Timing and Synchronization Configuration Guide, Cisco IOS XE 17 (Cisco Catalyst IR8340 Rugged Series Router)

First Published: 2023-02-10

Last Modified: 2024-09-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Configuring Clocking and Timing** 1

Clocking and Timing Overview 1

Frequency Synchronization 2

Time or Phase Synchronization 2

Time of Day (ToD) and 1PPS 2

Information about IRIG-B 3

IRIG-B Configuration 4

PRTC Mode With GNSS 5

CHAPTER 2 **Configuring Precision Time Protocol (PTP)** 7

Information About Precision Time Protocol 7

Why PTP? 7

Message-Based Synchronization 8

PTP Event Message Sequences 9

Synchronizing with Boundary Clocks 9

Synchronizing with Peer-to-Peer Transparent Clocks 10

Synchronizing the Local Clock 11

Best Master Clock Algorithm 11

PTP Clocks 12

Grandmaster Clock 12

Ordinary Clock 12

Boundary Clock 12

Transparent Clock 13

PTP Profiles 14

Default Profile Mode 14
Power Profile Mode 14
802.1AS Profile 15
PTP Profile Comparison 16
Tagging Behavior for PTP Packets 17
PTP Clock Modes Supported on the IR8340 Router 17
Configurable Boundary Clock Synchronization Algorithm 18
NTP to PTP Time Conversion 18
Clock Manager 19
GMC Block 20
Packet Flow 21
Guidelines and Limitations 22
PTP Messages 22
PTP Mode and Profile 22
Packet Format 22
VLAN Configuration 23
Clock Configuration 23
PTP Interaction with Other Features 23
NTP to PTP Conversion 24
Default Settings 24
Configuring GMC Mode 24
Configuring GMC Mode for a Default Profile 24
Configuring GMC Mode for a Power Profile 25
Configuring PTP Default Profile 25
Configuring an Ordinary Clock Client 26
Configuring a Boundary Clock 27
Configuring a Transparent Clock 28
Configuring PTP Power Profile 30
Configuring an Ordinary Clock 30
Configuring a Boundary Clock 31
Configuring a Transparent Clock 33
Configuring 802.1AS Profile 34
Configuring a Boundary Clock 34
Disable PTP 35

PTP Multidomain 36
Verifying the Configuration 36

CHAPTER 3 Configuring Network Time Protocol 39
Restrictions for Network Time Protocol 39
Information About Network Time Protocol 40
Network Time Protocol 40
Poll-Based NTP Associations 41
Broadcast-Based NTP Associations 42
NTP Access Group 42
NTP Services on a Specific Interface 43
Source IP Address for NTP Packets 43
System as an Authoritative NTP Server 43
How to Configure Network Time Protocol 44
Configuring NTP 44
Configuring Poll-Based NTP Associations 44
Configuring Broadcast-Based NTP Associations 45
Configuring an External Reference Clock 46
Configuring NTP Authentication 47
Verifying Network Time Protocol 48
Configuration Examples for Network Time Protocol 49
Example: Configuring Network Time Protocol 49
Additional References for Network Time Protocol 50
Related Documents 50
Standards and RFCs 50
Technical Assistance 50
Feature Information for Network Time Protocol 50

CHAPTER 4 NTP Timing Based on PTP Clock 53
PTP as a Reference Clock for NTP 53
Enabling PTP as a Reference Clock for NTP 53
Validate the PTP Reference Clock 54
Troubleshooting PTP as an NTP Reference Clock 54
Checking PTP-NTP Synchronization 54

Troubleshooting Commands 55
Viewing Peering Details 55

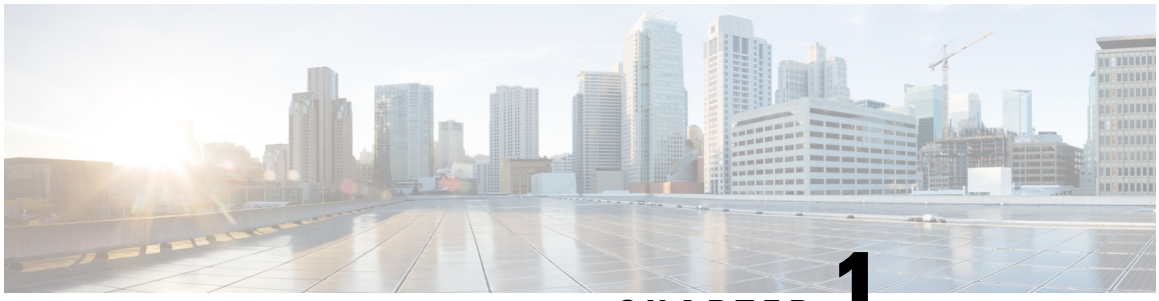
CHAPTER 5 G.8265.1 Profile 57
Information about G.8265.1 Profile 57
G.8265.1 Profile Mapping 58
Configuring G.8265.1 Server and Client Ordinary Clock 59
Configuring Server Ordinary Clock 59
Configuring Client Ordinary Clock 61
Verifying the Configuration 63

CHAPTER 6 G.8275.1 Profile 67
Information About G.8275.1 67
Synchronization Model 67
PTP Domains 68
PTP Messages and Transport 68
Best Master Clock Algorithm 68
Configuring the G.8275.1 Profile 69
Configuration On T-GM 69
Configuration On T-TSC 70
Configuration On T-BC 70
Verifying the Configuration 70
Debugging Commands 73

CHAPTER 7 Configuring Synchronous Ethernet ESMC and SSM 77
Understanding Synchronous Ethernet 77
Clock Selection Modes 77
Configuring Synchronous Ethernet ESMC and SSM 78

CHAPTER 8 Configuring the Global Navigation Satellite System 81
Information About GNSS 81
GNSS Signaling 82
GNSS LED 83
Guidelines and Limitations 83

Configuring the Satellite Constellation for GNSS 84
Verifying Configuration 84



CHAPTER 1

Configuring Clocking and Timing

The terms *IR8340* and *router* are used throughout this document in text and CLI examples to refer to the Cisco Catalyst IR8340 Rugged Series Router, unless otherwise noted.

- Clocking and Timing Overview, on page 1
- Time of Day (ToD) and 1PPS, on page 2
- Information about IRIG-B, on page 3
- PRTC Mode With GNSS, on page 5

Clocking and Timing Overview

The Cisco IR8340 Routers have the capability of frequency and time synchronization. The router WAN ports (GigabitEthernet 0/0/0 and GigabitEthernet 0/0/1) are capable of distributing frequency and phase information. The LAN ports (GigabitEthernet 0/1/0 - GigabitEthernet 0/1/11) are capable of distributing phase information only. IR8340 can synchronize to a GPS source. The IR8340 router can also distribute phase via an external IRIG-B interface and external ToD RS-485 interface.

The IR8340 router supports a pluggable timing module (Cisco PID: IRM-TIMING-MOD) from Cisco IOS-XE Release 17.9.1, which has the following timing ports:

- ToD + 1 PPS Output—Provide or receive time of day (ToD) messages or one pulse-per-second (1 PPS) messages
- IRIG-B (analog and digital Input/Output) interfaces
- GNSS Receiver

Note You need license Network-Advantage on IR8340 to support all timing features (GNSS, IRIG-B and PTP profile like G.8265.1, G.8275.1, 1558v2, Power and Dot1as profiles). The **license boot level network-advantage** command enables license network-advantage.

Use the **show inventory** command to display the status of the timing module:

```
IR8340#show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco IR8340-K9 Chassis Type"
```

```
PID: IR8340-K9          , VID: V00  , SN: FDO2523J1BL
NAME: "Power Supply Module 0", DESCR: "150W AC Power Supply Module for Cisco IR8340-K9"
PID: PWR-RGD-AC-DC-H    , VID: V01  , SN: DTH251705BY
NAME: "module 0", DESCR: "Cisco IR8340 Built-In NIM controller"
PID: IR8340-K9          , VID: V00  , SN: FDO252207UG
NAME: "Timing", DESCR: "Timing Module"
PID: IRM-TIMING-MOD     , VID: V00  , SN: FDO253409KG
NAME: "NIM subslot 0/0", DESCR: "Front Panel 2 ports Gigabitethernet Module"
PID: IR8340K9-2x1GC     , VID: V01  , SN:
```

Frequency Synchronization

IR8340 can recover the reference clock frequency from any of the following input sources:

- GNSS
- SyncE
- PTP Telecom Profile (G.8265.1/G.8275.1)
- Local Oscillator

When a reference clock is selected, it is propagated to downstream network elements via SyncE or PTP Telecom Profile (G.8265.1/G.8275.1).

Time or Phase Synchronization

It is important to precisely synchronize the time-of-day between different network devices. This is essential in calculating network delays.

The time/phase synchronization on IR8340 is by one of the following input sources:

- GNSS
- PTP
- IRIG-B

Time of Day (ToD) and 1PPS

You can use the time of day (ToD) and 1PPS port on the IR8340 router to exchange ToD clocking. By default, TOD is in UBX format when GNSS is source and in locked state.

Use the **show ptp wan tod** command to display ToD information:

```
IR8340#show ptp wan tod
PTPd ToD information:

Time: 01/05/22 11:35:21
```

Information about IRIG-B

The Inter-Range Instrumentation Group (IRIG) time codes are the result of the US military's need to standardize test ranges' timing codes towards the end of the 1950s. This standardization resulted in a common set of time codes that eliminated incompatibility challenges and allowed for the exchange of synchronized test data across ranges. Six IRIG codes variations were developed (A, B, D, E, G, H) of which IRIG time code B (IRIG-B) became widely accepted for time distribution with power, industrial automation, and control industries.

The IRIG standard was first published in 1960 with the latest version, IRIG standard 200-04, "IRIG Serial Time Code Formats," updated in September 2004. The IRIG-B time protocol is widely used by electric utilities and other verticals to establish and maintain time synchronization between system devices (e.g., power breakers, relays, meters, etc.) IRIG sends a complete time frame once per second, and each frame is composed of 100 bits. It contains time-of-year and year information in a BCD format, and (optionally) seconds-of-day in SBS. Though it is considered to be a reliable and predictable timing source distribution framework (dedicated timing signals) it traditionally relies on a precise timing source, e.g., GPS.

The IRIG protocol in the IR8340 has been implemented for format-B (IRIG-B) per IRIG standard 200-04 with capabilities to receive (INPUT) or transmit (OUTPUT) 4x Analog (AM) and 4x Digital (TTL) time code formats, see table below.

IR8340 IRIG-B Modes		Format ID	IRIG Signal
Analog (AM)	AM02	AM-B122	Amplitude Modulated, 1kHz / 1ms resolution, BCD_{TOY}
	AM03	AM-B123	Amplitude Modulated, 1kHz / 1ms resolution, BCD_{TOY}, SBS
	AM06	AM-B126	Amplitude Modulated, 1kHz / 1ms resolution, BCD_{TOY}, BCD_{YEAR}
	AM07	AM-B127	Amplitude Modulated, 1kHz / 1ms resolution, BCD_{TOY}, BCD_{YEAR}, SBS
Digital (TTL)	TTL02	TTL-B002	Unmodulated, DCLS, pulse-width-coded, BCD_{TOY}
	TTL03	TTL-B003	Unmodulated, DCLS, pulse-width-coded, BCD_{TOY}, SBS
	TTL06	TTL-B006	Unmodulated, DCLS, pulse-width-coded, BCD_{TOY}, BCD_{YEAR}
	TTL07	TTL-B007	Unmodulated, DCLS, pulse-width-code, BCD_{TOY}, BCD_{YEAR}, SBS

Note

- BCD: day of year, hours, minutes, and seconds.
- BCD_Year: BCD plus Year 00 – 99, which century is not coded.
- SBS: Straight Binary Seconds, 0 – 86339.

The IR8340 hardware has two physical interfaces, one for analog (AM) and one for digital (TTL), with INPUT or OUTPUT signal capabilities per interface.

This IRIG-B **INPUT** / **OUTPUT** signaling support allows the IR8340 to be a central timing device in multiple use-cases:

- **INPUT**: The IR8340 receives IRIG-B timing signaling (AM or TTL) from an IRIG-B time source if only available or so required. In this case IRIG-B can be used as the IR8340's clock source for PTP (only) - IR8340 configured as Grand Master Clock (GMC) for time distribution.

- **OUTPUT**: The IR8340 utilizes other precise timing sources, e.g., GNSS/GPS, PTP, NTP, as a clock source. The IRIG-B interface(s) can be used to transmit timing signal to IRIG-B dependent devices in location.

The IR8340 supports IRIG-B IN and IRIG-B OUT in addition to the GNSS interface. The following table shows the mapping of Time Source to time distribution protocol alignment (i.e. one will serve as time source to the other).

Time Source	Time Distribution
IRIG-B IN	PTP
GNSS, PTP, NTP	IRIG-B OUT

IRIG-B Configuration

Use the following command to configure IRIG mode (AM or TTL) and direction (IN or OUT) on the interface:

[**no**] **irig mode** {**TTL2**|**TTL3**|**TTL6**|**TTL7**|**AM2**|**AM3**|**AM6**|**AM7**} **dir** {**in | out**}

- TTL2 = IRIG-B002, TTL3 = IRIG-B003, TTL6 = IRIG-B006, TTL7 = IRIG-B007
- AM2 = IRIG-B122, AM3 = IRIG-B123, AM6 = IRIG-B126, AM7 = IRIG-B127

Use the **no** form of the command to disable the IRIG feature on the interface.

Note To switch input from digital to analog or vice versa, you must remove the input configuration on one port before reconfiguring the input on another port.

You can use the **show irig** command to display IRIG-B mode and direction configurations on the IR8340.

The following example shows output from IR8340 OUT direction.

```
IR8340#show irig
IRIG-B Digital mode disabled
IRIG-B Analog mode AM02 dir OUT
IRIG-B Clk Id 1 Source PTP  time: Year: 2021 Day: 343 Hour 8 Min 33 Sec 35.    //Source can
 be different based on what it's getting (can be GNSS/NTP/PTP/HANDSET/NONE).
                            ns 1639038815645806587 [0x16BF091E6BA52FFB]
IRIG-B Virtual Clock State: INACTIVE
*** IRIG-B input is disabled ***
```

The following example shows output from IR8340 IN direction.

```
IRIG-B Digital mode disabled
IRIG-B Analog mode AM02 dir IN
IRIG-B Clk Id 5 Source IRIG-B  time: Year: 2021 Day: 343 Hour 8 Min 36 Sec 25.  //Because
it's IN direction, the source is IRIG-B.
                            ns 1639038985184125000 [0x16BF0945E4EAA048]
IRIG-B Virtual Clock State: ACTIVE
*** IRIG-B AM input mode ***
B122 : Day 343 Hour 8 Min 36 Sec 24
NOTE: Input time shown is the last received frame time
```

PRTC Mode With GNSS

IR8340 can act in Primary Reference Time Clock (PRTC) mode, when GNSS is locked and no telecom profiles are configured. In PRTC mode, IR8340 provides TOD + 1pps output with TOD in UBX format.

Once IR8340 is in PRTC mode, ordinary clock and transparent clocks are not supported under LAN profiles. All boundary clocks under LAN profiles will be GMC-BC mode, which fetches timestamps and grandmaster clock details as per the GNSS input.

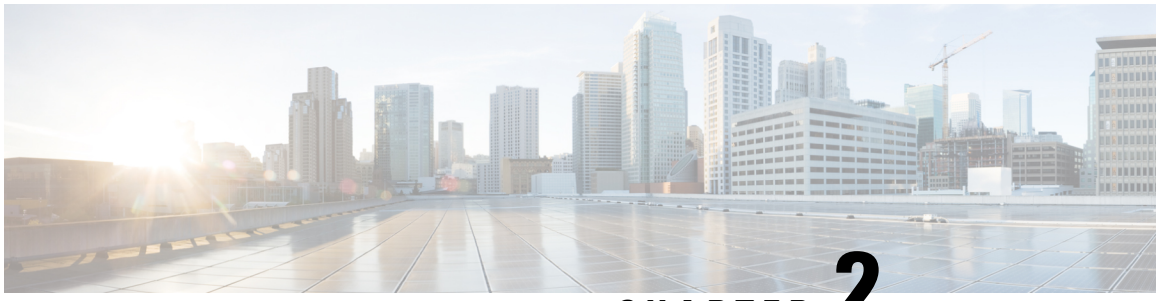
The following clock quality values will be provided by the GMC-BC master clock:

```
Clock Quality:
    Class: 6                        //----GNSS CLASS
    Accuracy: Within 250ns          //----GNSS Accuracy
    Offset (log variance): 20061    //----GNSS Variance
```

PRTC mode is supported on PTP Default and Power profile. The conversion will take place automatically when GNSS moves to locked state.

Note GNSS cannot be configured when the one of the following is configured:

- 802.1AS
- PTP TC mode
- GMC-BC options



CHAPTER 2

Configuring Precision Time Protocol (PTP)

PTP configuration is supported from Cisco IOS XE Release 17.7.x.

- Information About Precision Time Protocol, on page 7
- Configuring GMC Mode, on page 24
- Configuring PTP Default Profile, on page 25
- Configuring PTP Power Profile, on page 30
- Configuring 802.1AS Profile, on page 34
- Disable PTP, on page 35
- PTP Multidomain, on page 36
- Verifying the Configuration, on page 36

Information About Precision Time Protocol

Precision Time Protocol (PTP) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

A Network Advantage license is required to enable the PTP feature or to execute the CLIs on the router.

To configure the license level to network-advantage, use the following CLI:

license boot level network-advantage

```
Router#config terminal
Router(config)#license boot level network-advantage
Do you want to accept terms? Y
```

Why PTP?

