

Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers, IOS XR Release 26.1.x, 26.2.x, 26.3.x

First Published: 2025-02-07

Last Modified: 2026-09-11

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)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Using YANG Data Models** 1

CHAPTER 2 **Synchronous Ethernet ESMC and SSM** 3

- Frequency Synchronization Timing Concepts 9
  - Sources 9
  - Selection Points 9
  - Restrictions 10
- Configuring Frequency Synchronization 10
  - Enabling Frequency Synchronization on the Router 10
  - Configuring Frequency Synchronization on an Interface 10
  - Configuring Frequency Synchronization on a Clock Interface 11
  - SyncE Preference for PTP Receiver Interface 12
    - Configure SyncE Preference for PTP Receiver Interface 13
- Verifying the Frequency Synchronization Configuration 14
- Verifying the ESMC Configuration 16
- Verifying Synchronous Ethernet LEDs 17

CHAPTER 3 **Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP)** 19

- Restrictions for Smart SFP 19
- Configuring TPoP and CSoP 21
- VPWS with Smart SFP 23
- Multi Router Automatic Protection Switching 24
- Field-Pluggable Device (FPD) Version Upgrade for Smart SFP 25
- Cisco Smart SFP Destination MAC address 27
  - How destination MAC address helps packet transmission using Cisco Smart SFP 28
  - Guidelines for Cisco Smart SFP Destination MAC address 29

Limitations for Cisco Smart SFP Destination MAC address 30
Configure the destination MAC Addresses on Cisco Smart SFPs 30

CHAPTER 4 TSoP Smart SFP for SDH and SONET Encapsulation 31
Prerequisites for TSoP 32
Restrictions for TSoP 32
Guidelines for TSoP Smart SFP 33
De-jitter Buffer 33
Configuration for TSoP 34

CHAPTER 5 Understanding PTP 41
Why PTP? 43
Routers and Delays 43
Message-Based Synchronization 43
PTP Event Message Sequences 44
Synchronizing with Boundary Clocks 44
Synchronizing the Local Clock 45
PTP Clocks 46
Restrictions for PTP 46
PTP Phase Difference Threshold Between Passive and Secondary Ports 47
Isolate Foreign Masters Causing Packet Timing Signal Fail 49
Advance monitoring 52
Configure advance monitoring 54
PTP Profiles 55
ITU-T Telecom Profiles for PTP 57
G.8265.1 57
G.8275.1 58
G.8275.2 59
PTP Virtual Port 61
Configuring the G.8265.1 Profile 63
Configuring the G.8275.1 Profile 64
Configuring the G.8275.2 Profile 65
Example: Configuring G.8275.2 in Hybrid Mode 67
Example: Configuring G.8275.2 in Non-Hybrid Mode 70

Configuring Virtual Port 72
Configuring APTS 73
Monitor PTP virtual port using PTP timeReceiver ports 74
Alarm conditions 75
Configure threshold to monitor PTP virtual port using PTP timeReceiver ports 76
Configuration example 76
Verify PTP virtual port using PTP timeReceiver ports 77
Restriction to monitor PTP virtual port using PTP timeReceiver ports 79
Slow Tracking 79
PTP Holdover Traceability Suppression 80
IEEE Default Profile 81
Example: Global PTP Configuration 81
Example: PTP Master Configuration 82
Example:PTP Slave Configuration 82
PTP Hybrid Mode 82
Configuring PTP Hybrid Mode 83
Configure PTP for SyncE and PTP Traceability 84
Verifying the PTP Hybrid Mode Configurations 85
Performance Monitoring for PTP Networks 86
Configure PTP Performance Monitoring 88

CHAPTER 6 **External Timing Source** 93
GPS 93
Configuring GPS Settings for the Grandmaster Clock 94
Verifying the GPS Input 94
Building Integrated Timing Supply (BITS) 95
Prerequisite for BITS 95
Configuring BITS-IN 95
Configuring BITS-OUT 96
Verifying BITS-IN Configuration 96
Verifying BITS-OUT Configuration 97
Verify Quality Level Received and Clock Interfaces 97

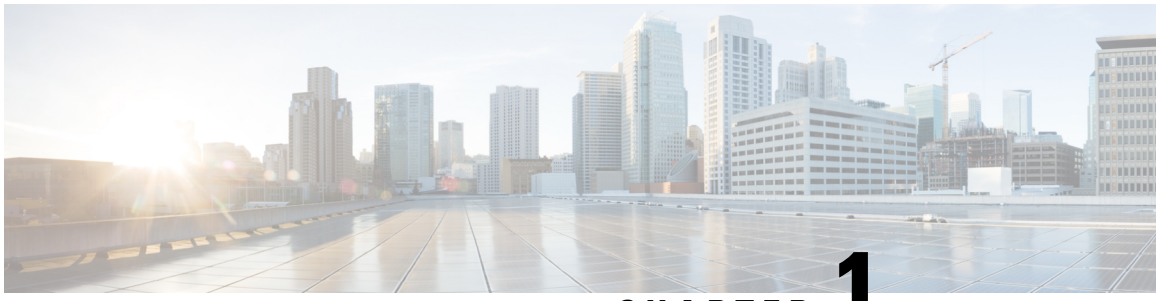
CHAPTER 7 **Implementing NTP** 99

Information About Implementing NTP 99
Best Practices for NTP configuration 100
Configuring NTP 101
PTP-NTP Interworking 101
Enable PTP-NTP Interworking 102
Configuring Poll-Based Associations 102
Configuring Broadcast-Based Associations 103
Configuring NTP Access Groups 103
Configuring NTP Authentication 104
Disabling NTP on an Interface 104
Configuring the System as an Authoritative NTP Server 104
Updating the Hardware Clock 105
Configuring NTP Server Inside VRF Interface 105

CHAPTER 8 **Workflow and Use Case** 107

CHAPTER 9 **Configure the Global Navigation Satellite System** 111
Overview of GNSS 111
Operation of GNSS Module 113
Prerequisites for GNSS 114
Restrictions for GNSS 115
Configure GNSS 115

