

Step 1 Enable the NTP server functionality.

1. Run the **undo ntp-service server disable** command to enable IPv4 NTP server functionality.

Step 2 Configure the NTP active peer.

1. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
2. Run the **ntp-service unicast-peer** command to configure the NTP peer mode, and specify the IP address of the remote server that functions as the local timer server and the interface for transmitting and receiving NTP packets.

 NOTE

- In this command, *ip-address* is a unicast address, which cannot be a broadcast address, a multicast address, or the IP address of a reference clock.
- After the source interface of the NTP packets is specified by *source-interface*, the source IP address of the NTP packets is configured as the primary IP address of the specified interface.

Step 3 Add a VLAN interface.

1. Run the **vlan** command to create a VLAN.
2. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
3. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
4. Configure the IP address based on the system.
 - Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.

----End

Example

Assume the following configurations (IPv4): One MA5800 functions as the NTP active peer (IP address of the Layer 3 interface of VLAN 2: 10.10.10.10/24) and works on clock stratum 4, the other MA5800 (IP address: 10.10.10.20/24) functions as the NTP passive peer, the active peer sends a clock synchronization request packet through the VLAN interface to the passive peer, the passive peer responds to the request packet, and the peer with a higher clock stratum is synchronized by the peer with a lower clock stratum. To perform these configurations, do as follows:

```
huawei(config)#undo ntp-service server disable
huawei(config)#ntp-service refclock-master 4
huawei(config)#ntp-service unicast-peer 10.10.10.20 source-interface vlanif 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
```

14.7.3.6 Configuring the NTP Multicast Mode

This topic describes how to configure the MA5800 for clock synchronization in the NTP multicast mode. The multicast mode is a mechanism used by NTP clients to

dynamically discover NTP servers. After the multicast mode is enabled, unicast NTP servers do not need to be manually configured for clients.

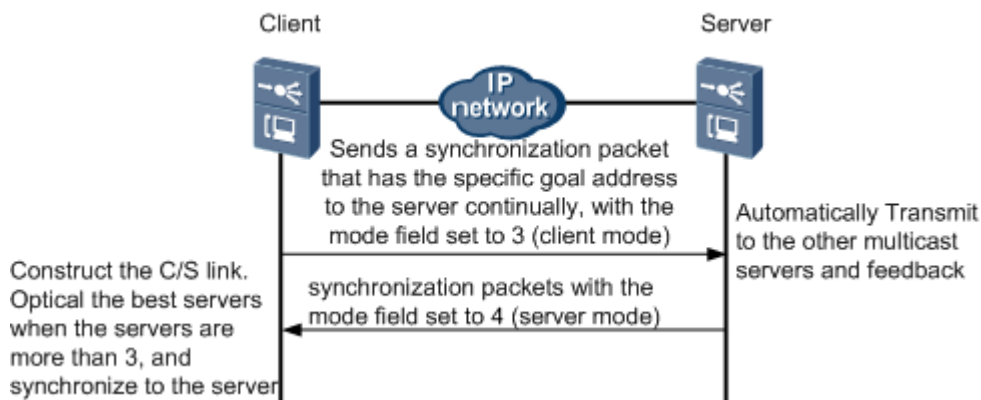
Prerequisites

Before configuring the NTP multicast mode, make sure that the network interface and the routing protocol of the MA5800 are configured so that the server and the client are reachable to each other at the network layer.

Context

In the multicast mode, multicast clients search multicast NTP servers by sending NTP packets using the specified multicast IP address as the destination IP address. The mode field in the packets is set to 3 (client mode). Multicast NTP servers listen to the multicast IP address, and send response packets after receiving the packets. The mode field in the response packets is set to 4 (server mode). After receiving the response packets, the multicast clients set up temporary client/server (C/S) connections. After setting up a certain number of C/S connections (the required number of C/S connections have a fixed value of 3), the multicast clients stop searching and select the optimal NTP server from the C/S connections. The unselected C/S connections will be aged. [Figure 14-43](#) shows the NTP multicast mode.

Figure 14-43 NTP multicast mode



Precaution

1. In the multicast mode, you should configure both the NTP server and the NTP client.
2. The clock stratum of the synchronizing device must be higher than or equal to that of the synchronized device. Otherwise, the clock synchronization fails.

Procedure

- Configure the NTP multicast server host.
 - a. Run the **undo ntp-service server disable** command to enable the IPv4 NTP server function.

- b. Run the **ntp-service refclock-master** command to configure the local clock as the master NTP clock, and specify the stratum of the master NTP clock.
- c. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

- i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
- d. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.
 - iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
 - iv. Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
- e. Run the **ntp-service multicast-server** command to configure the NTP multicast server mode of the host, and specify the key ID for the server to send packets to the client.

- Configure the NTP multicast client host.

- a. (Optional) Configure NTP authentication.