Smart grid power automation applications such as peak-hour billing, virtual power generators, and outage monitoring and management, require extremely precise time accuracy and stability. Timing precision improves network monitoring accuracy and troubleshooting ability.

In addition to providing time accuracy and synchronization, the PTP message-based protocol can be implemented on packet-based networks, such as Ethernet networks. The benefits of using PTP in an Ethernet network include:

- Low cost and easy setup in existing Ethernet networks
- Limited bandwidth is required for PTP data packets

Message-Based Synchronization

To ensure clock synchronization, PTP requires an accurate measurement of the communication path delay between time source (grandmaster clock) and the time recipient. PTP sends messages between the time source and time recipient to determine the delay measurement. Then, PTP measures the exact message transmit and receive times and uses these times to calculate the communication path delay. PTP then adjusts current time information contained in network data for the calculated delay, resulting in more accurate time information.

This delay measurement principle determines path delay between devices on the network, and the local clocks are adjusted for this delay using a series of messages sent between time source and time recipient devices. The one-way delay time is calculated by averaging the path delay of the transmit and receive messages. This calculation assumes a symmetrical communication path; however, switched networks do not necessarily have symmetrical communication paths, due to the buffering process.

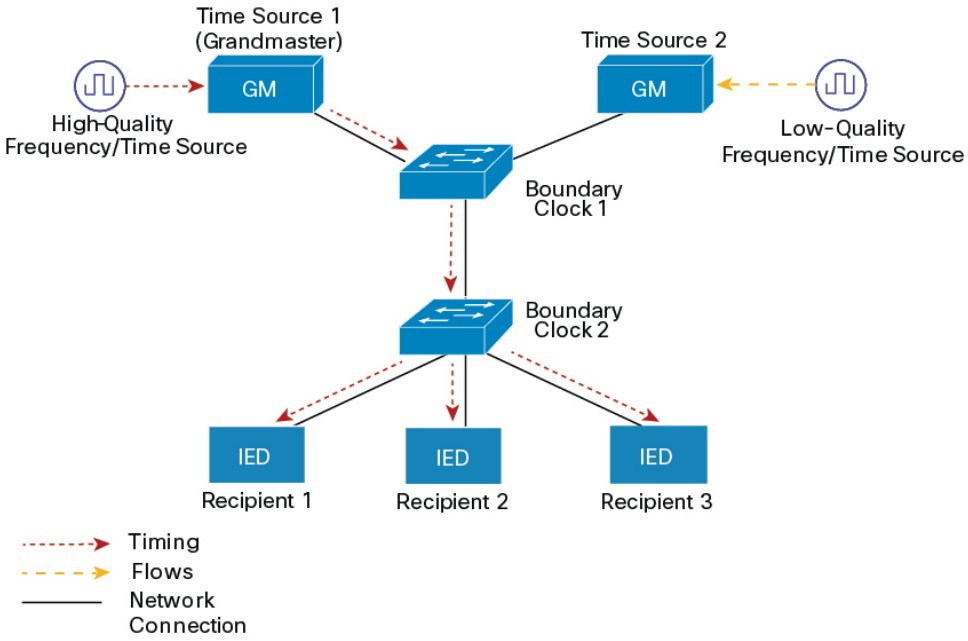
PTP provides a method, using transparent clocks, to measure and account for the delay in a time-interval field in network timing packets, making the switches temporarily transparent to the time source and time recipient nodes on the network. An end-to-end transparent clock forwards all messages on the network in the same way that a switch does.

Note Cisco PTP supports multicast PTP messages only.

To read a detailed description of synchronization messages, refer to PTP Event Message Sequences, on page 9. To learn more about how transparent clocks calculate network delays, refer to Transparent Clock, on page 13.

The following figure shows a typical 1588 PTP network that includes grandmaster clocks, switches in boundary clock mode, and Intelligent Electronic Device (IEDs) such as a digital relays or protection devices. In this diagram, Time Source 1 is the grandmaster clock. If Time Source 1 becomes unavailable, the time recipient boundary clocks switch to Time Source 2 for synchronization.

Figure 1: PTP Network



PTP Event Message Sequences

This section describes the PTP event message sequences that occur during synchronization.

Synchronizing with Boundary Clocks

The ordinary and boundary clocks configured for the delay request-response mechanism use the following event messages to generate and communicate timing information:

- Sync
- Delay_Req
- Follow_Up
- Delay_Resp

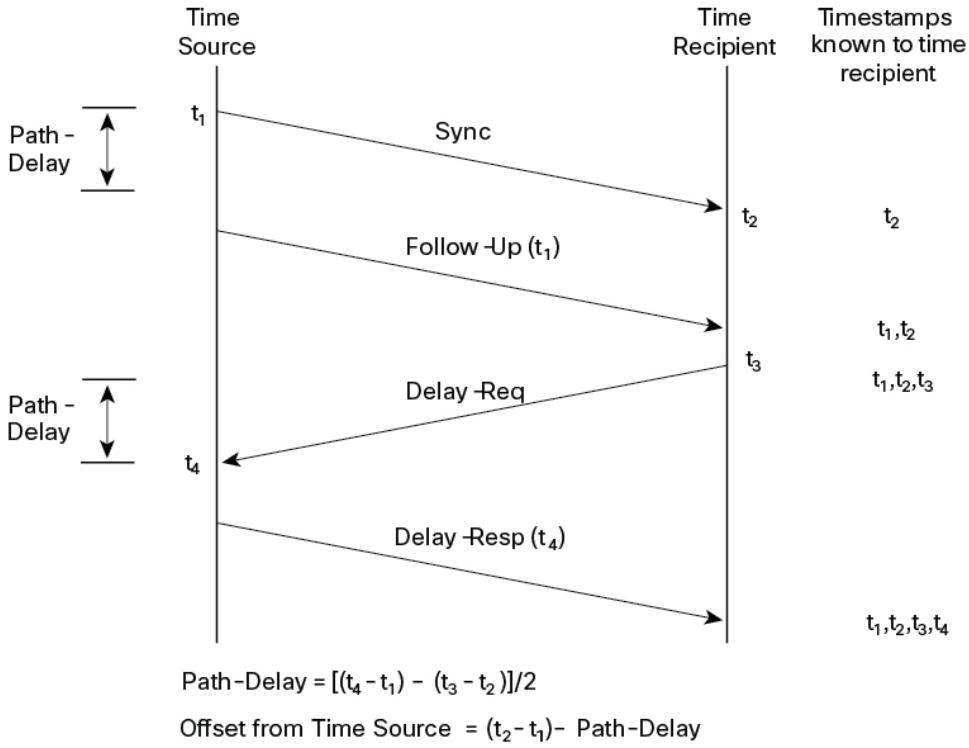
These messages are sent in the following sequence:

1. The time source sends a Sync message to the time recipient and notes the time (t1) at which it was sent.
2. The time recipient receives the Sync message and notes the time of reception (t2).
3. The time source conveys to the time recipient the timestamp t1 by embedding the timestamp t1 in a Follow_Up message.
4. The time recipient sends a Delay_Req message to the time source and notes the time (t3) at which it was sent.
5. The time source receives the Delay_Req message and notes the time of reception (t4).
6. The time source conveys to the time recipient the timestamp t4 by embedding it in a Delay_Resp message.

After this sequence, the time recipient possesses all four timestamps. These timestamps can be used to compute the offset of the time recipient clock relative to the time source, and the mean propagation time of messages between the two clocks.

The offset calculation is based on the assumption that the time for the message to propagate from time source to time recipient is the same as the time required from time recipient to time source. This assumption is not always valid on an Ethernet network due to asymmetrical packet delay times.

Figure 2: Detailed Steps—Boundary Clock Synchronization



Synchronizing with Peer-to-Peer Transparent Clocks

When the network includes multiple levels of boundary clocks in the hierarchy, with non-PTP enabled devices between them, synchronization accuracy decreases.

The round-trip time is assumed to be equal to mean_path_delay/2, however this is not always valid for Ethernet networks. To improve accuracy, the resident time of each intermediary clock is added to the offset in the end-to-end transparent clock. Resident time, however, does not take into consideration the link delay between peers, which is handled by peer-to-peer transparent clocks.

Peer-to-peer transparent clocks measure the link delay between two clock ports implementing the peer delay mechanism. The link delay is used to correct timing information in Sync and Follow_Up messages.

Peer-to-peer transparent clocks use the following event messages:

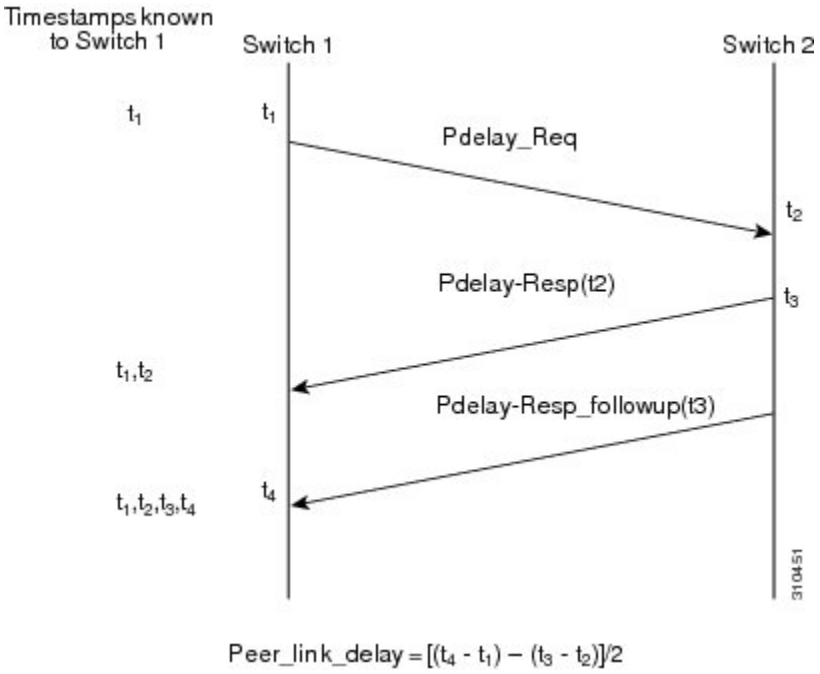
- Pdelay_Req
- Pdelay_Resp
- Pdelay_Resp_Follow_Up

These messages are sent in the following sequence:

1. Port 1 generates timestamp t1 for a Pdelay_Req message.
2. Port 2 receives and generates timestamp t2 for this message.
3. Port 2 returns and generates timestamp t3 for a Pdelay_Resp message.

   To minimize errors due to any frequency offset between the two ports, Port 2 returns the Pdelay_Resp message as quickly as possible after the receipt of the Pdelay_Req message.
4. Port 2 returns timestamps t2 and t3 in the Pdelay_Resp and Pdelay_Resp_Follow_Up messages respectively.
5. Port 1 generates timestamp t4 after receiving the Pdelay_Resp message. Port 1 then uses the four timestamps (t1, t2, t3, and t4) to calculate the mean link delay.

Figure 3: Detailed Steps—Peer-to-Peer Transparent Clock Synchronization



Synchronizing the Local Clock

In an ideal PTP network, the time source and time recipient clocks operate at the same frequency. However, *drift* can occur on the network. Drift is the frequency difference between the time source and time recipient clocks. You can compensate for drift by using the time stamp information in the device hardware and follow-up messages (intercepted by the switch) to adjust the frequency of the local clock to match the frequency of the time source clock.

Best Master Clock Algorithm

The Best Master Clock Algorithm (BMCA) is the basis of PTP functionality. The BMCA specifies how each clock on the network determines the best time source clock in its subdomain of all the clocks it can see,

including itself. The BMCA runs on the network continuously and quickly adjusts for changes in network configuration.

The BMCA uses the following criteria to determine the best time source clock in the subdomain:

- Clock quality (for example, GPS is considered the highest quality)
- Clock accuracy of the clock's time base.
- Stability of the local oscillator
- Closest clock to the grandmaster

In addition to identifying the best time source clock, the BMCA also ensures that clock conflicts do not occur on the PTP network by ensuring that:

- Clocks do not have to negotiate with one another
- There is no misconfiguration, such as two time source clocks or no time source clocks, as a result of the time source clock identification process

PTP Clocks

A PTP network is made up of PTP-enabled devices and devices that are not using PTP. The PTP-enabled devices typically consist of the following clock types.

Grandmaster Clock

The grandmaster clock is a network device physically attached to the server time source. All clocks are synchronized to the grandmaster clock.

Within a PTP domain, the grandmaster clock is the primary source of time for clock synchronization using PTP. The grandmaster clock usually has a very precise time source, such as a GPS or atomic clock. When the network does not require any external time reference and only needs to be synchronized internally, the grandmaster clock can free run.

Ordinary Clock

An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes:

- Server mode—Distributes timing information over the network to one or more client clocks, thus allowing the client to synchronize its clock to the server.
- Client mode—Synchronizes its clock to a server clock. You can enable the client mode on up to two interfaces simultaneously in order to connect to two different server clocks.

Ordinary clocks are the most common clock type on a PTP network because they are used as end nodes on a network that is connected to devices requiring synchronization.

Boundary Clock

A boundary clock in a PTP network operates in place of a standard network switch or router. Boundary clocks have more than one PTP port, and each port provides access to a separate PTP communication path. Boundary clocks provide an interface between PTP domains. They intercept and process all PTP messages, and pass all other network traffic. The boundary clock uses the BMCA to select the best clock seen by any port. The

selected port is then set to non-master mode. The master port synchronizes the clocks connected downstream, while the non-master port synchronizes with the upstream master clock.

Transparent Clock

The role of transparent clocks in a PTP network is to update the time-interval field that is part of the PTP event message. This update compensates for switch delay and has an accuracy of within one picosecond.

There are two types of transparent clocks:

End-to-end (E2E) transparent clocks measure the PTP event message transit time (also known as *resident time*) for SYNC and DELAY_REQUEST messages. This measured transit time is added to a data field (correction field) in the corresponding messages:

- The measured transit time of a SYNC message is added to the correction field of the corresponding SYNC or the FOLLOW_UP message.
- The measured transit time of a DELAY_REQUEST message is added to the correction field of the corresponding DELAY_RESPONSE message.

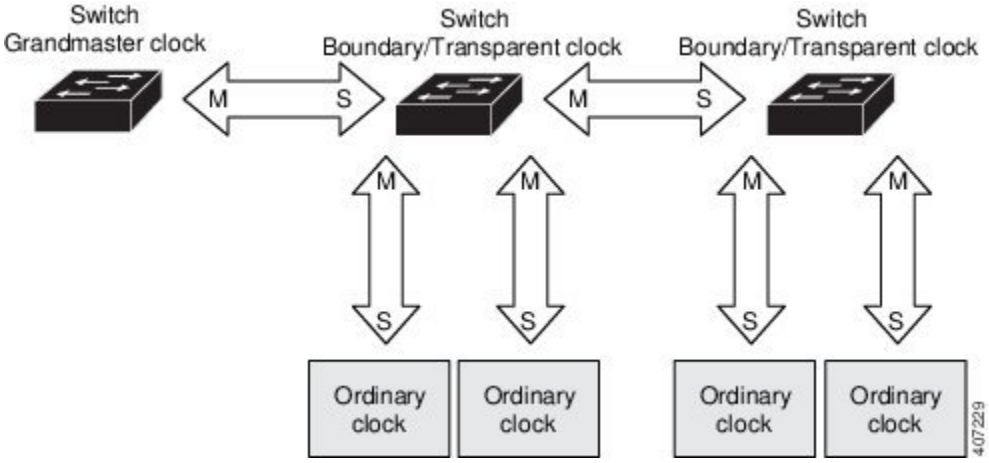
The time recipient uses this information when determining the offset between the time recipient's and the time source's time. E2E transparent clocks do not provide correction for the propagation delay of the link itself.

Peer-to-peer (P2P) transparent clocks measure PTP event message transit time in the same way E2E transparent clocks do, as described above. In addition, P2P transparent clocks measure the upstream link delay. The upstream link delay is the estimated packet propagation delay between the upstream neighbor P2P transparent clock and the P2P transparent clock under consideration.

These two times (message transit time and upstream link delay time) are both added to the correction field of the PTP event message, and the correction field of the message received by the time recipient contains the sum of all link delays. In theory, this is the total end-to-end delay (from time source to time recipient) of the SYNC packet.

The following figure illustrates PTP clocks in a time source-time recipient hierarchy within a PTP network.

Figure 4: PTP Clock Hierarchy



PTP Profiles

This section describes the following PTP profiles available on the router:

- Default Profile
- Power Profile
- 802.1AS Profile

Cisco IOS-XE Release 17.7.1 supports Power Profile-2011. It is defined in PC37.238-2011 - IEEE Draft Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications. This documentation uses the terms Power Profile mode and Default Profile mode when referring to this IEEE 1588 profile and its associated configuration values.

Beginning in Cisco IOS-XE Release 17.8.1, two Power Profiles are supported: Power Profile-2011 and Power Profile-2017. Power Profile-2017 is defined in IEEE Standard C37.238™-2017 (Revision of IEEE Std C37.238-2011) for use of IEEE 1588 Precision Time Protocol in Power System Applications.

The IEEE 1588 definition of a PTP profile is *the set of allowed PTP features applicable to a device*. A PTP profile is usually specific to a particular type of application or environment and defines the following values:

- Best master clock algorithm options
- Configuration management options
- Path delay mechanisms (peer delay or delay request-response)
- Range and default values of all PTP configurable attributes and data set members
- Transport mechanisms that are required, permitted, or prohibited
- Node types that are required, permitted, or prohibited
- Options that are required, permitted, or prohibited

Default Profile Mode

The default PTP profile mode on the router is Default Profile mode. In this mode:

- IR8340 supports ordinary clock (OC)- slave, boundary clock (BC), and transparent clock (TC) on default profile.
- IR8340 doesn’t support OC-master.
- All PTP profiles over bundles or port-channels are not supported on IR8340.