CHAPTER 10 **Network Synchronization Design Best Practices** 119
Network Synchronization Decision Tree 119
Restrictions for Network Synchronization 120
General Guidelines for Successful Synchronization Deployments 120
Guidelines for Phase Synchronization Deployments 122
PTP over IP Network Design 123
Selecting the Correct Profile For Network Synchronization 123
Reducing Asymmetry 124
Reducing Packet Delay Variation 124
Remediating Transport Asymmetry 125
Synchronizing Across Networks 125



CHAPTER 1

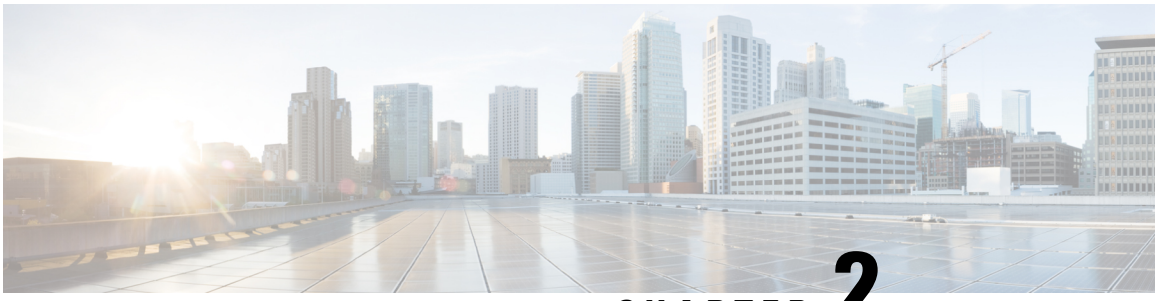
Using YANG Data Models

Cisco IOS XR supports a programmatic way of configuring and collecting operational data of a network device using YANG data models. Although configurations using CLIs are easier and human-readable, automating the configuration using model-driven programmability results in scalability.

The data models are available in the release image, and are also published in the Github repository. Navigate to the release folder of interest to view the list of supported data models and their definitions. Each data model defines a complete and cohesive model, or augments an existing data model with additional XPaths. To view a comprehensive list of the data models supported in a release, navigate to the **Available-Content.md** file in the repository. The unsupported sensor paths are documented as deviations. For example, `openconfig-acl.yang` provides details about the supported sensor paths, whereas `cisco-xr-openconfig-acl-deviations.yang` shows the unsupported sensor paths for `openconfig-acl.yang` model on Cisco IOS XR routers.

You can also view the data model definitions using the YANG Data Models Navigator tool. This GUI-based and easy-to-use tool helps you explore the nuances of the data model and view the dependencies between various containers in the model. You can view the list of models supported across Cisco IOS XR releases and platforms, locate a specific model, view the containers and their respective lists, leaves, and leaf lists presented visually in a tree structure. This visual tree form helps you get insights into nodes that can help you automate your network.

To get started with using the data models, see the Programmability Configuration Guide for Cisco NCS 540 Series Routers.



CHAPTER 2

Synchronous Ethernet ESMC and SSM

Table 1: Feature History Table

Feature Name	Release Information	Description
Synchronous Ethernet ESMC and SSM on N540X-6Z6G-SYS	Release 25.4.1	With Enhanced SyncE (eSyncE) and Extended Ethernet Synchronization Message Channel (eESMC) support, the NCS 540 Series Routers are capable of handling the following SyncE clocks on the network: • Enhanced primary reference clock (ePRC) • Enhanced primary reference timing clock (ePRTC Synchronous Ethernet ESMC and SSM are now supported on: • N540X-6Z6G-SYS For 1G ports, SyncE clock recovery is not supported.

Feature Name	Release Information	Description
Synchronous Ethernet ESMC and SSM on N540-24Q8L2DD-SYS	Release 25.4.1	With Enhanced SyncE (eSyncE) and Extended Ethernet Synchronization Message Channel (eESMC) support, the NCS 540 Series Routers are capable of handling the following SyncE clocks on the network: • Enhanced primary reference clock (ePRC) • Enhanced primary reference timing clock (ePRTC In this release, eSyncE and eESMC are supported on these Cisco NCS 540 router variants: • N540-24Q8L2DD-SYS
Synchronous Ethernet ESMC and SSM on N540-24Q2C2DD-SYS	Release 25.1.1	Synchronous Ethernet ESMC and SSM are now supported on: • N540-24Q2C2DD-SYS For 1G ports, SyncE clock recovery is not supported.

Feature Name	Release Information	Description
Enhanced SyncE and extended ESMC	Release 7.11.1	ITU-T G.8262.1 recommendation defines the requirements for timing devices used in synchronizing network equipment. For example, bandwidth, frequency accuracy, holdover, and noise generation. With Enhanced SyncE (eSyncE) and Extended Ethernet Synchronization Message Channel (eESMC) support, the NCS 540 Series Routers are capable of handling the following SyncE clocks on the network: • Enhanced primary reference clock (ePRC) • Enhanced primary reference timing clock (ePRTC In this release, eSyncE and eESMC are supported on the following Cisco NCS 540 router variants: • N540-6Z14S-SYS-D • N540-6Z18G-SYS-A/D • N540X-4Z14G2Q-A/D • N540X-8Z16G-SYS-A/D • N540X-6Z18G-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540-24Q8L2DD-SYS
Synchronous Ethernet ESMC and SSM on N540X-16Z4G8Q2C-A/D	Release 7.7.1	Synchronous Ethernet ESMC and SSM are now supported on the following Cisco NCS 540 router variant: • N540X-16Z4G8Q2C-A/D For 1G ports, clock recovery is supported only on ports 4 to 19.