In certain networks that have strict requirements on security, it is recommended that you enable NTP authentication when running the NTP protocol. The configuration of the server must be the same as that of the client.

- i. Run the **ntp-service authentication enable** command to enable NTP authentication.
 - ii. Run the **ntp-service authentication-keyid** command to set an NTP authentication key.
 - iii. Run the **ntp-service reliable authentication-keyid** command to declare that the key is reliable.
 - b. Add a VLAN interface.
 - i. Run the **vlan** command to create a VLAN.
 - ii. Run the **port vlan** command to add an upstream port to the VLAN so that the user packets carrying the VLAN tag are transmitted upstream through the upstream port.

- iii. In the global config mode, run the **interface vlan** command to create a VLAN interface, and then enter the VLANIF mode to configure the Layer 3 interface.
- iv. Run the **ip address** command to configure the IPv4 address and subnet mask of the VLAN interface so that the IP packets in the VLAN can participate in the Layer 3 forwarding.
- c. Run the **ntp-service manycast-client** command to configure a host as the NTP multicast client.

----End

Example

(IPv4) Assume the following configurations: MA5800_S uses the local clock as the master NTP clock on stratum 2 and works in the NTP multicast mode, listening to clock synchronization packets that use 10.10.10.10/24 as the destination IP address through IP address 10.10.10.10/24 of the Layer 3 interface of VLAN 2 and establishing C/S connections with multicast clients, and MA5800_C functions as the NTP multicast client, multicasting clock synchronization packets that use 10.10.10.10/24 as the destination IP address continuously through IP address 10.10.10.20/24 of the Layer 3 interface of VLAN 2 and synchronizing with the clock on the multicast server by establishing C/S connections with the multicast server. To perform these configurations, do as follows:

1. On MA5800_S:

```
huawei(config)#undo ntp-service server disable
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service manycast-server
huawei(config-if-vlanif2)#quit
```
2. On MA5800_C:

```
huawei(config)#undo ntp-service server disable
huawei(config)#vlan 2 standard
huawei(config)#port vlan 2 0/9 1
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service manycast-client
huawei(config-if-vlanif2)#quit
```

14.7.3.7 (Optional) Configuring NTPv4 Control Signaling KOD

Kiss-o'-Death (KOD) packets are NTPv4-defined control signaling packets used for state advertisement during Network Time Protocol (NTP) message exchange and for access control. The KOD packets do not apply to time synchronization. The KOD packets can help the users to control the interval that the client transmits packets to the server.

Prerequisites

- The client sends NTP packets to the server for multiple times.
- The server filters packets sent by the client.

Context

KOD packets carry KOD codes that are indicated by a four-character ASCII character string. The KOD codes are called KISS codes. Different KISS codes have different meanings. The system supports RATE and DENY KISS codes.

KISS Code	Server Configuration	Application Scenario
DENY	Run the ntp-service access command to configure access control. Then the server sends KOD packets that carry DENY KISS codes to the client when the client's access request is denied because of restricted rights.	This configuration applies when an NTP server is only configured for specified clients, which provides protection for the clients.
RATE	Run the ntp-service access limited command to configure rate control, and the ntp-service discard command to configure the minimum interval and average interval allowed by the server for the client to transmit packets. • When the client sends packets at an interval shorter than the minimum or average interval, the server sends KOD packets that carry RATE KISS codes to the client. • When the client sends packets at an interval longer than the minimum and average intervals, the server does not send any KOD packets.	This configuration applies to servers of poor performance.

Precaution

The following operations are performed only on servers.

Procedure

- Step 1** Run the **undo ntp-service server disable** command to enable IPv4 NTP server functionality.
- Step 2** Run the **ntp-service kod-enable** command to enable the KOD function globally. Then the server sends KOD packets that carry appropriate KISS codes in different scenarios, which controls packet transmission of the client.
- Step 3** Run the **ntp-service access** command to enable the access control function on the server. Then the server can control the client's access based on the client's rights. If the client's access is denied, the server sends KOD packets that carry **DENY** KISS codes.
- Step 4** Run the **ntp-service discard** command to configure the minimum interval and average interval allowed by the server for the client to transmit packets. Then the server controls packet transmission of the client using **RATE** KISS codes in KOD packets based on packet transmission frequency.

----End

Example

IPv4: Assume that server A in an IPv4 system has poor performance. The access control function needs to be enabled for server A to only receive NTP packets sent by clients at the minimum and average intervals longer than 3. To perform these configurations, do as follows:

```
huawei(config)#undo ntp-service server disable
huawei(config)#ntp-service kod-enable
huawei(config)#ntp-service access limited 2000
huawei(config)#ntp-service discard ntp-service discard min-interval 3 avg-interval 3
```

14.7.4 NTP Standards and Protocols Compliance

Reference documents:

- RFC 1305: Basis of the NTP module requirements specification
- RFC 5905: NTP version 4 Protocol and algorithm specification