Power Profile Mode

The IEEE Power Profile defines specific or allowed values for PTP networks used in power substations. The defined values include the optimum physical layer, the higher level protocol for PTP messages, and the preferred best master clock algorithm. The Power Profile values ensure consistent and reliable network time distribution within substations, between substations, and across wide geographic areas.

The router is optimized for PTP in these ways:

- Hardware—The router uses FPGA and PHY for the PTP function. The PHY time stamps the Fast Ethernet and Gigabit Ethernet ports.

- Software—In Power Profile mode, the router uses the configuration values defined in the IEEE 1588 Power Profile standard.

The following table lists the configuration values defined by the IEEE 1588 Power Profile and the values that the router uses for each PTP profile mode.

Table 1: Configuration Values for the IEEE PTP Power Profile and Router Modes

PTP Field	Router Configuration Value	
	Power Profile Mode	**Default Profile Mode**
Message transmission	**Access Ports**–Untagged Layer 2 packets. **Trunk Ports**–802.1Q tagged Layer 2 packets. PTP packets are tagged with the PTP VLAN. If the PTP VLAN is not configured, packets go untagged over the native VLAN.	Layer 3 packets. By default, 802.1q tagging is disabled.
MAC address– Non-peer delay messages	01-00-5e-00-01-81.	Default profile uses L3 transport multicast address 224.0.1.129 for all PTP messages. Equivalent mac address is 01-00-5e-00-01-81
MAC address– Peer delay messages	01-80-C2-00-00-0E.	Not applicable to this mode.
Domain number	0.	0.
Path delay calculation	Peer-to-peer transparent clocks using the peer_delay mechanism.	End-to-end transparent clocks using the delay_request mechanism.
BMCA	Enabled.	Enabled.
Clock type	Two-step.	Two-step.
Time scale	Epoch.	Epoch.
Grandmaster ID and local time determination	PTP-specific TLV to indicate Grandmaster ID.	PTP-specific type, length, and value to indicate Grandmaster ID.
Time accuracy over network hops	Over 16 hops, slave device synchronization accuracy is within 1 usec (1 microsecond).	Not applicable in this mode.

802.1AS Profile

The IEEE 802.1AS standard "Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks" specifies the protocol and procedures used to ensure that synchronization requirements are met for time-sensitive applications across bridged and virtual bridged local area networks.

802.1AS specifies the use of IEEE 1588 (PTP) specifications where applicable in the context of IEEE Std 802.1D -2004 and IEEE Std 802.1Q -2005.1. The 802.1AS standard is one of three 802.1 AVB draft standards. 802.1AS over Ethernet (802.3) qualifies as a Profile of IEEE 1588-2008. It simplifies IEEE 1588 and defines synchronization over different types of media.

Note 802.1 AS can be configured with domain 0 only on IR8340 platform.

Key characteristics of 802.1AS are:

- For Ethernet full-duplex links, it uses the peer delay mechanism.
- All devices in the domain need to be 802.1AS capable.
- Transportation of 802.1AS packets is L2 multicast only, with no VLAN tag.
- It requires two-step processing (use of Follow_Up and Pdelay_Resp_Follow_Up messages to communicate timestamps).
- There is only a single active grandmaster in a time-aware network. That is, there is only a single 802.1AS domain.
- The BMCA (Best Master Clock Algorithm) is same as that used in IEEE 1588 with the following exceptions:
  - Announce messages received on a time recipient port that were not sent by the receiving time-aware system are used immediately; that is, there is no foreign-time source qualification.
  - A port that the BMCA determines should be a time source port enters the time source state immediately; that is, there is no pre-time source state.
  - The uncalibrated state is not needed and therefore not used.
  - All time-aware systems are required to participate in best master selection (even if the system is not grandmaster capable).

802.1AS is used in the Time Sensitive Network (TSN) feature. However, as a precise timing distribution mechanism, 802.1AS runs by itself without TSN configuration or inputs. The 802.1AS feature software implementation is based on the existing time stamping functionality of FPGA and has no new requirement on hardware beyond other PTP profiles.

The end-to-end time-synchronization performance of 802.1AS is as follows:

- Any two time-aware systems separated by six or fewer time-aware systems (that is, seven or fewer hops) will be synchronized to within 1 μs peak-to-peak of each other during steady-state operation.
- Performance beyond 7 hops is not defined.

PTP Profile Comparison

Table 2: Comparison of PTP Profiles on IE Switches

Profile	Default (*)	Power Profile-2011	Power Profile-2017	802.1AS
Standard	IEEE1588 v2 (J.3)	IEEE C37.238-2011	IEEE C37.238-2017	IEEE802.1AS

Profile	Default (*)		Power Profile-2011		Power Profile-2017	802.1AS
Mode	Boundary	End-to-End transparent	Boundary	Peer-to-Peer transparent	Peer-to-Peer transparent	**
Path Delay	Delay req/res	Delay req/res	Peer delay req/res	Peer delay req/res	Peer delay req/res	Peer delay req/res
Non-PTP device allowed in PTP domain	Yes	Yes	No	No	No	No
Transport	UDP over IP (multicast)		L2 Multicast		L2 Multicast	L2 Multicast

* Delay Request-Response Default PTP profile (as defined in IEEE1588 J.3).

** There is no mode setting for 802.1AS. Mathematically it is equivalent to P2P transparent, but it works differently from a transparent clock.

Tagging Behavior for PTP Packets

The following table describes the switch tagging behavior in Power Profile and Default Profile modes.

Table 3: Tagging Behavior for PTP Packets

Switch Port Mode	Configuration	Power Profile Mode		Default Profile Mode	
		Behavior	Priority	Behavior	Priority
Trunk Port	**vlan dot1q tag native** enabled	Switch tags packets	7	Switch tags packets	7
Trunk Port	**vlan dot1q tag native** disabled	PTP software tags packets	4	Untagged	None
Access Port	N/A	Untagged	None	Untagged	None

PTP Clock Modes Supported on the IR8340 Router

PTP synchronization behavior depends on the PTP clock mode that you configure on the router. You can configure the router for one of the following global modes.

See Guidelines and Limitations, on page 22 for guidelines for configuring each of the clock modes.

IR8340 supports the following PTP device types:

- OC-slave , boundary clock, and transparent clock on Default Profile/IEEE 1588.
- Boundary clock and transparent clock on Power profile.
- Boundary clock on Dot1as profile.

Note Currently all above profiles support two-step mode and don't support one-step mode on IR8340.

Configurable Boundary Clock Synchronization Algorithm

You can configure the BC synchronization algorithm to accommodate various PTP use cases, depending on whether you need to prioritize filtering of input time errors or faster convergence. A PTP algorithm that filters packet delay variation (PDV) converges more slowly than a PTP algorithm that does not.

By default, the BC uses a linear feedback controller (that is, a servo) to set the BC's time output to the next clock. The linear servo provides a small amount of PDV filtering and converges in an average amount of time. For improved convergence time, BCs can use the TC feedforward algorithm to measure the delay added by the network elements forwarding plane (the disturbance) and use that measured delay to control the time output.

While the feedforward BC dramatically speeds up the boundary clock, the feedforward BC does not filter any PDV. The adaptive PDV filter provides high quality time synchronization in the presence of PDV over wireless access points (APs) and enterprise switches that do not support PTP and that add significant PDV.

Three options are available for BC synchronization (all are compliant with IEEE 1588-2008):

- Feedforward—For very fast and accurate convergence; no PDV filtering.
- Adaptive—Filters as much PDV as possible, given a set of assumptions about the PDV characteristics, the hardware configuration, and the environmental conditions.

Note With the adaptive filter, the switch does not meet the time performance requirements specified in ITU-T G.8261.

- Linear—Provides simple linear filtering (the default).

Adaptive mode (**ptp transfer filter adaptive**) is not available in Power Profile mode.

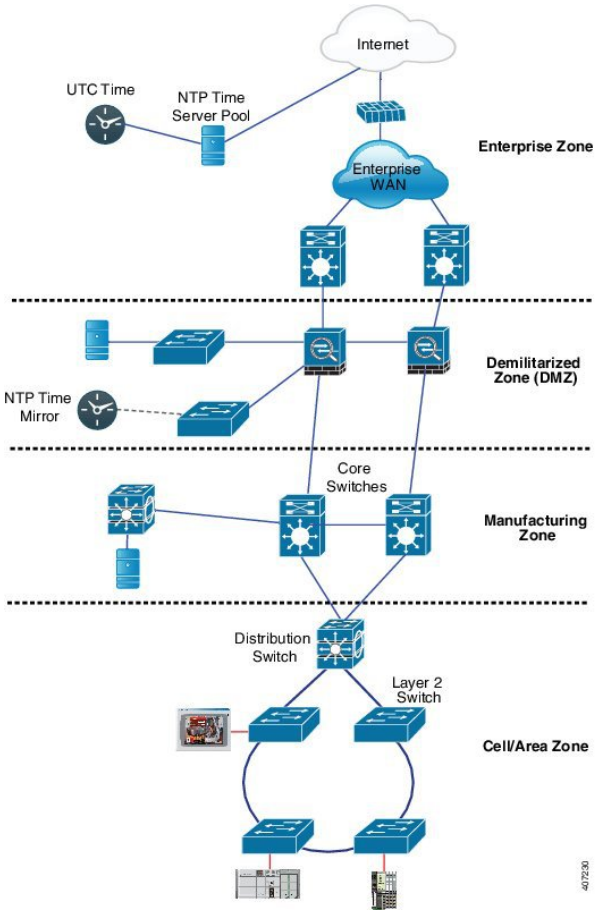
NTP to PTP Time Conversion

NTP to PTP Time Conversion allows you to use Network Time Protocol (NTP) as a time source for PTP. Customers who use PTP for very precise synchronization within a site can use NTP across sites, where precise synchronization is not required.

NTP is the traditional method of synchronizing clocks across packet based networks. NTP uses a two-way time transfer mechanism, between a time source and an end device. NTP is capable of synchronizing a device within a few 100 milliseconds across the Internet, and within a few milliseconds in a tightly controlled LAN. The ability to use NTP as a time source for PTP allows customers to correlate data generated in their PTP network with data in their enterprise data centers running NTP.

The following figure shows an example of an industrial network based on the Industrial Automation and Control System Reference Model. The enterprise zone and demilitarized zone run NTP, and the manufacturing zone and cell/area zone run PTP with NTP as the time source. The switch with the NTP to PTP conversion feature can be either the Layer 2 Switch or the Distribution Switch in the Cell/Area Zone.

Figure 5: Industrial Network with NTP and PTP



Clock Manager

The clock manager is the component in the Cisco NTP to PTP software architecture that keeps track of the various time services and selects the clock that actively provides time. The clock manager notifies the time services of important changes, such as state changes, leap seconds, or daylight saving time.

The clock manager selects the NTP or manually-set clock first, followed by PTP and the real-time clock if NTP is not active. The following table shows the results of the clock selection process.

Table 4: Time Service Selection

NTP (Active) or Manually Set	PTP (Active)	Real-Time Clock	Selected Output
True	Don’t care	Don’t care	NTP or Manually Set
False	True	Don’t care	PTP
False	False	True	Real-Time Clock

In general, the clock manager ensures that the time displayed in the Cisco IOS commands show ptp lan clock and **show clock** match. The **show clock** command always follows this priority, but there are two corner cases where the show ptp lan clock time may differ:

- The router is either a TC or a BC, and there is no other active reference on the network. To preserve backwards compatibility, the TC and BC never take their time from the clock manager, only from the network's PTP GMC. If there is no active PTP GMC, then the time displayed in the **show clock** and the **show ptp lan clock** command output may differ.
- The router is a syntonizing TC, a BC with a slave port, or a GMC-BC with slave port, and the time provided by the PTP GMC does not match the time provided by NTP or the user (that is, manually set). In this case, the PTP clock must forward the time from the PTP GMC. If the PTP clock does not follow the PTP GMC, then the PTP network will end up with two different time bases, which would break any control loops or sequence of event applications using PTP.

The following table shows how the Cisco IOS and PTP clocks behave given the various configurations. Most of the time, the two clocks match. Occasionally, the two clocks are different; those configurations are highlighted in the table.

Table 5: Expected Time Flow

IOS Clock Configuration	PTP Clock Configuration	IOS Clock Source	PTP Clock Source
Calendar	PTP BC, E2E TC, or GMC-BC in BC Mode	PTP	PTP
Manual	PTP BC, E2E TC, or GMC-BC in BC Mode	Manual	PTP
NTP	PTP BC, E2E TC, or GMC-BC in BC Mode	NTP	PTP
Calendar	GMC-BC in GM Mode	Calendar	Calendar
Manual	GMC-BC in GM Mode	Manual	Manual
NTP	GMC-BC in GM Mode	NTP	NTP

GMC Block

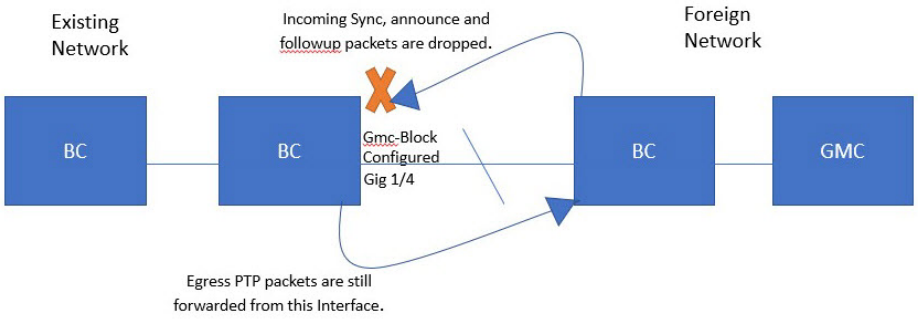
GMC Block protects an existing network from any rogue GMC that might try to synchronize with the devices inside the network. This feature is supported for all PTP clock modes except Forward mode. After the feature is enabled on an interface, only the egress Announce, Sync, and Followup PTP packets are allowed and all ingress Announce, Sync, and Followup packets are dropped on this interface. This prevents the port state transition to time recipient.

Information about a rogue GMC is retrieved from the packets before dropping them. However, egress PTP packets are still allowed from this interface, so it can act as a GMC. To identify the rogue device, details such as IP address and clock ID are stored and displayed for the interface. Two Syslog messages are also generated to notify the presence and clearance of rogue devices.

You can configure PTP gmc-block on multiple ports, if you suspect multiple foreign networks are connected to your existing system. Per-port Syslog messages are displayed after an interval of 30 seconds of receiving rogue packets and after 180 -240 seconds when packets stop coming. Relay minor alarms and SNMP traps are also generated to notify of the presence of foreign rogue devices.

Packet Flow

The following figure shows an example of a PTP network topology with the GMC Block feature configured on an interface.

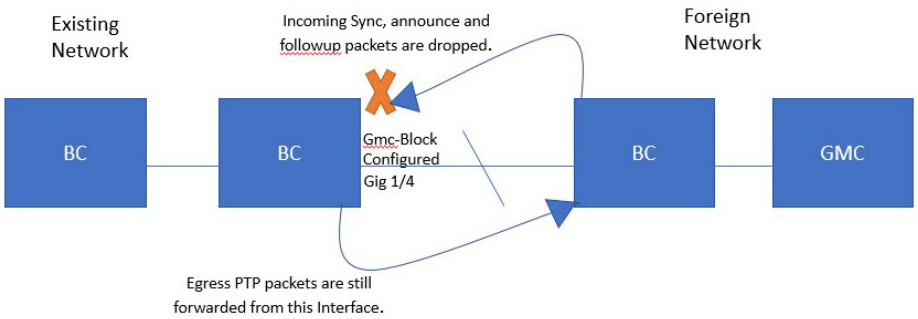


PTP packets originate in the GMC of the foreign network in an attempt to sync with the existing network. When the PTP packets reach the port configured with GMC Block, the packets are dropped after the system retrieves the required information from them.

Because packets from the foreign network are restricted, the system syncs with the local GMC present in the existing system. PTP packets originated on the port configured with GMC Block are still allowed to egress from this interface, which allows devices in the existing network to be GMC.

Packet Flow

The following figure shows an example of a PTP network topology with the GMC Block feature configured on an interface.



PTP packets originate in the GMC of the foreign network in an attempt to sync with the existing network. When the PTP packets reach the port configured with GMC Block, the packets are dropped after the system retrieves the required information from them.

Because packets from the foreign network are restricted, the system syncs with the local GMC present in the existing system. PTP packets originated on the port configured with GMC Block are still allowed to egress from this interface, which allows devices in the existing network to be GMC.

Guidelines and Limitations

PTP Messages

- The Cisco PTP implementation supports only the two-step clock and not the one-step clock.
- Cisco PTP supports multicast PTP messages only.

PTP Mode and Profile

- The router and the grandmaster clock must be in the same PTP domain.
- When Power Profile mode is enabled, the router drops the PTP announce messages that do not include these two Types, Length, Value (TLV) message extensions: *Organization_extension* and *Alternate_timescale*.

  If the grandmaster clock is not compliant with PTP and sends announce messages without these TLVs, configure the router to process the announce message by entering the following command:

  ```
  ptp clock boundary domain 1 profile power
  allow-without-tlv
  ```

- When the router is in Power Profile mode, only the peer_delay mechanism is supported.