Feature Name	Release Information	Description
Synchronous Ethernet ESMC and SSM on N540-6Z14S-SYS-D	Release 7.5.2	SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. Synchronous Ethernet ESMC and SSM are now supported on the following Cisco NCS 540 router variants: • N540-6Z14S-SYS-D

Feature Name	Release Information	Description
Synchronous Ethernet ESMC and SSM, and ITU-T G.8262.1	Release 7.6.1	Ethernet Synchronization Message Channel (ESMC) allows you to transmit Synchronization Status Message (SSM) information by using the ESMC protocol data units (PDUs). In this release, Synchronous Ethernet ESMC and SSM are supported on the following Cisco NCS 540 router variants: • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS • N540-FH-CSR-SYS • N540-FH-AGG-SYS ITU-T G.8262.1 defines the Timing characteristics of a synchronous equipment slave clock. In this release, ITU-T G.8262.1 is supported on the following Cisco NCS 540 router variants: • N540-28Z4C-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540-12Z20G-SYS-A/D • 540X-12Z16G-SYS-A/D • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS • N540-FH-CSR-SYS • N540-FH-AGG-SYS

Feature Name	Release Information	Description
Frequency Synchronization on the N540X-4Z14G2Q-SYS-A/D routers.	Release 7.4.1	Based on the ITU-T G.8262 recommendations, precision frequency is enabled on timing devices to deliver frequency synchronization for bandwidth, frequency accuracy, holdover, and noise generation. This support allows for correct network operations when synchronous equipment is timed from either another synchronous equipment clock or a higher-quality clock.

Note On 1G ports of Cisco N540X-16Z4G8Q2C-A/D, clock recovery is supported only on ports 4 to 19.

Note On Cisco N540X-4Z14G2Q-SYS-A/D routers, the Synchronous Ethernet (SyncE) feature is not supported on ports 14 and 15.

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. It supports the Synchronization Status Message (SSM) and Ethernet Synchronization Message Channel (ESMC) for synchronous Ethernet clock synchronization.

Synchronous Ethernet 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, Ethernet Synchronization Message Channel (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 QL-enabled mode.

- Frequency Synchronization Timing Concepts, on page 9
- Configuring Frequency Synchronization, on page 10
- Verifying the Frequency Synchronization Configuration, on page 14
- Verifying the ESMC Configuration, on page 16
- Verifying Synchronous Ethernet LEDs, on page 17

Frequency Synchronization Timing Concepts

The Cisco IOS XR frequency synchronization infrastructure is used to select between different frequency sources to set the router backplane frequency and time-of-day. There are two important concepts that must be understood with respect to the frequency synchronization implementation.

Sources

A source is a piece of hardware that inputs frequency signals into the system or transmits them out of the system. There are four types of sources:

- Line interfaces: This includes SyncE interfaces.
- Clock interfaces: These are external connectors for connecting other timing signals, such as, GPS, BITS.
- PTP clock: If IEEE 1588 version 2 is configured on the router, a PTP clock may be available to frequency synchronization as a source of the time-of-day and frequency.
- Internal oscillator: This is a free-running internal oscillator chip.

Each timing source has a Quality Level (QL) associated with it which gives the accuracy of the clock. This QL information is transmitted across the network via SSMs over the Ethernet Synchronization Messaging Channel (ESMC) or SSMs contained in the SONET/SDH frames so that devices know the best available source to synchronize to. In order to define a preferred network synchronization flow, and to help prevent timing loops, you can assign priority values to particular timing sources on each router. The combination of QL information and user-assigned priority levels allows each router to choose a timing source to use to clock its SyncE and SONET/SDH interfaces, as described in the ITU standard G.781.

Priority Levels

You can specify the priority of the frequency source on a controller or an interface. Values can range from 1 (highest priority) to 254 (lowest priority). The default value is 100. The priority is used in the clock-selection algorithm to choose between two sources that have the same quality level (QL). Lower priority values are preferred. For example, you can set the priority value for a GNSS clock source by using this command:

```
Router(config-gnss-freqsync)# priority 5
```

The router first considers the QL advertised by different timing sources. If two sources have the same QL, the router selects the source with a lower priority value for network synchronization.

Selection Points

A selection point is any point where a choice is made between several frequency signals, and possibly one or more of them are selected. Selection points form a graph representing the flow of timing signals between the different cards in a router running Cisco IOS XR software. For example, one or multiple selection points select between the different Synchronous Ethernet inputs available on a single line card, and the result of these selection points is forwarded to a selection point on the RSP to select between the selected source from each card.

The input signals to the selection points can be:

- Received directly from a source.
- The output from another selection point on the same card.

- The output from a selection point on a different card.

The output of a selection point can be used in a number of ways:

- Used to drive the signals sent out of a set of sources.
- As input into another selection point on the card.
- As input into a selection point on another card.

Use the show frequency synchronization selection command to see a detailed view of the different selection points within the system.

Restrictions

- SyncE isn't supported on Gigabit Ethernet 0/0/0/20 to 0/0/0/27 ports of N540X-16Z4G8Q2C-A and N540X-16Z4G8Q2C-D variants.
- System limitation: On Cisco N540X-16Z4G8Q2C-D routers, use dedicated copper ports 0 through 3 for copper connectivity. Do not install a copper SFP in an optical port, as this can cause SyncE problems.
- For copper ports, configure one endpoint as a SyncE master and the peer as a SyncE client. SyncE may not work, or the port might not come up, if both endpoints are configured with the same role.



Note The following restrictions are applicable only for N540-24Z8Q2C-SYS, N540X-ACC-SYS, N540-ACC-SYS, and N540-28Z4C-SYS variants.

- SyncE isn't supported on Gigabit Ethernet 0/0/0/24 to 0/0/0/31 ports.

Configuring Frequency Synchronization

Enabling Frequency Synchronization on the Router

This task describes the router-level configuration required to enable frequency synchronization.

```
RP/0/RP0/CPU0:Router# configure
RP/0/RP0/CPU0:Router(config)# frequency synchronization
RP/0/RP0/CPU0:Router(config-freqsync)# clock-interface timing-mode system
RP/0/RP0/CPU0:Router(config-freqsync)# quality itu-t option 1 generation 1
RP/0/RP0/CPU0:Router(config-freqsync)# log selection changes
RP/0/RP0/CPU0:Router(config-freqsync)# commit
```

Configuring Frequency Synchronization on an Interface

By default, there is no frequency synchronization on line interfaces. Use this task to configure an interface to participate in frequency synchronization.