  To enable power profile boundary mode and associate interfaces using the clock-port suboption, enter the following command:

  ```
  ptp clock boundary domain 1 profile power
  clock-port 1
  transport ethernet multicast interface gi0/1/1
  ```

- To disable power profile transparent mode, enter the following command, which returns the router to forward mode.

  ```
  no ptp clock transparent domain x profile power
  ```

- To enable the E2E transparent clock, use the following command:

  ```
  ptp clock transparent domain x profile default
  ```

- In Default Profile mode, only the delay_request mechanism is supported.

  To enable default profile boundary clock mode and interfaces associated with clock-port suboption, enter the following command:

  ```
  ptp clock boundary domain 1 profile default
  clock-port 1
  transport ipv4 multicast interface gi0/1/1
  ```

- The 802.1AS profile does not have a clock mode setting.

Packet Format

- The packet format for PTP messages can be 802.1q tagged packets or untagged packets.
- The router does not support 802.1q QinQ tunneling.
- In Power Profile mode:

  - When the PTP interface is configured as an access port, PTP messages are sent as untagged, Layer 2 packets.
  - When the PTP interface is configured as a trunk port, PTP packets are sent as 802.1q tagged Layer 2 packets over the port native VLAN.

- Time recipient IEDs must support tagged and untagged packets.
- When PTP packets are sent on the native VLAN in E2E Transparent Clock Mode, they are sent as untagged packets. To configure the switch to send them as tagged packets, enter the global **vlan dot1q tag native** command.

VLAN Configuration

- Sets the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port.
- In boundary mode, only PTP packets in PTP VLAN will be processed, PTP packets from other VLANs will be dropped.
- Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.
- Most grandmaster clocks use the default VLAN 0. In Power Profile mode, the router default VLAN is VLAN 1 and VLAN 0 is reserved. When you change the default grandmaster clock VLAN, it must be changed to a VLAN other than 0.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.

Clock Configuration

- All PHY PTP clocks are synchronized to the grandmaster clock. The router system clock is not synchronized as part of PTP configuration and processes.
- When VLAN is enabled on the grandmaster clock, it must be in the same VLAN as the native VLAN of the PTP port on the router.
- Grandmaster clocks can drop untagged PTP messages when a VLAN is configured on the grandmaster clock. To force the router to send tagged packets to the grandmaster clock, enter the global **vlan dot1q tag native** command.

PTP Interaction with Other Features

- IR8340 does not support PTP over Port Channels.
- The following PTP clock modes only operate on a single VLAN:
  - e2etransparent
  - p2ptransparent

NTP to PTP Conversion

- The NTP to PTP feature supports the Default E2E Profile and Power Profile.

Default Settings

- PTP is enabled on the router by default.
- By default, the router uses configuration values defined in the Default Profile (Default Profile mode is enabled).
- The router default PTP clock mode is E2E Transparent Clock Mode.
- The default BC synchronization algorithm is linear filter.

Configuring GMC Mode

The following sections provide steps for configuring GMC mode for default and power profiles.

Configuring GMC Mode for a Default Profile

Follow these steps to configure GMC mode for a default profile:

SUMMARY STEPS

1. **ptp clock boundary domain** *domain-number* **profile default**
2. **gmc-bc default**
3. **clock-port** *port-name*
4. **transport ipv4 multicast** *interface-type interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ptp clock boundary domain** *domain-number* **profile default** **Example:** `router(config)# ptp clock boundary domain 0 profile default`	Enable the default profile boundary mode.
Step 2	**gmc-bc default** **Example:** `router(config-ptp-clk)# gmc-bc default`	Enable the GMC boundary clock.
Step 3	**clock-port** *port-name* **Example:** `router(config-ptp-clk)# clock-port port1`	Define a new clock port.

	Command or Action	Purpose
Step 4	**transport ipv4 multicast** *interface-type interface-number* **Example:** `router(config-ptp-port)# transport ipv4 multicast interface Gi0/1/1`	Specify the transport mechanism for clocking traffic.

Configuring GMC Mode for a Power Profile

Complete the steps in this section to configure GMC mode for a power profile.

SUMMARY STEPS

1. **ptp clock boundary domain** *domain-number* **profile power**
2. **gmc-bc default**
3. **clock-port** *port-name*
4. **transport ethernet multicast** *interface-type interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ptp clock boundary domain** *domain-number* **profile power** **Example:** `router(config)# ptp clock boundary domain 0 profile power`	Enable the power profile boundary mode.
Step 2	**gmc-bc default** **Example:** `router(config-ptp-clk)# gmc-bc default`	Enable the GMC boundary clock.
Step 3	**clock-port** *port-name* **Example:** `routerrouter(config-ptp-clk)# clock-port port1`	Defines a new clock port.
Step 4	**transport ethernet multicast** *interface-type interface-number* **Example:** `router(config-ptp-port)# transport ethernet multicast interface gi0/1/1`	Specifies the transport mechanism for clocking traffic.

Configuring PTP Default Profile

This section describes how to configure the router to operate in Default Profile mode.

Configuring an Ordinary Clock Client

Follow these steps to configure the router as an ordinary clock client:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain** *domain-number* **profile default**
4. **clock-port** *port-name* {**master** | **slave**}
5. **transport ipv4 multicast interface** *interface-type interface-number*
6. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock ordinary domain** *domain-number* **profile default** **Example:** `Router(config)# ptp clock ordinary domain 0 profile default`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream. • transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	**clock-port** *port-name* {**master**	**slave**} **Example:** `Router(config-ptp-clk)# clock-port slave slave`	Defines a new clock port and sets the port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.
Step 5	**transport ipv4 multicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ipv4 multicast interface Gi0/1/11`	Specifies the transport mechanism for clocking traffic.
Step 6	(Optional) **vlan** *vlan-id* **Example:**	Configure VLAN for tagged packets.

	Command or Action	Purpose
	`vlan 100`	

Example

Example of Untagged

```
ptp clock ordinary domain 0  profile default
 clock-port slave slave
  transport ipv4 multicast interface Gi0/1/11
```

Example of Tagged

```
ptp clock ordinary domain 0  profile default
 clock-port slave slave
  transport ipv4 multicast interface Gi0/1/11
  vlan 100
```

Configuring a Boundary Clock

If an interface is not added as part of BC clock, it will be in forward mode exchanging PTP packets, which will cause instability in PTP operation. To avoid this, it is recommended to disable PTP on all such interfaces using the **no ptp enable** command.

Follow these steps to configure the router as a boundary clock:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock boundary domain** *domain-number* **profile default**
4. **clock-port** *port-name*
5. **transport ipv4 multicast interface** *interface-type interface-number*
6. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock boundary domain** *domain-number* **profile default** **Example:**	Configures the PTP clock. You can create the following clock types:

	Command or Action	Purpose
	`Router(config)# ptp clock boundary domain 0 profile default`	• ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream. • transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	**clock-port** *port-name* **Example:** `Router(config-ptp-clk)# clock-port dyn1`	Defines a new clock port.
Step 5	**transport ipv4 multicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ipv4 multicast interface Gi0/1/0`	Specifies the transport mechanism for clocking traffic.
Step 6	(Optional) **vlan** *vlan-id* **Example:** `vlan 100`	Configure VLAN for tagged packets.

Example

Example of Untagged

```
ptp clock boundary domain 0  profile default
 clock-port dyn1
  transport ipv4 multicast interface Gi0/1/0
 clock-port dyn2
  transport ipv4 multicast interface Gi0/1/2
```

Example of Tagged

```
ptp clock boundary domain 0  profile default
 clock-port dyn1
  transport ipv4 multicast interface Gi0/1/0
  vlan 100
 clock-port dyn2
  transport ipv4 multicast interface Gi0/1/2
  vlan 200
```

Configuring a Transparent Clock

All interfaces will be part of TC mode once configured.

Follow these steps to configure the router as a transparent clock.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock transparent domain** *domain-number* **profile default**
4. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock transparent domain** *domain-number* **profile default** **Example:** `Router(config)# ptp clock transparent domain 0 profile default`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream. • transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	(Optional) **vlan** *vlan-id* **Example:** `vlan 100`	Configure VLAN for tagged packets.

Example

Example of Untagged

```
ptp clock transparent domain 0  profile default
```

Example of Tagged

```
ptp clock transparent domain 0  profile default
vlan 100
```

Example of not Including TLV Extensions: Power Profile-2011

```
ptp clock transparent domain 0 profile power
allow-without-tlv
```

Example of not Including TLV Extensions: Power Profile-2017

```
ptp clock transparent domain 0 profile power-2017
allow-without-tlv
```

Configuring PTP Power Profile

This section describes how to configure the router to use the PTP Power Profile.

The Power Profile defines a subset of PTP which is intended to run over layer 2 networks, that is, Ethernet, but no Internet Protocol.

Note Power Profile-2017 is supported only in Transparent Clock mode.

Configuring an Ordinary Clock

Follow these steps to configure the router as an ordinary clock:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain** *domain-number* **profile power**
4. **clock-port** *port-name* {**master** | **slave**}
5. **transport ipv4 multicast interface** *interface-type interface-number*
6. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock ordinary domain** *domain-number* **profile power** **Example:** `Router(config)# ptp clock ordinary domain 0 profile power`	Configures the PTP clock. You can create the following clock types: • ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode. • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream.

	Command or Action	Purpose
		• transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	**clock-port** *port-name* {**master** | **slave**} **Example:** `Router(config-ptp-clk)# clock-port slave slave`	Defines a new clock port and sets the port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.
Step 5	**transport ipv4 multicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ipv4 multicast interface Gi0/1/11`	Specifies the transport mechanism for clocking traffic.
Step 6	(Optional) **vlan** *vlan-id* **Example:** `vlan 100`	Configure VLAN for tagged packets.

Example

Example of Untagged

```
ptp clock ordinary domain 0  profile power
 clock-port slave slave
  transport ipv4 multicast interface Gi0/1/11
```

Example of Tagged

```
ptp clock ordinary domain 0  profile power
 clock-port slave slave
  transport ipv4 multicast interface Gi0/1/11
  vlan 100
```

Configuring a Boundary Clock

If an interface is not added as part of BC clock, it will be in forward mode exchanging PTP packets, which will cause instability in PTP operation. To avoid this, it is recommended to disable PTP on all such interfaces using the **no ptp enable** command.

Follow these steps to configure the router as a boundary clock:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock boundary domain** *domain-number* **profile power**
4. **clock-port** *port-name*
5. **transport ethernet multicast interface** *interface-type interface-number*
6. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock boundary domain** *domain-number* **profile power** **Example:** `Router(config)# ptp clock boundary domain 0 profile default`	Configures the PTP clock. You can create the following clock types: • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream. • transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	**clock-port** *port-name* **Example:** `Router(config-ptp-clk)# clock-port dyn1`	Defines a new clock port.
Step 5	**transport ethernet multicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ethernet multicast interface Gi0/1/0`	Specifies the transport mechanism for clocking traffic.
Step 6	(Optional) **vlan** *vlan-id* **Example:** `vlan 100`	Configure VLAN for tagged packets.

Example

Example of Untagged

```
ptp clock boundary domain 0  profile power
 clock-port dyn1
  transport ethernet multicast interface Gi0/1/0
 clock-port dyn2
  transport ethernet multicast interface Gi0/1/2
```

Example of Tagged

```
ptp clock boundary domain 0  profile power
 clock-port dyn1
  transport ethernet multicast interface Gi0/1/0
  vlan 100
 clock-port dyn2
```

```
transport ethernet multicast interface Gi0/1/2
vlan 100
```

Configuring a Transparent Clock

Follow these steps to configure the router as a transparent clock.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock transparent domain** *domain-number* **profile power**
4. (Optional) **vlan** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock transparent domain** *domain-number* **profile power** **Example:** `Router(config)# ptp clock transparent domain 0 profile power`	Configures the PTP clock. You can create the following clock types: • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream. • transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.
Step 4	(Optional) **vlan** *vlan-id* **Example:** `vlan 100`	Configure VLAN for tagged packets.

Example

Example of Untagged

```
ptp clock transparent domain 0  profile power
```

Example of Tagged

```
ptp clock transparent domain 0  profile power
vlan 100
```

Example of not Including TLV Extensions: Power Profile-2011

```
ptp clock transparent domain 0 profile power
allow-without-tlv
```

Example of not Including TLV Extensions: Power Profile-2017

```
ptp clock transparent domain 0 profile power-2017
allow-without-tlv
```

Configuring 802.1AS Profile

This section describes how to configure the router to use the 802.1AS Profile.

Generalized Precision Time Protocol (gPTP) is an IEEE 802.1AS standard, which provides a mechanism to synchronize clocks of the bridges and end point devices in an AVB network. It defines the mechanism to elect the grandmaster clock (BMCA) among the time-aware bridges and talker and listener. The grandmaster is the root of the timing hierarchy that gets established in the time-aware network and distributes time to nodes below to enable synchronization.

A gPTP domain, hereafter referred to as simply a domain, consists of one or more time-aware systems and links that meet the requirements of this standard and communicate with each other as defined by the IEEE 802.1AS protocol. A gPTP domain defines the scope of gPTP message communication, state, operations, data sets, and timescale.

The domain number of a gPTP domain shall be 0.

There are two types of time-aware systems used in a gPTP domain, as follows:

- time-aware end station
- time-aware Bridge

Note Dot1as profile supports BC type only. It does not support TC and OC-slave.

Note Dot1as profile is not supported when GNSS is enabled on the device.

Configuring a Boundary Clock

If an interface is not added as part of BC clock, it will be in forward mode exchanging PTP packets, which will cause instability in PTP operation. To avoid this, it is recommended to disable PTP on all such interfaces using the **no ptp enable** command.

Follow these steps to configure the router as a boundary clock:

SUMMARY STEPS

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

3. **ptp clock boundary domain** *domain-number* **profile dot1as**
4. **clock-port** *port-name*
5. **transport ethernet multicast interface** *interface-type interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters configuration mode.
Step 3	**ptp clock boundary domain** *domain-number* **profile dot1as** **Example:** `Router(config)# ptp clock boundary domain 0 profile dot1as`	Configures the PTP clock. You can create the following clock type: • boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream.
Step 4	**clock-port** *port-name* **Example:** `Router(config-ptp-clk)# clock-port dyn1`	Defines a new clock port.
Step 5	**transport ethernet multicast interface** *interface-type interface-number* **Example:** `Router(config-ptp-port)# transport ethernet multicast interface Gi0/1/0`	Specifies the transport mechanism for clocking traffic.

Example

```
ptp clock boundary domain 0  profile dot1as
 clock-port dyn1
  transport ethernet multicast interface Gi0/1/0
 clock-port dyn2
  transport ethernet multicast interface Gi0/1/2
```

Disable PTP

Complete the steps in this section to disable PTP on an interface.

Note The following procedure applies to both default and power modes.

SUMMARY STEPS

1. **interface** *interface-id*
2. **no ptp enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *interface-id* **Example:** `router(config)# interface gi0/1/1`	Enter interface configuration mode.
Step 2	**no ptp enable**	Disable PTP on the interface.

PTP Multidomain

IR8340 can configure up to 4 different clock domains. All domains can be of different profiles and roles. There is a restriction of supporting only one TC at a time, but you can have multiple BC/OC domains.

```
DUT1#show run | sec ptp
ptp clock boundary domain 1  profile default
 clock-port 1
  transport ipv4 multicast interface Gi0/1/0
ptp clock boundary domain 2  profile power
 clock-port mas
  transport ethernet multicast interface Gi0/1/1
ptp clock ordinary domain 3  profile default
 clock-port sl slave
  transport ipv4 multicast interface Gi0/1/2
ptp clock transparent domain 4  profile power
```

GMC COMMANDS:

```
ptp clock boundary domain 2  profile power|default
Gmc-bc source 0 ntp or Gmc-bc source 0 ptp domain 1 --- we can specifically mention sources
Gmc-bc default --- This command will take NTP|Handset based on availability and class value.
```

Verifying the Configuration

You can use the following commands to verify the PTP configuration:

- show ptp clock dataset parent
- show ptp clock dataset current
- show ptp clock dataset time-properties
- show ptp clock dataset default
- show ptp clock running
- show ptp port dataset port

- show ptp lan clock
- show ptp lan port counters messages
- show ptp lan port counters errors
- show ptp lan foreign-master-record
- show ptp lan rogue-master-record
- show ptp lan histogram ?

  delay—Show PTP histogram of mean path delay

  offset—Show PTP histogram of offset

  time-error—Show PTP history of time error (last 15 days)
- show ptp lan history ?

  delay—Show PTP history of mean path delay (last 15 days)

  offset—Show PTP history of offset (last 15 days)

  time-error—Show PTP history of time error (last 15 days)

The following example shows the Default Profile configuration:

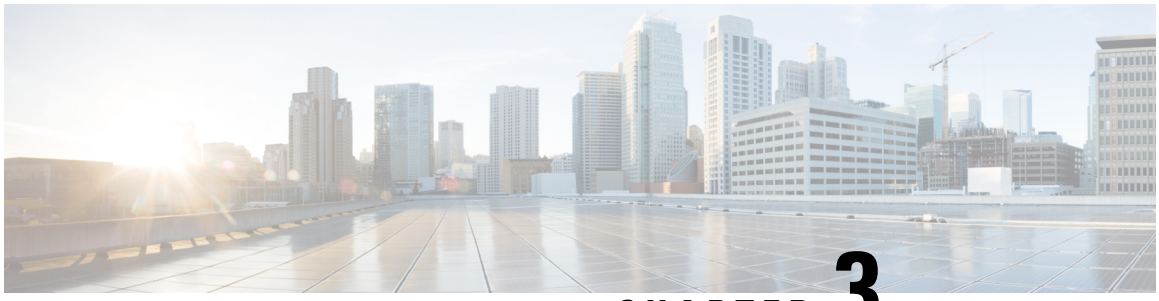
```
DUT1#show ptp lan clock running
                    PTP Boundary Clock [Domain 0]  [Profile: default]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              7340           13877          Hot standby
                              PORT SUMMARY
                                                                     PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
1     mcast       negotiated   Gi0/1/0     Slave        1            UNKNOWN
DUT1#
```

The following example shows the Power Profile configuration:

```
DUT1#show ptp clock running
                    PTP Boundary Clock [Domain 0]  [Profile: power]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              193            46             Hot standby
                              PORT SUMMARY
                                                                       PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
1     mcast       negotiated   Ethernet     Slave        1            UNKNOWN
DUT1#
```

The following example shows the 802.1AS Profile configuration:

```
DUT1#show ptp clock running
                    PTP Boundary Clock [Domain 0]  [Profile: dot1as]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              1193            1146             Hot standby
                              PORT SUMMARY
                                                                       PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
1     mcast       negotiated   Ethernet     Slave        1            UNKNOWN
DUT1#
```



CHAPTER 3

Configuring Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 is documented in RFC 1305.

This chapter explains how to configure Network Time Protocol on IR8340.

NTP configuration is supported from Cisco IOS XE Release 17.7.x.

- Restrictions for Network Time Protocol, on page 39
- Information About Network Time Protocol, on page 40
- How to Configure Network Time Protocol, on page 44
- Configuration Examples for Network Time Protocol, on page 49
- Additional References for Network Time Protocol, on page 50
- Feature Information for Network Time Protocol, on page 50

Restrictions for Network Time Protocol

The Network Time Protocol (NTP) package contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. NTP versions 4.2.4p7 and earlier are vulnerable.

The vulnerability is due to an error in handling of certain malformed messages. An unauthenticated, remote attacker could send a malicious NTP packet with a spoofed source IP address to a vulnerable host. The host that processes the packet sends a response packet back to the transmitter. This action could start a loop of messages between the two hosts that could cause both the hosts to consume excessive CPU resources, use up the disk space by writing messages to log files, and consume the network bandwidth. All of these could cause a DoS condition on the affected hosts.

For more information, see the Network Time Protocol Package Remote Message Loop Denial of Service Vulnerability web page.

Cisco software releases that support NTPv4 are not affected. All other versions of Cisco software are affected.

To display whether a device is configured with NTP, use the **show running-config | include ntp** command. If the output returns any of the following commands, then that device is vulnerable to the attack:

- **ntp broadcast client**
- **ntp primary**
- **ntp multicast client**
- **ntp peer**

- **ntp server**

For more information on understanding Cisco software releases, see the White Paper: Cisco IOS and NX-OS Software Reference Guide.

There are no workarounds for this vulnerability other than disabling NTP on the device. Only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Depending on your release, your feature will process NTP mode 7 packets and will display the message "NTP: Receive: dropping message: Received NTP private mode 7 packet " if debugs for NTP are enabled. Configure the **ntp allow mode private** command to process NTP mode 7 packets. This command is disabled by default.

Note NTP peer authentication is not a workaround and is a vulnerable configuration.

NTP services are disabled on all interfaces by default.

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

Line Aux 0 option is disabled by default.

Information About Network Time Protocol

Network Time Protocol

Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs on User Datagram Protocol (UDP), which in turn runs on IP. NTP Version 3 is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to the accuracy of within a millisecond of one another.

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

NTP has two ways to avoid synchronizing to a machine whose time may not be accurate. NTP will never synchronize to a machine that is not in turn synchronized. NTP will compare the time reported by several machines, and will not synchronize to a machine whose time is significantly different from others, even if its stratum is lower. This strategy effectively builds a self-organizing tree of NTP servers.

The Cisco implementation of NTP does not support stratum 1 service; that is, you cannot connect to a radio or atomic clock (for some specific platforms, however, you can connect to a GPS time-source device). Cisco recommends that the time service for your network be derived from the public NTP servers available in the IP Internet.

If the network is isolated from the Internet, the Cisco implementation of NTP allows a machine to be configured so that it acts as though it is synchronized via NTP, when in fact it has determined the time using other means. Other machines can then synchronize to that machine via NTP.

A number of manufacturers include NTP software for their host systems and a publicly available version for systems running UNIX. This software also allows UNIX-derivative servers to acquire the time directly from an atomic clock, which would subsequently propagate time information along to Cisco routers.

The communications between machines running NTP (known as associations) are usually statically configured; each machine is given the IP address of all machines with which it should form associations. Accurate timekeeping is made possible through exchange of NTP messages between each pair of machines with an association.

However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each machine can be configured to send or receive broadcast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

The time kept on a machine is a critical resource, so Cisco strongly recommends that you use the security features of NTP to avoid the accidental or malicious setting of incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

When multiple sources of time (Virtual Integrated Network System (VINES), hardware clock, manual configuration) are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

NTP services are disabled on all interfaces by default.

For more information about NTP, see the following sections:

Poll-Based NTP Associations

Networking devices running NTP can be configured to operate in variety of association modes when synchronizing time with reference time sources. A networking device can obtain time information on a network in two ways—by polling host servers and by listening to NTP broadcasts. This section focuses on the poll-based association modes. Broadcast-based NTP associations are discussed in the *Broadcast-Based NTP Associations* section.

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

- Client mode
- Symmetric active mode

The client and the symmetric active modes should be used when NTP is required to provide a high level of time accuracy and reliability.

When a networking device is operating in the client mode, it polls its assigned time-serving hosts for the current time. The networking device will then pick a host from among all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host will not capture or use any time information sent by the local client device. This mode is most suited for file-server and workstation clients that are not required to provide any form of time synchronization to other local clients. Use the **ntp server** command to individually specify the time server that you want your networking device to consider synchronizing with and to set your networking device to operate in the client mode.

When a networking device is operating in the symmetric active mode, it polls its assigned time-serving hosts for the current time and it responds to polls by its hosts. Because this is a peer-to-peer relationship, the host

will also retain time-related information of the local networking device that it is communicating with. This mode should be used when a number of mutually redundant servers are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet adopt this form of network setup. Use the **ntp peer** command to individually specify the time serving hosts that you want your networking device to consider synchronizing with and to set your networking device to operate in the symmetric active mode.

The specific mode that you should set for each of your networking devices depends primarily on the role that you want them to assume as a timekeeping device (server or client) and the device's proximity to a stratum 1 timekeeping server.

A networking device engages in polling when it is operating as a client or a host in the client mode or when it is acting as a peer in the symmetric active mode. Although polling does not usually place a burden on memory and CPU resources such as bandwidth, an exceedingly large number of ongoing and simultaneous polls on a system can seriously impact the performance of a system or slow the performance of a given network. To avoid having an excessive number of ongoing polls on a network, you should limit the number of direct, peer-to-peer or client-to-server associations. Instead, you should consider using NTP broadcasts to propagate time information within a localized network.

Broadcast-Based NTP Associations

Broadcast-based NTP associations should be used when time accuracy and reliability requirements are modest and if your network is localized and has more than 20 clients. Broadcast-based NTP associations are also recommended for use on networks that have limited bandwidth, system memory, or CPU resources.

A networking device operating in the broadcast client mode does not engage in any polling. Instead, it listens for NTP broadcast packets that are transmitted by broadcast time servers. Consequently, time accuracy can be marginally reduced because time information flows only one way.

Use the **ntp broadcast client** command to set your networking device to listen for NTP broadcast packets propagated through a network. For broadcast client mode to work, the broadcast server and its clients must be located on the same subnet. You must enable the time server that transmits NTP broadcast packets on the interface of the given device by using the **ntp broadcast** command.

NTP Access Group

The access list-based restriction scheme allows you to grant or deny certain access privileges to an entire network, a subnet within a network, or a host within a subnet. To define an NTP access group, use the **ntp access-group** command in global configuration mode.

The access group options are scanned in the following order, from least restrictive to the most restrictive:

1. **ipv4** —Configures IPv4 access lists.
2. **ipv6** —Configures IPv6 access lists.
3. **peer** —Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
4. **serve** —Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
5. **serve-only** —Allows only time requests from a system whose address passes the access list criteria.
6. **query-only** —Allows only NTP control queries from a system whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted access. If no access groups are specified, all access types are granted access to all systems. If any access groups are specified, only the specified access types will be granted access.

For details on NTP control queries, see RFC 1305 (NTP Version 3).

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

The authentication process begins from the moment an NTP packet is created. Cryptographic checksum keys are generated using the message digest algorithm 5 (MD5) and are embedded into the NTP synchronization packet that is sent to a receiving client. Once a packet is received by a client, its cryptographic checksum key is decrypted and checked against a list of trusted keys. If the packet contains a matching authentication key, the time-stamp information that is contained within the packet is accepted by the receiving client. NTP synchronization packets that do not contain a matching authenticator key are ignored.

Note In large networks, where many trusted keys must be configured, the Range of Trusted Key Configuration feature enables configuring multiple keys simultaneously.

It is important to note that the encryption and decryption processes used in NTP authentication can be very CPU-intensive and can seriously degrade the accuracy of the time that is propagated within a network. If your network setup permits a more comprehensive model of access control, you should consider the use of the access list-based form of control.

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

NTP Services on a Specific Interface

Network Time Protocol (NTP) services are disabled on all interfaces by default. NTP is enabled globally when any NTP commands are entered. You can selectively prevent NTP packets from being received through a specific interface by using the **ntp disable** command in interface configuration mode.

Source IP Address for NTP Packets

When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the **ntp source** interface command in global configuration mode to configure a specific interface from which the IP source address will be taken.

This interface will be used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** command.

System as an Authoritative NTP Server

Use the **ntp** command in global configuration mode if you want the system to be an authoritative NTP server, even if the system is not synchronized to an outside time source.

Note Use the **ntp primary** command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **ntp primary** command can cause instability in timekeeping if the machines do not agree on the time.

How to Configure Network Time Protocol

Configuring NTP

Configuring Poll-Based NTP Associations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**]
4. **ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**ntp peer** *ip-address* [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Router(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer`	Forms a peer association with another system.
Step 4	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Router(config)# ntp server 192.168.10.1 version 2 prefer`	Forms a server association with another system.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Broadcast-Based NTP Associations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ntp broadcast version** *number*
5. **ntp broadcast client**
6. **ntp broadcastdelay** *microseconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ntp broadcast version** *number* **Example:** `Router(config-if)# ntp broadcast version 2`	Configures the specified interface to send NTP broadcast packets.
Step 5	**ntp broadcast client** **Example:** `Router(config-if)# ntp broadcast client`	Configures the specified interface to receive NTP broadcast packets.
Step 6	**ntp broadcastdelay** *microseconds* **Example:** `Router(config-if)# ntp broadcastdelay 100`	Adjusts the estimated round-trip delay for NTP broadcasts.

	Command or Action	Purpose
Step 7	**end** **Example:** `Router(config)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring an External Reference Clock

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line aux** *line-number*
4. **end**
5. **show ntp associations**
6. **show ntp status**
7. **debug ntp refclock**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**line aux** *line-number* **Example:** `Router(config)# line aux 0`	Enters line configuration mode for the auxiliary port 0.
Step 4	**end** **Example:** `Router(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.
Step 5	**show ntp associations** **Example:** `Router# show ntp associations`	Displays the status of NTP associations, including the status of the GPS reference clock.
Step 6	**show ntp status** **Example:** `Router# show ntp status`	Displays the status of NTP.

	Command or Action	Purpose
Step 7	**debug ntp refclock** **Example:** `Router# debug ntp refclock`	Allows advanced monitoring of reference clock activities for the purposes of debugging.

Configuring NTP Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ntp authenticate**
4. **ntp authentication-key** *number* **md5** *key*
5. **ntp authentication-key** *number* **md5** *key*
6. **ntp authentication-key** *number* **md5** *key*
7. **ntp trusted-key** *key-number* [- *end-key*]
8. **ntp server** *ip-address* **key** *key-id*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**ntp authenticate** **Example:** `Router(config)# ntp authenticate`	Enables the NTP Authentication feature.
Step 4	**ntp authentication-key** *number* **md5** *key* **Example:** `Router(config)# ntp authentication-key 1 md5 key1`	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 5	**ntp authentication-key** *number* **md5** *key* **Example:** `Router(config)# ntp authentication-key 2 md5 key2`	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 6	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.

	Command or Action	Purpose
	`Router(config)# ntp authentication-key 3 md5 key3`	
Step 7	**ntp trusted-key** *key-number* [- *end-key*] **Example:** `Router(config)# ntp trusted-key 1 - 3`	Defines trusted authentication keys. • If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets.
Step 8	**ntp server** *ip-address* **key** *key-id* **Example:** `Router(config)# ntp server 172.16.22.44 key 2`	Allows the software clock to be synchronized by an NTP time server.
Step 9	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Network Time Protocol

show clock [detail]

This command displays the current software clock time. The following is sample output from this command.

Example:

```
Device# show clock detail

*18:38:21.655 UTC Tue Jan 4 2011
Time source is hardware calendar
```

show ntp associations detail

This command displays the status of NTP associations. The following is sample output from this command.

Example:

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
delay 0.00 msec, offset 0.0000 msec, dispersion 15937.50
precision 2**24, version 4
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time D0CDE881.9A6A9005 (18:42:09.603 UTC Tue Jan 4 2011)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
192.168.45.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode client, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 16003.08
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**24, version 4
```

```
org time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
filtdelay =     0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filtoffset =    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00
filterror =  16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
minpoll = 6, maxpoll = 10
```

show ntp status

This command displays the status of NTP. The following is sample output from this command.

Example:

```
Device# show ntp status

Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
reference time is D25AF07C.4B439650 (15:26:04.294 PDT Tue Oct 21 2011)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 16, last update was 10 sec ago.
```

Configuration Examples for Network Time Protocol

Example: Configuring Network Time Protocol

In the following example, a device with a hardware clock that has server associations with two other systems sends broadcast NTP packets, periodically updates the hardware clock, and redistributes time into VINES:

```
clock timezone PST -8
clock summer-time PDT recurring

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
In the following example, a device with a hardware clock has no outside time source, so it
 uses the hardware clock as an authoritative time source and distributes the time via NTP
broadcast packets:


clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
The following example shows Line Aux 0 option is disabled by default.

config-register 0x0
reload
rommon 1 > set
rommon 2 >  AUX_PORT=1
rommon 3 > SYNC
rommon 4 > reset
rommon 1 > set
```

```
rommon 2 > confreg 0x2102
rommon 3 > reset
```

Additional References for Network Time Protocol

Related Documents

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

Standards and RFCs

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

Technical Assistance

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

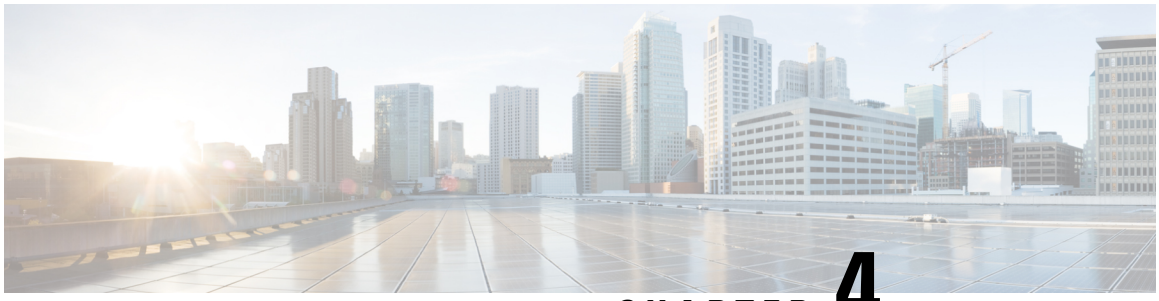
Feature Information for Network Time Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 6: Feature Information for Network Time Protocol

Feature Name	Feature Information
Network Time Protocol	NTP is a protocol designed to time-synchronize a network of machines. NTP runs on UDP, which in turn runs on IP. NTP is documented in RFC 1305.



CHAPTER 4

NTP Timing Based on PTP Clock

- PTP as a Reference Clock for NTP, on page 53
- Enabling PTP as a Reference Clock for NTP, on page 53
- Validate the PTP Reference Clock, on page 54
- Troubleshooting PTP as an NTP Reference Clock, on page 54

PTP as a Reference Clock for NTP

You can configure Precision Timing Protocol (PTP) time as the reference clock for Network Time Protocol (NTP) by enabling the feature on the IR8340 router.

PTP time acts as a stratum 0 source, and the Cisco IOS NTP server acts as a stratum 1 device. The server then provides clock information to its NTP clients (strata 2 and 3).

The feature is supported on Cisco Catalyst IR8340 Rugged Series Routers beginning with the Cisco IOS-XE Release 17.9.1. A Network Advantage license is required.

Enabling PTP as a Reference Clock for NTP

The PTP reference clock feature is disabled by default. You enable it by entering a CLI command. Before you begin, configure PTP and ensure that it is in slave mode. See the chapter Configuring Precision Time Protocol (PTP), on page 7 in this guide for configuration instructions.

To enable PTP as a reference clock for NTP, enter the **ntp refclock ptp** command.

You disable the PTP reference clock feature by entering the **no ntp refclock ptp** command.

Note On IR8340, this feature is supported only with PTP Default, Power, and Dot1as profiles. Telecom profiles (8265.1/8275.1) as source are not supported. You can only enable this feature when **ntp refclock gnss** is disabled, as NTP can take only one reference at a time, either GNSS or PTP.

To validate the PTP reference clock configuration on the router, see Validate the PTP Reference Clock, on page 54.

Validate the PTP Reference Clock

After you enable PTP as the reference clock for NTP, you can enter CLI commands to validate the configuration.

Step 1 Ccheck that the PTP reference clock configuration is correct and that the feature is running.

Example:

```
#show run | sec ptp|ntp
ntp refclock ptp
ptp clock boundary domain 0  profile power
 clock-port 1
  transport ethernet multicast interface Gi0/1/4
```

Step 2 Check that PTP is in slave mode; that is PTP is in phase aligned state, which means it is locked to a master clock.

Example:

```
#show ptp clock running
                    PTP Boundary Clock [Domain 0]  [Profile: power]
        State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
        PHASE_ALIGNED  1              629978         633            Hot standby
                              PORT SUMMARY
                                                                        PTP Master
Name  Tx Mode      Role         Transport    State         Sessions     Port Addr
1     mcast       negotiated   Ethernet     Slave         1            UNKNOWN
```

Step 3 Check that NTP is using PTP as its reference clock.

Example:

```
#show ntp status
Clock is synchronized, stratum 1, reference is .PTP.
nominal freq is 250.0000 Hz, actual freq is 249.9998 Hz, precision is 2**10
ntp uptime is 28233900 (1/100 of seconds), resolution is 4016
reference time is E6161FA8.FFBE7988 (08:26:16.999 UTC Fri Apr 29 2022)
clock offset is 0.9998 msec, root delay is 0.00 msec
root dispersion is 3940.49 msec, peer dispersion is 3938.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000856 s/s
system poll interval is 64, last update was 4 sec ago.
#
```

Troubleshooting PTP as an NTP Reference Clock

Checking PTP-NTP Synchronization

You can check the time on the PTP and NTP cocks to ensure that they are synchronized, as shown in the following example.