Before You Begin

You must enable frequency synchronization globally on the router.

```
RP/0/RP0/CPU0:R1#config terminal
RP/0/RP0/CPU0:R1(config)#interface TenGigabitEthernet 0/0/0/0
RP/0/RP0/CPU0:R1(config-if)#frequency synchronization
RP/0/RP0/CPU0:R1(config-if-freqsync)#selection input
RP/0/RP0/CPU0:R1(config-if-freqsync)#wait-to-restore 10
RP/0/RP0/CPU0:R1(config-if-freqsync)#priority 5
RP/0/RP0/CPU0:R1(config-if-freqsync)#quality transmit exact itu-t option 1 PRC
RP/0/RP0/CPU0:R1(config-if-freqsync)#quality receive exact itu-t option 1 PRC
RP/0/RP0/CPU0:R1(config-if-freqsync)#commit
or
RP/0/RP0/CPU0:router(config-freqsync)# commit
```

Configuring Frequency Synchronization on a Clock Interface

To enable a clock interface to be used as frequency input or output, you must configure the port parameters and frequency synchronization, as described in this task.

```
RP/0/RP0/CPU0:R1#configure
RP/0/RP0/CPU0:R1(config)# clock-interface sync 2 location 0/RP0/CPU0
RP/0/RP0/CPU0:R1(config-clock-if)# port-parameters
RP/0/RP0/CPU0:R1(config-clk-parms)# gps-input tod-format cisco pps-input tt1
RP/0/RP0/CPU0:R1(config-clk-parms)# exit
RP/0/RP0/CPU0:R1(config-clock-if)# frequency synchronization
RP/0/RP0/CPU0:R1(config-clk-freqsync)# selection input
RP/0/RP0/CPU0:R1(config-clk-freqsync)# wait-to-restore 1
RP/0/RP0/CPU0:R1(config-clk-freqsync)# quality receive exact itu-t option 1 PRC
```

SyncE Preference for PTP Receiver Interface

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
SyncE Preference for PTP Receiver Interface	Release 24.4.1	You can now mitigate synchronization issues when SyncE and PTP sources come from different, non-traceable origins. This feature ensures that SyncE selection among sources with equal Quality Levels (QL) and user priority prefers the interface on which the PTP receiver is selected. If the PTP source fails or its quality degrades, causing the system to switch to another PTP source, SyncE switches to the new PTP source, provided the new interface has the same SyncE QL and priority as the previously selected interface. This feature introduces these changes: **CLI:** • **synchronous-ethernet prefer-interface ptp-receiver**

In network deployments, users often utilize multiple clock sources to ensure redundancy, achieving synchronization through T-GM clocks powered by Primary Reference Time Clocks (PRTC) sources like GNSS. These clocks deliver frequency and time synchronization to other network nodes using both SyncE and PTP in hybrid mode. However, issues can arise when SyncE and PTP sources come from different, non-traceable origins, leading to synchronization failures in PTP.

To mitigate this issue, you can configure the **synchronous-ethernet prefer-interface ptp-receiver** command. When this command is configured, the SyncE selection among sources with equal Quality Levels (QL) and user priority prefers the interface on which the PTP receiver is selected.

- If either the QL or the user priority of the sources differ, then the syncE selection would follow the G.781 requirements.
- If the PTP source goes down or if the PTP quality degrades causing the system to switch to another PTP source, then with the above command, the SyncE selection also switches to the new PTP source, provided that the new interface has the same SyncE QL and priority as the previously selected interface.

Benefits of SyncE Preference for PTP Receiver Interface

- Enhanced Synchronization - Ensures that SyncE and PTP sources are traceable to the same clock source, preventing synchronization issues.
- Improved Reliability - Reduces the risk of PTP synchronization failures caused by rapid clock drifts.

- Simplified Configuration - Automates the selection process of SyncE sources to align with the PTP receiver, simplifying network management.

Restrictions for SyncE Preference for PTP Receiver Interface

SyncE auto-selection to the PTP-receiver interface happens only if the interface is part of the **show frequency synchronization selection** list of SyncE interfaces. If more than two SyncE interfaces are configured, it is possible that the PTP-receiver interface isn't part of the selection list, and auto-switching doesn't occur.

Configure SyncE Preference for PTP Receiver Interface

Enable SyncE preference for PTP Receiver Interface.

Procedure

Step 1 Enter the frequency synchronization mode.

Example:

```
Router#configure
Router(config)#frequency synchronization
```

Step 2 Configure SyncE to prefer the PTP receiver interface.

Example:

```
Router(config-freqsync)#synchronous-ethernet prefer-interface ptp-receiver
Router(config-freqsync)#commit
```

Step 3 Verify that SyncE is configured to prefer the PTP receiver interface.

Example:

```
Router#show ptp interfaces brief
Intf              Port         Port                  Line
Name              Number       State        Encap    State         Mechanism
-------------------------------------------------------------------------------
Te0/0/0/18        2            Passive      Ethernet up            -
Te0/0/0/19        1            Slave        Ethernet up            -
```

The **show ptp interfaces breif** command gives information about the ptp interfaces and then you can verify that the PTP receiver (Slave) interface is selected for frequency synchronization in **show frequency synchronization interfaces brief** command output.

```
Router#show frequency synchronization interfaces brief

Flags:  > - Up               D - Down             S - Assigned for selection
        d - SSM Disabled     x - Peer timed out   i - Init state
        s - Output squelched
Fl   Interface                QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
>S   TenGigE0/0/0/18          PRC   PRC   100 DNU   TenGigE0/0/0/19
>S   TenGigE0/0/0/19          PRC   PRC   100 PRC   TenGigE0/0/0/19
```

Verifying the Frequency Synchronization Configuration

After performing the frequency synchronization configuration tasks, use this task to check for configuration errors and verify the configuration.