```
#show ptp lan clock | inc time
Local clock time: 2022-4-29 8:48:39 UTC
#
#show clock detail
08:48:39.278 UTC Fri Apr 29 2022
```

```
Time source is NTP
#
```

Troubleshooting Commands

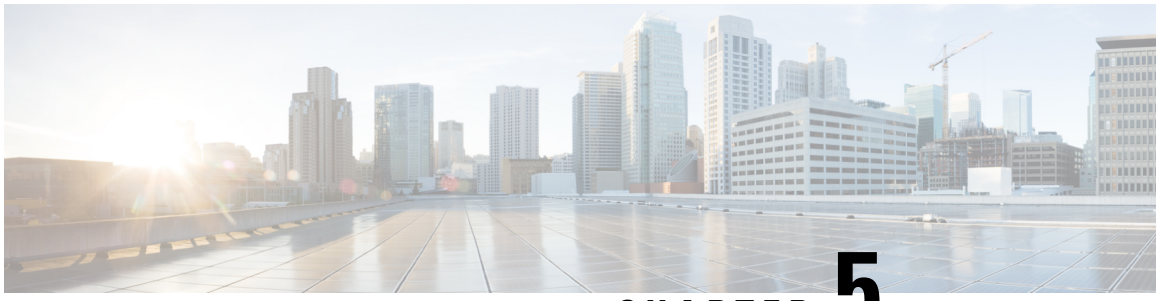
Table 7: Troubleshooting Commands

Command	Description
ntp logging	Enables syslogs from NTP.
debug ntp all	Provides the complete debugging logs for NTP processes.
debug platform software pd-ptp all	Provides debugging logs on the switch relating to PTP as a reference clock.
show ntp status	Shows detailed NTP status, including whether NTP is using PTP as its reference clock.
show ntp association detail	Shows detailed information about NTP peering.
show ptp clock running	Check that PTP is in slave mode; that is PTP is in phase aligned state, which means it is locked to a master clock.

Viewing Peering Details

The command output shows detailed information about NTP peering. You can use the command to check the amount of time the platform takes to switch to the next available timing source after the initial timing source goes down. In the following example, NTP waits 8x256 seconds to switch over to the next source.

```
#show ntp association detail
127.127.6.1 configured, ipv4, our_master, sane, valid, stratum 0
ref ID .PTP., time E61622E9.00000000 (08:40:09.000 UTC Fri Apr 29 2022)
our mode active, peer mode passive, our poll intvl 256, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 4.62
delay 0.00 msec, offset 0.9998 msec, dispersion 2.81, jitter 0.97 msec
precision 2**10, version 4
assoc id 63756, assoc name 127.127.6.1
assoc in packets 11, assoc out packets 17652, assoc error packets 0
org time E61622E8.FFBE7988 (08:40:08.999 UTC Fri Apr 29 2022)
rec time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
xmt time E61622E8.FFBE7988 (08:40:08.999 UTC Fri Apr 29 2022)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtoffset = 0.99 1.99 0.99 0.99 0.99 0.99 1.99 0.99
filterror = 0.97 2.89 4.81 6.73 8.65 10.57 11.53 12.49
minpoll = 4, maxpoll = 10
```



CHAPTER 5

G.8265.1 Profile

- Information about G.8265.1 Profile, on page 57
- G.8265.1 Profile Mapping, on page 58
- Configuring G.8265.1 Server and Client Ordinary Clock, on page 59
- Verifying the Configuration, on page 63

Information about G.8265.1 Profile

G.8265.1 profile fulfills specific frequency-distribution requirements in telecom networks. Features of G.8265.1 profile are:

- **Clock Advertisement**: G.8265.1 specifies changes to values used in Announce messages for advertising PTP clocks: the clock class value is used to advertise the QL of the clock, while other values are not used.
- **Clock Selection**: G.8265.1 profile also defines an alternate Best Master Clock Algorithm (BMCA) to select port states and clocks is defined for the profile. This profile also requires to receive Sync messages (and optionally, Delay-Response messages) to qualify a clock for selection.
- **Port State Decision**: The ports are statically configured to be Master or Slave instead of using FSM to dynamically set port states.
- **Packet Rates**: The packet rates higher than rates specified in the IEEE 1588-2008 standard are used. They are:
  - Sync/Follow-Up Packets: Rates from 128 packets-per-second to 16 seconds-per-packet.
  - Delay-Req/Delay-Resp Packets: Rates from 128 packets-per-second to 16 seconds-per-packet.
  - Announce Packets: Rates from 8 packets-per-second to 64 seconds-per-packet.
- **Transport Mechanism:** G.8265.1 restricts the PTP transport mechanism to IPv4. G.8265.1 mandates that all packets should be sent unicast, rather than multicast.
- **Clock Type**: G.8265.1 restricts the supported clock-types to Ordinary Clock (a clock with only a single PTP port). For a G.8265.1 slave, this means that all PTP ports on a single device operate independently of each other: functions such as clock selection operate outside of the context of each Ordinary Clock within the system.

- **Domain Numbers**: G.8265.1 restricts the range of domain numbers to between 4 and 23, with the default being 4.
- **Port Numbers**: G.8265.1 dictates that all port numbers for PTP ports should be 1, as all clocks within a G.8265.1 network are ordinary clocks.

  G.8265.1 also restricts the clock types in a network to Master and Slave clocks, meaning that neither boundary clock nor transparent clocks are supported. This document covers extensions to G.8265.1 in order to support boundary clock.

Limitations

- G.8265.1 doesn’t support on sub-interface.
- G.8265.1 doesn’t support on vrf interface.
- G.8265.1 doesn’t support on port-channel interfac.

G.8265.1 Profile Mapping

The following table provides the mapping of SSM/ESMC and G.8265.1 QL values.

Table 8: G.8265.1 Profile Mapping

SSM QL	ITU-T G.781			Clock Class
	Option I	Option II	Option III	
0001		QL-PRS		80
0000		QL-STU	QL-UNK	82
0010	QL-PRC			84
0111		QL-ST2		86
0011				88
0100	QL-SSU-A	QL-TNC		90
0101				92
0110				94
1000	QL-SSU-B			96
1001				98
1101		QL-ST3E		100
1010		QL-ST3/QL-EEC2		102
1011	QL-SEC/QL-EEC1		QL-SEC	104
1100		QL-SMC		106
1110		QL-PROV		108
1111		QL-DUS		110

Configuring G.8265.1 Server and Client Ordinary Clock

Configuring Server Ordinary Clock

Follow these steps to configure server ordinary clock:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain** *domain-number* **profile g8265.1**
4. **priority1** *priorityvalue*
5. **priority2** *priorityvalue*
6. **clock-port** *port-name* **master**
7. **transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**]
8. **sync interval** *interval*
9. **announce interval** *interval*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter configuration mode.
Step 3	**ptp clock ordinary domain** *domain-number* **profile g8265.1** **Example:** `Router(config)# ptp clock ordinary domain 4 profile g8265.1`	Configures the PTP ordinary clock. The **profile** keyword configures the clock to use the G.8265.1 profile. Using a telecom profile requires that the clock have a domain number of 4–23.
Step 4	**priority1** *priorityvalue* **Example:** `Router(config-ptp-clk)# priority1 priorityvalue`	Sets the preference level for a clock. Client devices use the priority1 value when selecting a server clock: a lower priority1 value indicates a preferred clock. The priority1 value is considered above all other clock attributes. Valid values are from 0-255. The default value is 128.
Step 5	**priority2** *priorityvalue* **Example:** `Router(config-ptp-clk)# priority1 priorityvalue`	Sets a secondary preference level for a clock. Subordinaate devices use the priority2 value when selecting a server clock: a lower priority2 value indicates a preferred clock.

	Command or Action	Purpose
		The priority2 value is considered only when the router is unable to use priority1 and other clock attributes to select a clock. Valid values are from 0-255. The default value is 128.
Step 6	**clock-port** *port-name* **master** **Example:** `Router(config-ptp-clk)# clock-port master master`	Sets the clock port to PTP server mode.
Step 7	**transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**] **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface GigabitEthernet 0/0/0 negotiation`	Specifies the transport mechanism for clocking traffic. Loopback interface can be used as well as the WAN ports. The client router IP address should be reachable via WAN interface (GigabitEthernet 0/0/0 or GigabitEthernet 0/0/1) so that PTP packets can be sent or received on the WAN ports. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources.
Step 8	**sync interval** *interval* **Example:** `Router(config-ptp-port)# sync interval -4`	Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows: • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second.
Step 9	**announce interval** *interval* **Example:** `Router(config-ptp-port)# announce interval 2`	Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: • 3—1 packet every 8 seconds

	Command or Action	Purpose
		• 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second
Step 10	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Configuring Client Ordinary Clock

Follow these steps to configure client ordinary clock:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ptp clock ordinary domain** *domain-number* **profile g8265.1**
4. **clock-port** *port-name* **slave**
5. **transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**]
6. **delay-req interval** *interval*
7. **announce timeout** *value*
8. **clock source** *source-address*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter configuration mode.

	Command or Action	Purpose
Step 3	**ptp clock ordinary domain** *domain-number* **profile g8265.1** **Example:** `Router(config)# ptp clock ordinary domain 4 profile g8265.1`	Configures the PTP ordinary clock. The **profile** keyword configures the clock to use the G.8265.1 profile. Using a telecom profile requires that the clock have a domain number of 4–23.
Step 4	**clock-port** *port-name* **slave** **Example:** `Router(config-ptp-clk)# clock-port client slave`	Sets the clock port to PTP client mode.
Step 5	**transport ipv4 unicast interface** *interface-type interface-number* [**negotiation**] **Example:** `Router(config-ptp-port)# transport ipv4 unicast interface GigabitEthernet 0/0/0 negotiation`	Specifies the transport mechanism for clocking traffic. Loopback interface can be used as well as the WAN ports. The server router IP address should be reachable via WAN interface (GigabitEthernet 0/0/0 or GigabitEthernet 0/0/1) so that PTP packets can be sent or received on the WAN ports. The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources.
Step 6	**delay-req interval** *interval* **Example:** `Router(config-ptp-port)# delay-req interval -4`	Configures the minimum interval allowed between PTP delay-request messages when the port is in the server state. The intervals are set using log base 2 values, as follows: • 3—1 packet every 8 seconds • 2—1 packet every 4 seconds • 1—1 packet every 2 seconds • 0—1 packet every second • -1—1 packet every 1/2 second, or 2 packets per second • -2—1 packet every 1/4 second, or 4 packets per second • -3—1 packet every 1/8 second, or 8 packets per second • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second. • -7—1 packet every 1/128 seconds, or 128 packets per second.
Step 7	**announce timeout** *value* **Example:**	Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10.

	Command or Action	Purpose
	`Router(config-ptp-port)# announce timeout 8`	
Step 8	**clock source** *source-address* **Example:** `Router(config-ptp-port)# clock-source 8.8.8.1`	Specifies the address of a PTP server clock.
Step 9	**end** **Example:** `Router(config-ptp-port)# end`	Exit configuration mode.

Verifying the Configuration

You can use the following commands to verify a clocking configuration:

- show ptp clock running domain <domain no>
- show ptp clock dataset default
- show ptp clock dataset parent
- show ptp port <name of virtual port>
- show ptp wan stat stream < stream id>
- show network-clock synchronization
- show ptp port dataset port
- show ptp wan tod
- show gnss time
- show gnss status

Examples

```
IR8340#show ptp clock running domain 4
                     PTP Ordinary Clock [Domain 4]  [Profile: g8265.1]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         ACQUIRING      1              1543           4680           Hot standby
                               PORT SUMMARY
                                                                      PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
slave unicast      slave        Gi0/0/1      Slave        1            2.3.1.1
                             SESSION INFORMATION
slave [Gi0/0/1] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 2.3.1.1            4680       1543       0          0
IR8340#

IR8340#show ptp clock running domain 4
                     PTP Ordinary Clock [Domain 4]  [Profile: g8265.1]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              44752          135639         Hot standby
                               PORT SUMMARY
                                                                        PTP Master
```

```
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
slave unicast      slave        Gi0/0/1      Slave        1            2.3.1.1
                              SESSION INFORMATION
slave [Gi0/0/1] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 2.3.1.1            135639     44752      0          0
IR8340#
```

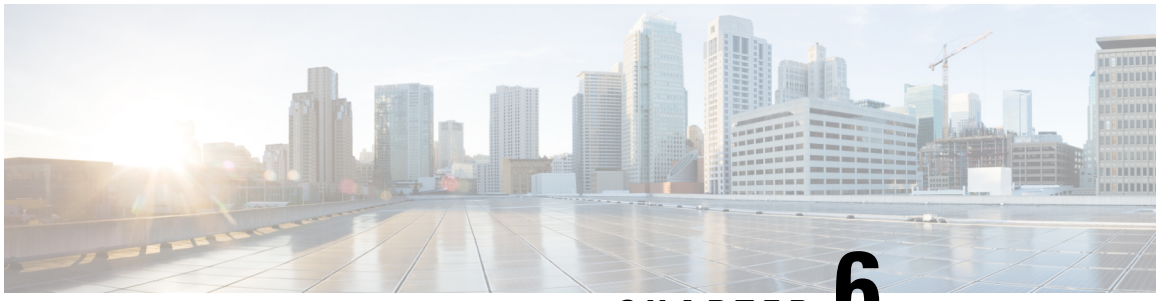
```
IR8340#show ptp clock dataset default
CLOCK [Ordinary Clock, domain 4]
  Profile: g8265.1
  Two Step Flag: No
  Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
  Number Of Ports: 1
  Priority1: 128
  Priority2: 128
  Domain Number: 4
  Slave Only: Yes
  Clock Quality:
    Class: 255
    Accuracy: Unknown
    Offset (log variance): 0
IR8340#
```

```
IR8340#show ptp clock dataset parent
CLOCK [Ordinary Clock, domain 4]
  Profile: g8265.1
  Parent Clock Identity: 0x44:B6:BE:FF:FE:42:EF:13
  Parent Port Number: 0
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 0
  Grandmaster Clock:
    Identity: 0x44:B6:BE:FF:FE:42:EF:13
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 104
      Accuracy: Unknown
      Offset (log variance): 52592
IR8340#
```

```
IR8340#show ptp clock dataset time-properties
CLOCK [Ordinary Clock, domain 4]

  Current UTC Offset Valid: FALSE
  Current UTC Offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: FALSE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: Internal Oscillator
IR8340#
```

```
IR8340#show ptp port dataset port
PORT [slave]
  Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
  Clock Profile: g8265.1
  Transport Interface: GigabitEthernet0/0/1
  Port Number: 1
  Port State: Slave
  Min Delay Req Interval (log base 2): -4
  Peer Mean Path Delay: 0
  Announce interval (log base 2): 1
  Announce Receipt Timeout: 3
```

```
  Sync Interval (log base 2): -5
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): -4
  PTP version: 2
IR8340#

IR8340#show ptp wan stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -5, Acting Interval -5
  Tx packets : 0,  Rx Packets : 96215
  Last Seq Number : 30678,  Error Packets : 0
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 48107, Rx Packets : 0
  Last Seq Number : 0, Error Packets : 0
Delay Response Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 0, Rx Packets : 48107
  Last Seq Number : 48106, Error Packets : 0
Announce Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 1, Acting Interval : 1
  Tx packets : 0, Rx Packets :  1509
  Last Seq Number 1508 Error Packets 0
Signalling Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval : 0
  Tx packets : 12, Rx Packets : 12
  Last Seq Number : 0, Error Packets : 0
Current Data Set                            Units     Within tolerance?
  Offset from master :  +0.000000000        seconds          Yes
  Mean Path Delay    :  +0.000000027        seconds          Yes
  Forward Path Delay :  +0.000000027        seconds          Yes
  Reverse Path Delay :  +0.000000028        seconds          Yes
  Steps Removed 1
IR8340#

IR8340#show ptp wan tod
PTPd ToD information:

Time: 01/05/22 11:35:21

IR8340#
```



CHAPTER 6

G.8275.1 Profile

- Information About G.8275.1, on page 67
- Configuring the G.8275.1 Profile, on page 69
- Verifying the Configuration, on page 70
- Debugging Commands, on page 73

Information About G.8275.1

The IEEE 1588-2008 standard, in which the Precision Time Protocol (PTP) is defined, allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. ITU-T G.8275.1 with full timing support from the network is a PTP profile for use in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol and provide PHY-layer frequency support.

Synchronization Model

The model adopted for G.8275.1 is “hop-by-hop” synchronization. Each network element on the path from master to slave synchronizes its local clock to upstream devices and provides synchronization to downstream devices.

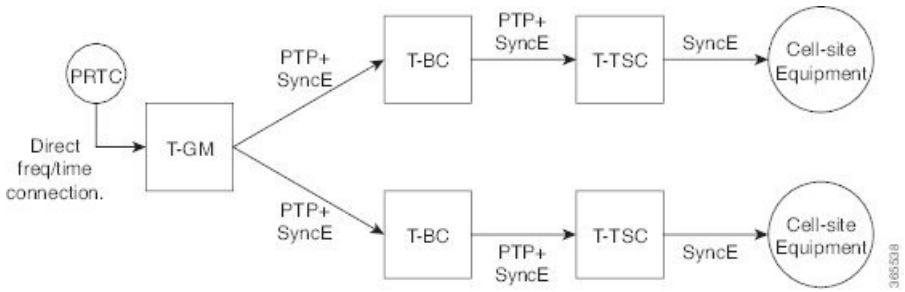
There are three types of clocks allowed in G.8275.1:

- **Telecom Grandmaster (T-GM):** A telecom grandmaster provides timing for other devices in the network, and is usually connected to a primary reference time source, such as a GPS antenna. It does not synchronize its local clock to other network elements.
- **Telecom Time Slave Clock (T-TSC):** A slave clock synchronizes its local clock to another PTP clock, and does not provide synchronization via PTP to any other devices.
- **Telecom Boundary Block (T-BC):** A telecom boundary clock synchronizes its local clock to a T-GM or upstream T-BC, and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster. G.8275.1 introduces the concept of a virtual port on the T-BC. A virtual port is an external frequency, phase and time input interface on a T-BC, which can participate in the source selection. Sumatra has gnss module on the timing card. When gnss is locked we can configure the T-BC to have a virtual port which takes time, phase and frequency from GNSS.

Non-participant devices (devices that merely forward PTP packets) and PTP transparent clocks are not permitted.

PTP is used to provide phase/time-of-day synchronization throughout the network. It is expected (although not required) that SyncE will be used in G.8275.1 deployments to provide better frequency stability for the phase/time-of-day synchronization (so called “hybrid mode”).

Figure 6: A Sample G.8275.1 Topology



PTP Domains

The allowed PTP domain numbers for use within G.8275.1 networks are in the range 24-43, inclusive. The default domain is 24.

PTP Messages and Transport

The following PTP transport parameters are defined in G.8275.1:

- Multicast PTP over Ethernet must be used. Either the forwardable multicast MAC address (01-1B-19-00-00-00) or the non-forwardable multicast MAC address (01-80-C2-00-00-0E) may be used. The MAC address in use is selected on a per-port basis via configuration.
- Either one- or two-step clock mode may be used.
- Two-way PTP operation is required, in order to allow phase/time-of-day delivery. The Delay-request-response mechanism is used for propagation delay measurement; the peer-delay mechanism is not used.
- The minimum packet rate for Announce messages is 8 packets-per-second. For Sync, Follow-Up, Delay-Req and Delay-Resp messages, the minimum rate is 16 packets-per-second.
- Signaling and management messages are not used.

Note G8275.1 is not supported for sub-interface, dot1q and port-channel.

Best Master Clock Algorithm

G.8275.1 specifies an alternate best master clock algorithm (BMCA), used by each device to select which clock (if any) to synchronize to, and to decide the port states of its local ports.

The following new parameters are defined as part of G.8275.1's alternate BMCA:

- "**notSlave**" flag: The notSlave flag is a per-port, configurable Boolean value which indicates whether a port can be placed in slave mode. If this is set on one of a PTP clock's ports, the clock will never synchronize to a clock received on that port.
- **Local priority**: Local priority is a per-port configuration item which is used as a tie-breaker when a PTP clock is selecting between clocks received on different ports, within the scope of a single network element. The network element's local clock also has a configurable local priority.

The G.8275.1 BMCA's clock comparison algorithm is based on the following parameters:

1. **Clock Class**: The profile defines a set of clock-classes for use by compliant clocks. The clock class selected depends on the type of clock, the clock's traceability and holdover status.
2. **Clock Accuracy**: The following clock accuracy values are used by G.8275.1:

   0x21: A T-GM locked to a PRTC uses this value.

   0xFE: A T-GM in holdover, or a T-BC, uses this value.
3. **Offset Scaled Log Variance**: The following offset scaled log variance values are used by G.8275.1:

   0x4E5D: A T-GM locked to a PRTC uses this value.

   0xFFFF: A T-GM in holdover, or a T-BC, uses this value.
4. **Priority 2**: Used as in the original 1588v2 BMCA. Note that priority 1 is not used.
5. **Local Priority**: Used as described above.
6. **Clock Identity**: The clock identity is used as a tie-breaker between different clocks (as in the original 1588v2 BMCA).
7. **Steps Removed**: The steps removed value is used to select between different ports which are receiving the same clock (as in the original 1588v2 BMCA).
8. **Port Identity**: The port identity is used as a tie-breaker between different ports on the same clock.

A G.8275.1-compliant clock ignores the following values in received Announce messages:

- The alternate master, unicast and the profile-specific members of the flag field.
- The control field.
- Priority1

Configuring the G.8275.1 Profile

Configuration On T-GM

PTP-OC-T-GM can take frequency and 1PPS input to synchronize itself with an upstream Grand Master.

The following example shows the configuration on T-GM:

```
ptp clock ordinary domain 24 profile G.8275.1
```

```
 tod R0 ubx
 input 1pps R0       //GNSS is locked and TOD+1PPS are feeding into T-GM G.8275.1.
  clock-port master-port master
  transport ethernet multicast interface Gig 0/0/1
```

Configuration On T-TSC

The following example shows the configuration on T-TSC:

```
ptp clock ordinary domain 24 hybrid g.8275.1
 tod R0 cisco
 output 1pps R0
  clock-port slave-port slave
  transport ethernet multicast interface Gig 0/0/0
```

Configuration On T-BC

The following example shows the configuration on T-BC:

```
ptp clock boundary domain 24 hybrid profile g.8275.1
 tod R0 cisco
 output 1pps R0
  clock-port bc-port-1
  transport ethernet multicast interface Gig 0/0/0
  clock-port bc-port-2
  transport ethernet multicast interface Gig 0/0/1
```

Verifying the Configuration

You can use the following commands to verify a clocking configuration:

- show ptp clock running domain <domain no>
- show ptp clock dataset default
- show ptp clock dataset parent
- show ptp port <name of virtual port>
- show ptp wan stat stream < stream id>
- show network-clock synchronization
- show ptp port dataset port
- show ptp wan tod
- show gnss time
- show gnss status

Examples

```
IR8340#show ptp clock running domain 24
 PTP Ordinary Clock [Domain 24] [Hybrid] [Profile: g8275.1]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
```

```
         FREQ_LOCKED    1              56             146            Hot standby
                                PORT SUMMARY
                                                                        PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
slave mcast       slave        Ethernet     Slave        1            UNKNOWN
IR8340#

IR8340#show ptp clock running
                     PTP Ordinary Clock [Domain 24] [Hybrid] [Profile: g8275.1]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED  1              1176           2946           Hot standby
                                PORT SUMMARY
                                                                PTP Master
Name  Tx Mode      Role         Transport    State        Sessions     Port Addr
slave mcast       slave        Ethernet     Slave        1            UNKNOWN
IR8340#

IR8340#show ptp clock dataset default
CLOCK [Ordinary Clock, domain 24]
  Profile: g8275.1
  Two Step Flag: No
  Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
  Number Of Ports: 1
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Domain Number: 24
  Slave Only: Yes
  Clock Quality:
    Class: 255
    Accuracy: Unknown
    Offset (log variance): 65535
IR8340#

IR8340#show ptp clock dataset parent
CLOCK [Ordinary Clock, domain 24]
  Profile: g8275.1
  Parent Clock Identity: 0x44:B6:BE:FF:FE:42:EF:13
  Parent Port Number: 0
  Parent Stats: No
  Observed Parent Offset (log variance): 0
  Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
    Identity: 0x44:B6:BE:FF:FE:42:EF:13
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 248
      Accuracy: Unknown
      Offset (log variance): 65535
IR8340#

IR8340#show ptp port dataset port
PORT [slave]
  Clock Identity: 0x6C:03:09:FF:FE:18:5F:03
  Clock Profile: g8275.1
  Transport Interface: GigabitEthernet0/0/1
  Port Number: 1
  Port State: Slave
  Min Delay Req Interval (log base 2): -4
  Peer Mean Path Delay: 0
  Announce interval (log base 2): -3
  Announce Receipt Timeout: 3
  Sync Interval (log base 2): -4
```

```
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): -4
  PTP version: 2
  Local Priority: 128
  Not-slave: False
IR8340#

IR8340#show ptp wan stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -5, Acting Interval -5
  Tx packets : 0,  Rx Packets : 96215
  Last Seq Number : 30678,  Error Packets : 0
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 48107, Rx Packets : 0
  Last Seq Number : 0, Error Packets : 0
Delay Response Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : -4, Acting Interval : -4
  Tx packets : 0, Rx Packets : 48107
  Last Seq Number : 48106, Error Packets : 0
Announce Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 1, Acting Interval : 1
  Tx packets : 0, Rx Packets :  1509
  Last Seq Number 1508 Error Packets 0
Signalling Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval : 0
  Tx packets : 12, Rx Packets : 12
  Last Seq Number : 0, Error Packets : 0
Current Data Set                            Units     Within tolerance?
  Offset from master :  +0.000000000        seconds          Yes
  Mean Path Delay    :  +0.000000027        seconds          Yes
  Forward Path Delay :  +0.000000027        seconds          Yes
  Reverse Path Delay :  +0.000000028        seconds          Yes
  Steps Removed 1
IR8340#

IR8340#show ptp wan tod
PTPd ToD information:

Time: 01/05/22 11:35:21

IR8340#

IR8340#show network-clocks synchronization detail
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/0/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-SEC
```

```
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (sf_change)->
 1A (ql_change)-> 1A
Nominated Interfaces
 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*Gi0/0/1              NA          Sync/En      1     QL-PRC    -         -
```

Debugging Commands

Use the following commands to debug your configuration:

- show esmc details
- show platform hardware network-clocks
- show network-clock synchronization detail
- show clocking details

Examples

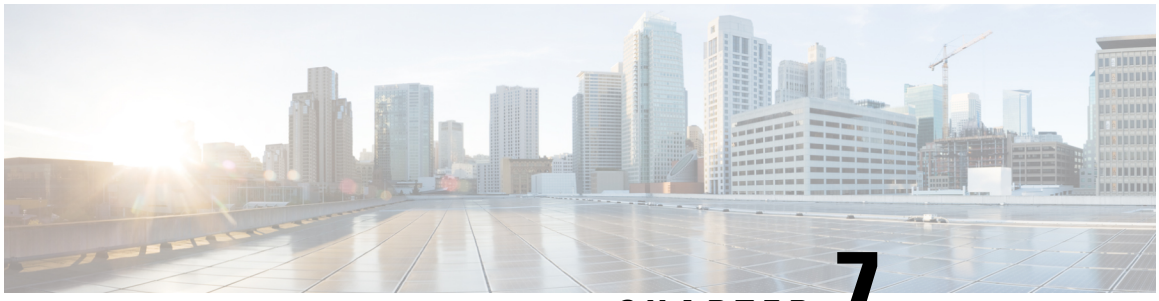
```
IR8340#show esmc detail
Interface: GigabitEthernet0/0/0
  Administrative configurations:
    Mode: Asynchronous
    ESMC TX: Disable
    ESMC RX: Disable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-DNU
    QL Transmit: -
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
    ESMC Tx Timer: Stopped
    ESMC Rx Timer: Stopped
    ESMC Tx interval count: 1
    ESMC INFO pkts in: 777
    ESMC INFO pkts out: 1068
    ESMC EVENT pkts in: 0
    ESMC EVENT pkts out: 2
```

```
IR8340#show esmc detail
IInterface: GigabitEthernet0/0/1
  Administrative configurations:
    Mode: Synchronous
    ESMC TX: Enable
    ESMC RX: Enable
    QL TX: -
    QL RX: -
  Operational status:
    Port status: UP
    QL Receive: QL-PRC
    QL Transmit: QL-DNU
    QL rx overrided: -
    ESMC Information rate: 1 packet/second
    ESMC Expiry: 5 second
    ESMC Tx Timer: Running
```

```
    ESMC Rx Timer: Running
    ESMC Tx interval count: 1
    ESMC INFO pkts in: 1169
    ESMC INFO pkts out: 1486
    ESMC EVENT pkts in: 0
    ESMC EVENT pkts out: 2
IR8340#

IR8340#show network-clocks synchronization detail
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/0/1
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-SEC
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (sf_change)->
 1A (ql_change)-> 1A
Nominated Interfaces
 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*Gi0/0/1              NA          Sync/En      1     QL-PRC    -         -

IR8340#show platform hardware network-clocks
Chassis Manager Netclk Status
----------------
DPLL1 Status:
-------------
Bandwidth: 1.7 Hz
Phase Slope Limit: 7500 ns/s
Current PLL1 Mode: MANUAL NORMAL
Current Input Selected: REF7 (CLK_REC_25M_WAN2)
Current PLL1 Holdover Status: OFF
Current PLL1 Lock Status: ON

IR8340#show platform hardware network-clocks
DPLL2 Status:
-------------
Bandwidth: 0.029 Hz
Phase Slope Limit: 750 ns/s
Current PLL2 Mode: TOP CLIENT (NCO)
Current Input Selected: none
Current PLL2 Holdover Status: OFF
Current PLL2 Lock Status: OFF

IR8340#show platform hardware network-clocks
Current Input Status:
  REF0 (CLK_LOOPBACK1)   : OK
  REF1 (CLK_LOOPBACK2)   : OK
  REF2 ((TDM_SYNC_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
  REF3 (RSV_2_M_PLL)      : FAIL (SCM, CFM, GST, PFM failed)
  REF4 (CLK_PPS_GPS_PLL)  : FAIL (SCM, CFM, GST, PFM failed)
  REF5 (CLK_PPS_MB_PLL)   : FAIL (SCM, CFM, GST, PFM failed)
  REF6 (CLK_REC_25M_WAN1) : FAIL (SCM, CFM, GST, PFM failed)
  REF7 (CLK_REC_25M_WAN2) : OK
```