1. **show frequency synchronization selection**

```
RP/0/RP0/CPU0:R5# show frequency synchronization selection
Fri Apr 24 12:49:32.833 UTC
Node 0/RP1/CPU0:
==============
Selection point: T0-SEL-B (3 inputs, 1 selected)
  Last programmed 3d04h ago, and selection made 3d04h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : CHASSIS-TOD-SEL
    Chassis scoped: LC_TX_SELECT
    Router scoped : None
  Uses frequency selection
  Used for local line interface output
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  4  HundredGigE0/7/0/0        0/RP1/CPU0 ETH_RXMUX 4      PRC   10  Locked
     PTP [0/RP1/CPU0]          n/a                         PRC  254  Available
     Internal0 [0/RP1/CPU0]    n/a                         SEC  255  Available

Selection point: 1588-SEL (2 inputs, 1 selected)
  Last programmed 3d04h ago, and selection made 3d04h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  4  HundredGigE0/7/0/0        0/RP1/CPU0 ETH_RXMUX 4      PRC   10  Locked
     Internal0 [0/RP1/CPU0]    n/a                         SEC  255  Available

Selection point: CHASSIS-TOD-SEL (2 inputs, 1 selected)
  Last programmed 3d04h ago, and selection made 3d04h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses time-of-day selection
  S  Input                     Last Selection Point      Pri  Time  Status
  == ========================  ========================  ===  ====  ===========
  1  PTP [0/RP1/CPU0]          n/a                       100  Yes   Available
     HundredGigE0/7/0/0        0/RP1/CPU0 T0-SEL-B 4     100  No    Available

Selection point: ETH_RXMUX (1 inputs, 1 selected)
  Last programmed 3d04h ago, and selection made 3d04h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0-SEL-B 1588-SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
```

```
  4  HundredGigE0/7/0/0        n/a                          PRC   10  Available
```

2. **show frequency synchronization configuration-errors**

```
RP/0/RP0/CPU0:router# show frequency synchronization configuration-errors
Node 0/2/CPU0:
==============
  interface GigabitEthernet0/2/0/0 frequency synchronization
    * Frequency synchronization is enabled on this interface, but isn't enabled globally.
interface GigabitEthernet0/2/0/0 frequency synchronization quality transmit exact itu-t
 option 2 generation 1 PRS
    * The QL that is configured is from a different QL option set than is configured
globally.
```

Displays any errors that are caused by inconsistencies between shared-plane (global) and local-plane (interface) configurations. There are two possible errors that can be displayed:

- Frequency Synchronization is configured on an interface (line interface or clock-interface), but is not configured globally.
- The QL option configured on some interface does not match the global QL option. Under an interface (line interface or clock interface), the QL option is specified using the quality transmit and quality receive commands. The value specified must match the value configured in the global quality itu-t option command, or match the default (option 1) if the global quality itu-t option command is not configured.

Once all the errors have been resolved, meaning there is no output from the command, continue to the next step.

3. **show frequency synchronization interfaces brief**

```
RP/0/RP0/CPU0:R5# show frequency synchronization interfaces brief
Thu Feb 1 06:30:02.945 UTC
Flags: > - Up
        d - SSM Disabled
        s - Output squelched
Fl   Interface
D - Down              S - Assigned for selection
 x - Peer timed out    i - Init state
Last Selection Point
Pri Time
Status
                              QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
>S   TenGigE0/0/0/0           PRC   PRC     1 DNU   TenGigE0/0/0/0
>x   TenGigE0/0/0/1           Fail  n/a   100 PRC   TenGigE0/0/0/0
>x   TwentyFiveGigE0/0/0/30   Fail  n/a   100 PRC   TenGigE0/0/0/0

RP/0/RP0/CPU0:R5#
```

Verifies the configuration. Note the following points:

- All line interface that have frequency synchronization configured are displayed.
- All clock interfaces and internal oscillators are displayed.
- Sources that have been nominated as inputs (in other words, have selection input configured) have ‘S’ in the Flags column; sources that have not been nominated as inputs do not have ‘S’ displayed.

Note Internal oscillators are always eligible as inputs.

- '>' or 'D' is displayed in the flags field as appropriate.

If any of these items are not true, continue to the next step.

4. **show processes fsyncmgr location node-id**

   This command verifies that the fsyncmgr process is running on the appropriate nodes.

```
RP/0/RP0/CPU0:R5# show processes fsyncmgr location 0/0/cPU0
Thu Feb 1 06:26:32.979 UTC
Job Id: 181
PID: HYPERLINK "tel:3411"3411
Process name: fsyncmgr
Executable path:
/opt/cisco/XR/packages/ncs540-iosxr-fwding-1.0.0.0-r63226I/all/bin/fsyncmgr Instance #:
 1
Version ID: 00.00.0000
Respawn: ON
Respawn count: 1
Last started: Tue Jan 23 04:26:57 HYPERLINK "tel:2018"2018
Process state: Run
Package state: Normal
core: MAINMEM
Max. core: 0
Level: 100
Placement: None
startup_path:
/opt/cisco/XR/packages/ncs540-iosxr-fwding-1.0.0.0-r63226I/all/startup/fsyncmgr.startup
 Ready: 2.063s
Process cpu time: 168.480 user, 129.980 kernel, 298.460 total
JID TID Stack pri state NAME rt_pri
181 HYPERLINK "tel:3411"3411 0K 20 Sleeping fsyncmgr 0
181 HYPERLINK "tel:3572"3572 0K 20 Sleeping lwm_debug_threa 0
181 HYPERLINK "tel:3573"3573 0K 20 Sleeping fsyncmgr 0
181 HYPERLINK "tel:3574"3574 0K 20 Sleeping lwm_service_thr 0
181 HYPERLINK "tel:3575"3575 0K 20 Sleeping qsm_service_thr 0
181 HYPERLINK "tel:3622"3622 0K 20 Sleeping fsyncmgr 0
181 HYPERLINK "tel:3781"3781 0K 20 Sleeping fsyncmgr 0
181 HYPERLINK "tel:3789"3789 0K 20 Sleeping fsyncmgr 0
```

Verifying the ESMC Configuration

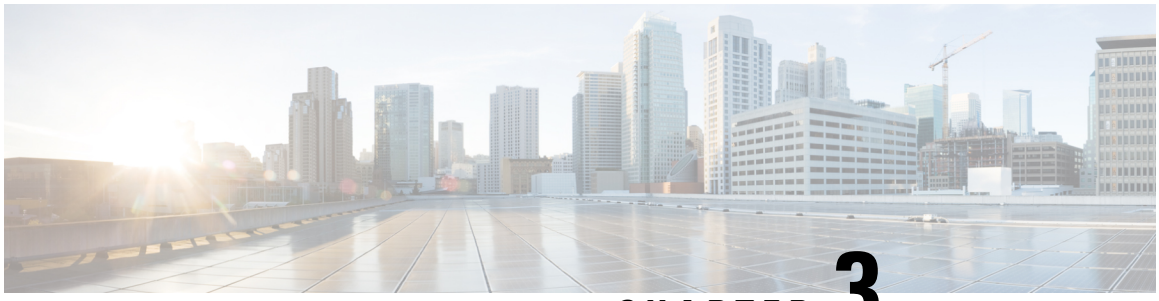
show frequency synchronization interfaces

```
RP/0/RP0/CPU0:R5# show frequency synchronization interfaces
                    Thu Feb 1 06:33:26.575 UTC
                    Interface TenGigE0/0/0/0 (up)
                    Assigned as input for selection
                    Wait-to-restore time 0 minutes
                    SSM Enabled
Peer Up for 2d01h, last SSM received 0.320s ago
Peer has come up 1 times and timed out 0 times
ESMC SSMs Total Information Event DNU/DUS
Sent: HYPERLINK "tel:178479"178479 HYPERLINK "tel:178477"178477 2 HYPERLINK "tel:178463"178463
```

```
                    Received: HYPERLINK "tel:178499"178499 HYPERLINK "tel:178499"178499 0
0
                    Input:
                    Up
                    Last received QL: Opt-I/PRC
                    Effective QL: Opt-I/PRC, Priority: 1, Time-of-day Priority 100
                    Supports frequency
                    Output:
                    Selected source: TenGigE0/0/0/0
                    Selected source QL: Opt-I/PRC
                    Effective QL: DNU
                    Next selection points: ETH_RXMUX
                    Interface TenGigE0/0/0/1 (up)
                    Wait-to-restore time 5 minutes
                    SSM Enabled
                    Peer Timed Out for 2d01h, last SSM received never
                    Peer has come up 0 times and timed out 1 times
                    ESMC SSMs Total Information Event DNU/DUS
                    Sent: HYPERLINK "tel:178479"178479 HYPERLINK "tel:178477"178477 2 0
                    Received: 0 0 0 0
                    Input:
                    Down - not assigned for selection
                    Supports frequency
                    Output:
                    Selected source: TenGigE0/0/0/0
                    Selected source QL: Opt-I/PRC
                    Effective QL: Opt-I/PRC
                    Next selection points: ETH_RXMUX
                    Interface TwentyFiveGigE0/0/0/30 (up)
                    Wait-to-restore time 5 minutes
                    SSM Enabled
                    Peer Timed Out for 01:50:24, last SSM received 01:50:30 ago
                    Peer has come up 1 times and timed out 1 times
ESMC SSMs Total Information Event DNU/DUS
Sent: HYPERLINK "tel:75086"75086 HYPERLINK "tel:75085"75085 1 0
Received: HYPERLINK "tel:68457"68457 HYPERLINK "tel:68455"68455 2 HYPERLINK "tel:68443"68443
Input:
Down - not assigned for selection
Supports frequency
Output:
Selected source: TenGigE0/0/0/0
Selected source QL: Opt-I/PRC
Effective QL: Opt-I/PRC
Next selection points: ETH_RXMUX
```

Verifying Synchronous Ethernet LEDs

```
RP/0/RP0/CPU0:ios# show led
Mon Nov 2 09:29:34.637 UTC
================================================================================
Location LED Name Mode Color
================================================================================
0/FT0
Status OPERATIONAL GREEN
0/RP0/CPU0
Alarm OPERATIONAL AMBER
Status OPERATIONAL GREEN
Sync OPERATIONAL AMBER
```



CHAPTER 3

Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP)

Transparent PDH over Packet (TPoP) Smart SFP converts E1 traffic to a packet stream using TDM over packet pseudo-wire technology. TPoP Smart SFP can be used on selected SFP slots in a router to transport PDH traffic across a packet network. TPoP Smart SFP is a plug-and-play device which can be used without any provisioning and simplifies configuration and service turn-up of E1 connections across a packet network. The integration of TPoP into an SFP greatly reduces system and network complexity, offers lower carbon footprint, and results in savings.

Channelized SDH over Packet (CSoP) Smart SFP converts a fully channelized SDH signal to a packet stream using TDM over packet pseudo-wire technology. CSoP Smart SFP can replace an existing SFP in a router or a switch and transport E1 traffic across a packet network. CSoP Smart SFP aggregates single E1 and enables each E1 channel to be processed individually to provide a high-density gateway between an SDH network and a TDM over packet ethernet or IP or MPLS network.

Following are the supported E1 and STM1 optical SFPs, for more information on the supported router variants based on the release versions, see Cisco Optics-to-Device Compatibility Matrix.

- Framed STM1-ch E1 type: SFP-CH-OC3STM1-I
- Framed PDH E1 type: SFP-E1F-SATOP-I
- Clear channel STM1 type: SFP-TS-OC3STM1-I

- Restrictions for Smart SFP, on page 19
- Configuring TPoP and CSoP, on page 21
- VPWS with Smart SFP, on page 23
- Multi Router Automatic Protection Switching, on page 24
- Field-Pluggable Device (FPD) Version Upgrade for Smart SFP, on page 25
- Cisco Smart SFP Destination MAC address, on page 27

Restrictions for Smart SFP

Warning If MR-APS is configured on the SFP, then remove MR-APS configuration before you remove the SFP from the port.