```
  REF8 (CLK20M_OCXO)      : OK
  REF9 (RSV_1_MB_PLL)     : FAIL (SCM, CFM, GST, PFM failed)
```

```
IR8340#show platform hardware network-clocks

  REF0 Freq Configured   : 25 Mhz
  REF1 Freq Configured   : 25 Mhz
  REF2 Freq Configured   : 8 Khz
  REF3 Freq Configured   : 10 Mhz
  REF4 Freq Configured   : 1 Hz
  REF5 Freq Configured   : 1 Hz
  REF6 Freq Configured   : 25 Mhz
  REF7 Freq Configured   : 25 Mhz
  REF8 Freq Configured   : 20 Mhz
  REF9 Freq Configured   : 25 Mhz
```



CHAPTER 7

Configuring Synchronous Ethernet ESMC and SSM

Synchronous Ethernet is an extension of Ethernet designed to provide the reliability found in traditional SONET/SDH and T1/E1 networks to Ethernet packet networks by incorporating clock synchronization features that support the Synchronization Status Message (SSM) and Ethernet Synchronization Message Channel (ESMC) for synchronous Ethernet clock synchronization.

- Understanding Synchronous Ethernet, on page 77
- Clock Selection Modes, on page 77
- Configuring Synchronous Ethernet ESMC and SSM, on page 78

Understanding Synchronous Ethernet

Synchronous Ethernet (SyncE), described in ITU G.781, provides the required synchronization at the physical level. In SyncE, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH.

Ethernet Synchronization Message Channel (ESMC) incorporates the Synchronization Status Message (SSM) used in Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) networks. While SONET and SDH transmit the SSM in a fixed location within the frame, ESMC transmits the SSM using a protocol: the IEEE 802.3 Organization-Specific Slow Protocol (OSSP) standard.

The ESMC carries a Quality Level (QL) value identifying the clock quality of a given synchronous Ethernet timing source. Clock quality values help a synchronous Ethernet node derive timing from the most reliable source and prevent timing loops.

When configured to use synchronous Ethernet, the router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

The router supports two clock selection modes: QL-enabled and QL-disabled. Each mode uses different criteria to select the best available clock source.

Clock Selection Modes

The IR8340 router supports two clock selection modes:

- QL-Enabled Mode—In QL-enabled mode, the router considers the following parameters when selecting a clock source:
  - Clock quality level (QL)
  - Clock availability
  - Priority
- QL-disabled mode—In QL-disabled mode, the router considers the following parameters when selecting a clock source:
  - Clock availability
  - Priority

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure Synchronous Ethernet ESMC and SSM on the Cisco IR8340 Router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **network-clock synchronization automatic**
4. **network-clock eec** {**1**|**2**}
5. **network-clock ynchronization ssm option** {**1**|**2** {**GEN1** | **GEN2** }}
6. **network-clock input-source** *priority* {**interface***interface_id*|**ptp domain** *domain_num* |{**external** {**R0** | **R1** [{**t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs** } **line-build-out** *length*} | **e1** [**crc4** | **fas**] [**125ohm** | **75ohm**] **linecode** [**hdb3** | **ami**] } | **10m**] }}
7. **network-clock synchronization mode ql-enabled**
8. **network-clock wait-to-restore** *seconds* **global**
9. **esmc process**
10. **network-clock quality-level** {**tx** | **rx**} *value* {**interface** *interface-id* | **controller** [**E1** | BITS] slot/card/port | **external** [2m | 10m] }
11. **interface** *interface-id*
12. **network-clock source quality-level** *value* {**tx**|**rx**}
13. **synchronous mode**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

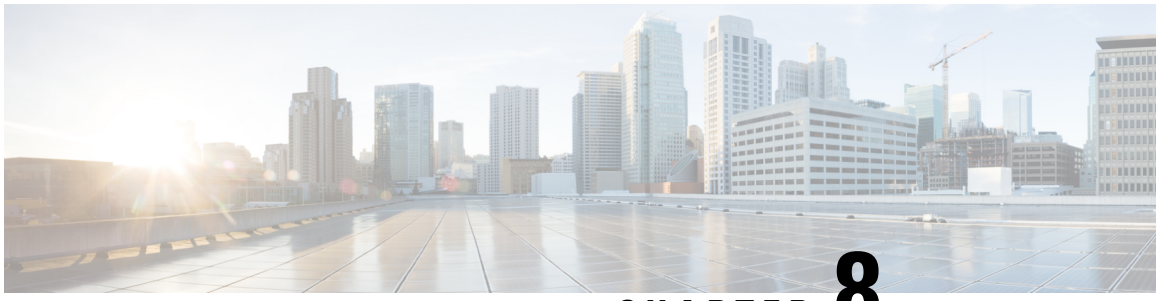
	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 3	**network-clock synchronization automatic** **Example:** `Router(config)# network-clock synchronization automatic`	Enables the network clock selection algorithm. This command disables the Cisco-specific network clock process and turns on the G.781-based automatic clock selection process. **Note** This command must be configured before any input source.
Step 4	**network-clock eec** {**1**|**2**} **Example:** `Router(config)# network-clock eec 1`	Specifies the Ethernet Equipment Clock (EEC) type. Valid values are • 1—ITU-T G.8262 option 1 (2048) • 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)
Step 5	**network-clock ynchronization ssm option** {**1**|**2** {**GEN1** | **GEN2** }} **Example:** `Router(config)# network-clock synchronization ssm option 2 GEN1`	Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command: • Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value. • Option 2 refers to G.781 synchronization option 2, which is designed for the United States. • GEN1 specifies option 2 Generation 1 synchronization. • GEN2 specifies option 2 Generation 2 synchronization.

Step 6	**network-clock input-source** *priority* {**interface***interface_id*|**ptp domain** *domain_num* |{**external** {**R0** | **R1** [{**t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs** } **line-build-out** *length*} | **e1** [**crc4** | **fas**] [**125ohm** | **75ohm**] **linecode** [**hdb3** | **ami**] } | **10m**] }}
	Example:
	`Router(config)# network-clock input-source 1 interface GigabitEthernet 0/0/0`
	`Router(config)# network-clock input-source 1 external R0 1hz`
	`Router(config)# network-clock input-source 2 controller t1 0/2/0`
	`Router(config)# network-clock input-source 3 ptp domain 4`
		Enables you to select an interface as an input clock for the router. You can select WAN interfaces (Gigabit Ethernet 0/0/0, Gigabit Ethernet 0/0/1), T1/E1 controllers, or an external interface. Selection priority for the clock source (1 is the highest priority). When the higher-priority clock source fails, the next-higher-priority clock source is selected.
		Note Before configuring ethernet intreface as clock source, you should configure synchronous mode under interface configuration.
		SyncE is not supported on LAN interfaces.

	Command or Action	Purpose
Step 7	**network-clock synchronization mode ql-enabled** **Example:** `Router(config)# network-clock synchronization mode ql-enabled`	Enables automatic selection of a clock source based on quality level (QL).
Step 8	**network-clock wait-to-restore** *seconds* **global** **Example:** `Router(config)# network-clock wait-to-restore 70 global`	(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process. Valid values are 0 to 86400 seconds. The default value is 300 seconds.
Step 9	**esmc process** **Example:** `Router(config)# esmc process`	Enables the ESMC process globally.

Step 10	**network-clock quality-level** {**tx** | **rx**} *value* {**interface** *interface-id* | **controller** [**E1** | BITS] slot/card/port | **external** [2m | 10m] }
	Example:
	`Router(config)# network-clock quality-level tx QL-SSU-A interface GigabitEthernet 0/0/0`
	`Router(config)# network-clock quality-level rx QL-SSU-A interface GigabitEthernet 0/0/0`
	`Router(config)# network-clock quality-level rx ql-prc external r0 1hz`
		Specifies a quality level for a line or external clock source.
		The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:
		• Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
		• Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
		• Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

Step 11	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies a trunk interface and enters interface configuration mode.
Step 12	**network-clock source quality-level** *value* {**tx**|**rx**} **Example:** `Router(config-if)# network-clock source quality-level QL-PRS tx`	(Optional) Provides the forced QL value to the local clock selection process.
Step 13	**synchronous mode** **Example:** `Router(config-if)# synchronous mode`	Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.
Step 14	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.



CHAPTER 8

Configuring the Global Navigation Satellite System

- Information About GNSS, on page 81
- Guidelines and Limitations, on page 83
- Configuring the Satellite Constellation for GNSS, on page 84
- Verifying Configuration, on page 84

Information About GNSS

Industrial automation and control, utilities, and military networks require large numbers of devices in their networks to have an accurate and synchronized view of time. The IR8340 timing module has a built-in Global Navigation Satellite System (GNSS) receiver that enables the router to determine its own location and get an accurate time from a satellite constellation. GNSS capability simplifies network synchronization planning and provides flexibility and resilience in resolving network synchronization issues in a hierarchical network.

GNSS Hardware

The IR8340 timing module uses a GNSS receiver with precise frequency and phase outputs for the host system. When connected to an external GNSS antenna, the receiver contains all the circuitry necessary to automatically acquire GNSS satellite signals, track up to 32 GNSS satellites, and compute location, speed, heading, and time. It provides an accurate one pulse-per-second (PPS) and stable 10 MHz frequency output. For more information, see GNSS Signaling, on page 82.

Note You are recommended to choose GPS LRM-400 cable for GNSS so that you can check all GNSS alarms. For a list of supported antennas and cables, see the *Cisco Catalyst IR8340 Rugged Series Router Harware Installation Guide*.

The GNSS chip supports the following frequency bands:

- AUTO—GPS + QZSS + GLONASS (default)
- GPS
- GLONASS
- BeiDou

- Galileo

Software

The GNSS feature supports the following functions:

- Time Mode—A special receiver mode where the position of the receiver is known and fixed, and only the time is calculated using all available satellites.
- Survey-in—The procedure that is carried out prior to using Time Mode. It determines a stationary receiver's position by building a weighted mean of all valid 3D position solutions. The receiver computes the average position over an extended time period until a predefined standard deviation has been reached and the minimum observation time has passed by. Afterwards the receiver will be automatically set to fixed mode and the timing features will be activated.
- Survey-in and fixed-position navigation reduce timing jitter, even at low signal levels, and enable synchronization to be maintained with as few as one single satellite in view.
- Time pulse accuracy—Clear sky: 20 ns | Indoor: 500 ns.
- Configures the GNSS receiver.
- After the receiver has gained lock, software performs the following functions once per second:
  - Reads the new time/date.
  - Reads the corresponding PPS timestamp from the hardware.
  - Feeds time/date and PPS timestamp into the Time Services SW Virtual Clock/Servo for GNSS.

    The GNSS SW Virtual Clock time can then be used to drive PTP output.

You can use the **constellation** CLI to choose between these constellations. When a constellation is changed, survey-in process is restarted to lock to a new constellation. For more information, see Configuring the Satellite Constellation for GNSS, on page 84.

Default TOD format is **ubx** and out 1PPS can get when GNSS is locked (for example, PRTC mode).

Frequency 1hz: the following commands are required to enable to get locked:

Router(config)# **network-clock synchronization automatic**

Router(config)# **network-clock synchronization mode QL-enabled**

Router(config)# **network-clock quality-level rx QL-PRC External R0 1hz**

Router(config)# **network-clock input-source 1 External R0 1hz**

Router(config)# **network-clock wait-to-restore 10 global**

GNSS Signaling

There are two stages in the process for the GNSS receiver to acquire satellites and provide timing signals to the host system:

- Self-Survey Mode: On reset, the GNSS receiver comes up in self-survey mode and attempts to lock on to a minimum of four different satellites to obtain a 3-D fix on its current position. It computes nearly 2000 different positions for these satellites, which takes about 35 minutes. Also during this stage, the

GNSS receiver is able to generate accurate timing signals and achieve “Normal (Locked to GPS)” state. Note that the timing signal obtained during self-survey mode can be off by 20 seconds; therefore, Cisco IOS collects PPS only during OD mode.

After the self-survey is complete, the results are saved to the GNSS receiver flash, which speeds up the transition to OD mode the next time the self-survey runs. You can manually restart the self-survey process with the **gnss self-survey restart** Cisco IOS command. After self-survey mode completes again, the results in the GNSS receiver flash are overwritten with the updated results.

- Over-determined (OD) clock mode: The device transitions to OD mode when self-survey mode is completed and the position information is stored in non-volatile memory on the device. In this mode, the GNSS receiver outputs timing information based on satellite positions obtained in self-survey mode.

The GNSS receiver remains in OD mode until there is a reason to leave it, such as:

- Detection of a position relocation of the antenna of more than 100m, which triggers an automatic restart of the self-survey.
- Manual restart of the self-survey using the **gnss self-survey restart** command.

After the GNSS receiver locks on to a satellite system, it sends a 10ms wide PPS pulse and the current time/date according to the satellite system to the Cisco IOS time service.

GNSS LED

The GNSS LED (labeled "GPS" on the cable side and power supply side LEDs) indicates the GNSS status. The following table shows LED colors and their meaning.

Table 9: GNSS LED

Color	Status
Blinking Green	Attempting to acquire satellite fix.
Solid Green	GNSS has valid signal/fix.
Blinking Amber	Antenna fault.
Off	GNSS not configured.

Guidelines and Limitations

- GNSS is available as a timing source for PTP default and power profiles only.
- GNSS is available as a timing source for PTP only when PTP is in GMC-BC mode.
- Syslog messages are sent when the following GNSS events occur:
  - GNSS is in self-survey mode.
  - GNSS reaches OD mode.
  - GNSS firmware upgrade is in progress, complete, or failed.

- If the router is the PTP grandmaster clock and it loses the antenna signal, the clock quality will degrade, resulting in a grandmaster clock switchover.
- The GPS antenna alarm will not trigger an external relay alarm.
- To configure GNSS Auto, you must have a minimum of 8 tracking satellites for each enabled major GNSS (GPS and GLONASS).
- The Antenna Open alarm may be triggered without a hardware issue. In such a scenario, you may configure constellation AUTO to GPS or another constellation available in the location.

Configuring the Satellite Constellation for GNSS

Perform these steps to configure the satellite constellation for GNSS.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 2	**gnss** **Example:** `Router(config)# gnss`	Enable GNSS. When GNSS is enabled, the GNSS process will run to collect GNSS pulse-per-second (PPS) timestamp information. When GNSS is disabled, the chip operates normally, but there is no software process running to collect GNSS timestamp and PPS information.
Step 3	[**no**] **constellation** {**auto** | **galileo** | **gps** | **glonass** | **beidou**} **Example:** `Router(config-gnss)# constellation gps`	(Optional) Configure the GNSS constellation. The default is auto (GPS+GLONASS+QZSS). Only one constellation is active at any given time.
Step 4	**exit** **Example:** `Router(config-gnss)# exit`	Exit GNSS configuration mode.

Verifying Configuration

Command	Purpose
show gnss status	Display the GNSS status. See example output with field descriptions below.

Command	Purpose
show gnss satellite {**all** | *satellite-number*}	Display status of satellites tracked by GNSS. The signal strength is displayed in the form *carrier-to-noise density* (C/N0). The Signal Strength unit is dB-Hz and refers to the ratio of the carrier power and the noise power (dB) *per unit bandwidth* (Hz). Received satellite signal power varies with user antenna gain, satellite elevation angle, and satellite age. Typical C/N0 range is from 35–55 dB-Hz.
show gnss time	Display GNSS time.
show gnss location	Display GNSS location.
show gnss device	Display GNSS device information.
show network-clocks synchronization	Display network clock synchronization status.
show platform hardware network-clocks	Display network clocks for the hardware.

The following example shows output for **show gnss status** after the GNSS receiver has completed self-survey mode and is providing timing information from the satellite system:

```
# show gnss status
  GNSS status:
  GNSS status: Enable
  Clock Progress: Locked (GnssFixOK)
  GNSS Fix Type: time only fix
  Constellation: GLONASS
  Satellite count: 9
  PDOP: 99.989998  TDOP: 0.350000
  HDOP: 99.989998  VDOP: 99.989998
  Major Alarm: False
  Minor Alarm: False
```

Status fields and possible values are:

- GNSS status
  - Enable
  - Disable
- Receiver Status
  - Auto—Auto mode for 2D/3D
  - 1SV—Single satellite
  - 2SV—Horizontal (2D)
  - 3SV—Full position (3D)
  - OD—Over-determined
- Survey progress—This field shows the progress of the survey as a percentage of fixes collected so far. The self-survey is complete when the self-survey progress reaches 100%.

- PDOP—Position dilution of precision
- HDOP—Horizontal dilution of precision
- VDOP—Vertical dilution of precision
- TDOP—Time dilution of precision
- Alarm
  - Antenna open
  - Antenna shorted
  - Not tracking satellites
  - Survey-in progress
  - No stored position
  - Leap second pending

Note If any GPS alarm conditions are present, the switch may not be providing timing information from the satellite system.

The alarm will clear automatically.

The following example shows output for **show gnss satellite**:

```
IR8340#show gnss satellite all
All Satellites Info:

SV ID  Channel  Eph Flag  SV Used  CNR  Azimuth  Elevation  Health  Quality

--------------------------------------------------------------------------------
   19        6         1        -   24      260          1       1        4
   18        6         1        -   31      219          2       1        7
   15        6         1     Used   46      223         42       1        7
   14        6         1     Used   44      340         73       1        7
   13        6         1     Used   36       22         20       1        7
    4        6         1     Used   48      349         27       1        7
    3        6         1     Used   48       53         51       1        7
    2        6         1     Used   45      114         24       1        7
```

The following examples show outputs for **show gnnss time** and **show gnss location**:

```
IR8340# show gnss time
  Current GNSS Time:
  Time: 2021/12/09  07:11:59 UTC

IR8340# show gnss location
  Current GNSS Location:
  LOC: 12:56.187572 N  77:41.742096 E  832.44 m
```

The following example shows output for **show gnnss device**:

```
IR8340#show gnss device
  GNSS device:
```

```
  Model: NEO-M8T-0
  Software version: EXT CORE 3.01 (111141)
  Hardware version: 00080000
  Protocol version: 22.00
  Firmware version: TIM 1.10
  Unique Chip ID: 311652325097
  Major GNSS Satellites supported: GPS;GLO;GAL;BDS
```

The following example shows output for **show network-clocks synchronization**:

```
IR8340#show network-clocks synchronization
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched
Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : External R0 1hz
Hold-off (global) : 300 ms
Wait-to-restore (global) : 10 sec
Tsm Delay : 180 ms
Revertive : No
Nominated Interfaces
 Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
 Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*External R0          1HZ         NA/Dis       1     QL-PRC    NA        NA
IR8340#
```

The following example shows output for **show platform hardware network-clocks**:

```
IR8340#show platform hardware network-clocks
DPLL1 Status:
-------------
Bandwidth: 0.001 Hz
Phase Slope Limit: 885 ns/s
Current PLL1 Mode: MANUAL NORMAL
Current Input Selected: REF4 (CLK_PPS_GPS_PLL)
Current PLL1 Holdover Status: OFF
Current PLL1 Lock Status: ON
DPLL2 Status:
-------------
Bandwidth: 0.001 Hz
Phase Slope Limit: 885 ns/s
Current PLL2 Mode: MANUAL NORMAL
Current Input Selected: REF4 (CLK_PPS_GPS_PLL)
Current PLL2 Holdover Status: OFF
Current PLL2 Lock Status: ON

IR8340#show platform hardware network-clocks
  Current Input Status:
  REF0 (CLK_LOOPBACK1)   : OK
  REF1 (CLK_LOOPBACK2)   : OK
  REF2 ((TDM_SYNC_MB_PLL) : FAIL (SCM, CFM, GST, PFM failed)
  REF3 (RSV_2_M_PLL)      : FAIL (SCM, CFM, GST, PFM failed)
  REF4 (CLK_PPS_GPS_PLL)  : OK
  REF5 (CLK_PPS_MB_PLL)   : FAIL (SCM, CFM, GST, PFM failed)
  REF6 (CLK_REC_25M_WAN1) : FAIL (SCM, CFM, GST, PFM failed)
  REF7 (CLK_REC_25M_WAN2) : FAIL (SCM, CFM, GST, PFM failed)
  REF8 (CLK20M_OCXO)      : OK
```

```
  REF9 (RSV_1_MB_PLL)     : FAIL (SCM, CFM, GST, PFM failed)

DCO Frequency:
  Current_DCO_Freq_Offset: -0.033687

IR8340#
```