- CEM interface configuration isn't supported.
- The following default attributes are available only under CEM interface configuration. But you can't configure these attributes, as the configuration CLIs aren't supported.
  - dummy mode
  - dummy pattern
  - idle pattern
- E1 emulation is supported only on Ethernet pseudowire (VPWS).
- CSoP doesn't support E1-AIS alarm.
- No support to Single Router–Automatic Protection Switching (SR-APS)
- CLI configuration for the E1 controller on a VLAN needs to be mapped to an Ethernet sub-interface (by configuring same VLAN dot1q under the sub-interface). Any xconnect, also must be configured with this ethernet sub-interface.
- Multi Router-Automatic Protection Switching (MR-APS) is supported only by using the VLAN PW.
- Ensure that you have more than one MPLS paths, in core to convergence during core failure scenario.
- Only 8 smart SFPs are supported per router.
- ACR clocking is not supported in TPoP and CSoP unframed SFPs. Only framed to framed connection is supported, so not supported on framed to unframed connections.
- STM1 CSoP:
  - E1 Level shutdown is not supported.
  - Controller shutdown won't inject AIS but injects only LOS towards CE.
  - Bit error rate test (BERT) can be run only on one E1 channelized controller.
- CSoP and TPoP:
  - 25G ports are not supported.
  - Bit error rate is not supported.
- SF or SD threshold is not supported.
- Only 16-byte J0 is supported.
- BERT is not supported in unframed SFP.
- Loopback is supported only on, one of the 63 channels of CSoP SFP.
- Configuration with same ECID for CSoP E1s is not supported. ECID must be unique for each E1 under CSoP.
- The **show alarm conditions** command is not supported in Release 7.5.1.
- High convergence of 100ms is observed for MR-APS for LOS based switchover (for CSoP E1s).

- With smart SFP, high convergence of 4-6 minutes is observed in MR-APS for router reload based switchover.
- CSoP loopback on framed STM1-ch E1 doesn't work over **reload warm** command with smart SFP. Applicable only in Release 7.5.1.
- FPD upgrade for smart SFP is supported only from Release 7.8.1.
- LCV counter updates are not supported for smart SFP.
- In Cisco IOS XR software version 25.2.1, the N540X-16Z4G8Q2C-A and N540X-16Z4G8Q2C-D does not suppot Smart SFPs.

Configuring TPoP and CSoP

Consider a deployment scenario with the TDM circuits from a base transceiver station is connected to an access router and must be transported to the base station controller through an aggregation router over an MPLS network through pseudowire.

During aggregation from transceiver to controller, the TDM circuits protect the data by using smart SFPs. For the E1 lines coming from transceiver, you must use TPoP SFPs and for the STM-1 lines coming from transceiver or controller, you must use CSoP SFPs.

You can monitor the alarms and performances on TPoP and CSoP smart SFPs.

Table 3: Support on E1 Transmission

Feature	E1 Framed
SATOP	Supported
Clock configuration	ACR, DCR, internal, Line
BERT - System/Line	Supported (Inverted-PRBS15)
PM -E1	SELS, LES, UAS, LCV, PCV Far End counters are NOT SUPPORTED
Alarms	LOS, AIS, LOF, RDI
Loopback - (local / line)	Supported
CEM counters	Supported

Table 4: Support on OC3-STM1 Transmission

Feature	OC3-STM1
E1 SATOP	STM-1 Channelized E1
Clock Configuration on Channelised-E1	ACR, DCR, internal, Line
E1 Channel BERT - System/Line channel prbs	Supported (Inverted-PRBS15)

Feature	OC3-STM1
PM-STM1 RS/MS	ES, SES, UAS Far End counters are NOT SUPPORTED
Threshold and its alerts	Supported
Alarms STM1	LOS, LOF, RS-TIM, MS-AIS, MS-RAI

Also consider a case, with Automatic Protection Switching (APS) protection being enabled on the controller, then the protect link coming from a single node or from multiple nodes with standby pseudowire is supported in the MPLS core.

Configuring Controller for PDH E1

To configure PDH E1 on a controller, ensure the Gigabit Ethernet port is up and enter the following commands:

```
enable
configure terminal
    controller e1  0/0/0/7
    vlan 100 ecid 1
end
```

You must mention a unique VLAN ID which is specific to that port and ecid number to identify E1.

Verifying Controller for PDH E1

Use the **show controller e1 x/y/z** command to verify the controller configuration on E1 for TPoP smart SFP.

```
Router# show controller e1 0/0/0/7
Controller State: Up
Transport Admin State: In Service
Framing: Unframed
Linecoding: High Density Bipolar Order 3
Loopback: None
Clock: Adaptive Clock Recovery (ACR)
Clock State: Locked
VLAN ID: 100
ecid:1
```

Configuring Controller for STM1

To configure STM1 on a controller, ensure the Gigabit Ethernet port is up and enter the following commands:

```
controller STM1 0/0/0/18
 aug-mapping au4 au-4 1
  mode tug3
   tug-3 1
    mode tug2
     tug-2 1 payload vc12
      vc12 1 mapping e1

/*Configure STM1-ch E1 */
```

Verifying Controller for STM1

Use the **show controller stm1 x/y/z** command to verify the controller configuration on STM1 for CSoP smart SFP.

```
Router# show controller STM1 0/0/0/18
Port STM 10/0/0/18

Status:
Primary State: Up
Configured Sec admin State: Normal
Inherited Sec admin State: Normal
Derived State: In Service
performance_monitoring_enabled
Loopback: None
```

Configuring Controller for STM1-ch E1

To configure each E1 on STM1 port, enter the following commands:

```
Config terminal
    controller E1 0/0/0/18/1/1/1/1
    vlan 200 ecid 1
```

You can configure the same VLAN ID for all the E1 under the same STM1 port or a different VLAN ID for each E1 under that STM1 port.

Verifying Controller for STM1-ch E1

Use the **show controller e1 x/y/z** command to verify the controller configuration on STM1.

```
Router# show controller e1 0/0/0/18/1/1/1/1
Controller State: Up
Transport Admin State: In Service
Framing: Unframed
Linecoding: None
Loopback: None
Clock: Internal

VLAN ID: 200
ecid:1
```

VPWS with Smart SFP

The TDM circuits flows through the VPWS with smart SFP packetizing the incoming TDM frames. Packetizing happens with the following process:

- All frames from the TDM lines are channelized until E1 and then packetized.
- The packetization is done by adding:
  - RTP header – For DCR clocking support
  - VLAN header – For uniquely identifying the E1 channel
  - ENET header – The Ethernet DMAC and SMAC
  - CW – control word for communicating the sequence number, faults in the access side
  - Payload – the incoming TDM frames are chopped into 193Bytes frames and added into the payload.
  - The packets mentioned previously sent to the NPU.
- The E1 channel is mapped into a sub-interface (with specific VLAN).

- The packets received into the NPU with that specific VLAN number go through the VPWS logic and gets pseudowired (xconnected) with the configuration in a specific sub-interface.
- QOS configured under the sub-interface gets applied to this PW.

Multi Router Automatic Protection Switching

The Multi Router Automatic Protection Switching (MR-APS) integration with hot standby pseudowire (HSPW) feature is a protection mechanism for SDH to switch to another circuit during failure.

Consider a deployment scenario with the MR-APS circuits from a base transceiver station is connected to access router and must be transported to the base station controller through an aggregation router over an MPLS network through pseudowire. When the pseudowire reaches the router with MR-APS, data is depacketized on the smart SFP and the raw TDM frames are sent towards the base station controller. The controller is connected to routers via two links, one as working link from router-A and other as protect link towards the router-B.

Configuring Xconnect on Sub-Interface

To configure E1 port based on the VLAN ID, create sub-interface Gigabit Ethernet port.

Note The **propagate-tdm-alarm** command enables the forwarding of port level alarms to Gigabit Ethernet port in which Smart SFP resides.

```
Config terminal
controller STM1 0/0/0/0
   propagate-tdm-alarm
!
interface GigabitEthernet0/0/0/18.200 l2transport
 encapsulation dot1q 200
!


interface GigabitEthernet0/0/0/7.100 l2transport
 encapsulation dot1q 100

l2vpn
 pw-class tdm_pw
  encapsulation mpls
  !
 !
 xconnect group tdm_csop
  p2p pw200
   interface GigabitEthernet0/0/0/18.200
   neighbor ipv4 2.2.2.2 pw-id 200
    pw-class tdm_pw
   !
  !
 !
 xconnect group tdm_tpop
  p2p pw100
   interface GigabitEthernet0/0/0/7.100
   neighbor ipv4 2.2.2.2 pw-id 100
    pw-class tdm_pw
   !
```

```
  !
 !
!
```

For more information on the standby pseudowire, see *Configure Pseudowire Redundancy* in chapter *Configure Point-to-Point Layer 2 Services* of the *L2VPN and Ethernet Services Configuration Guide*.

Field-Pluggable Device (FPD) Version Upgrade for Smart SFP

Note The following steps are applicable to Channelized SDH over Packet (CSoP) STM-1 SFPs and E1 Transparent PDH over Packet (TPoP) SFPs only.

Before you begin

To upgrade the FPD version on the Cisco NCS 540 Series Routers, perform the following steps:

1. To check the existing version of the FPD, run the **show hw-module fpd** command.

   Sample output for checking the current FPD version:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                          FPD Versions
                                                                          ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd

--------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          NEED UPGD   7.01      7.01

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT    13.01     13.01

0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00

0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

2. To upgrade the hardware, run the **upgrade hw-module location 0/RP0 fpd <> force** command.

   To check the status of upgrade, run the **show hw-module fpd** command until the upgrade progress reaches 100 percent. The following are sample outputs for checking the status of the upgrade:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                          FPD Versions
```

```
                                                                                 ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd

-------------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          30% UPGD    13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT     13.01     13.01

0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT     13.00     13.00

0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                                  FPD Versions
                                                                                 ==============
Location   Card type            HWver FPD device       ATR Status    Running   Programd

-------------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          75% UPGD    13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT     13.01     13.01

0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT     13.00     13.00

0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

Procedure

Step 1 After the Smart SFP FPD upgrade completes 100 percent or after receiving the upgrade success message, wait for 15 seconds.

Step 2 Perform an online insertion and removal (OIR) of the Smart SFP:

a) Remove the Smart SFP and wait for two minutes for the clean-up to complete.

b) Insert the Smart SFP on the same port.

This step recreates the controller with all its configurations.

Step 3 To verify the Smart SFP version, run the **show hw-module fpd** command.

Sample command output for checking the FPD version of the Smart SFP:

```
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                                FPD Versions
                                                                                ============
Location   Card type             HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/RP0      N540-ACC-SYS          0.5   MB-MIFPGA            CURRENT     0.05      0.05
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_12          CURRENT    13.01     13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_E1F_4           CURRENT    13.01     13.01
0/RP0      N540-ACC-SYS          1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00
0/RP0      N540-ACC-SYS          0.5   Bootloader           NEED UPGD   1.14      1.14
0/RP0      N540-ACC-SYS          0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07
0/RP0      N540-ACC-SYS          0.5   MB-IOFPGA            NEED UPGD   0.23      0.23
0/RP0      N540-ACC-SYS          0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

Cisco Smart SFP Destination MAC address

A Destination MAC address is a unique hardware address for Cisco Smart SFPs that:

- Allows seamless communication between Cisco Smart SFPs and third-party devices requiring MAC address validation
- Ensures interoperability by enabling users to configure a specific destination MAC address in the SFP, and
- Resolves validation issues caused by the default destination MAC address of 0, ensuring data packets are accepted by the destination device.

Table 5: Feature History Table

Feature Name	Release Information	Feature Description
Cisco Smart SFP Destination MAC address	Release 25.3.1	The feature is now supported on these platforms: • N540X-16Z4G8Q2C-A • N540X-16Z8Q2C-D

Feature Name	Release Information	Feature Description
Cisco Smart SFP Destination MAC address	Release 25.2.1	We now allow seamless interoperability between Cisco Smart SFPs and third-party devices that require MAC address validation. This capability is achieved by allowing the configuration of a destination MAC address directly on Cisco Smart SFPs. You can configure a specific destination MAC address on Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP) Smart SFPs enabling Cisco Smart SFPs to ensure that data packets are successfully accepted by the destination device. By default, the destination MAC address on the Cisco smart SFPs is zero. The feature is supported only on: • N540-24Z8Q2C-M • NCS540-ACC-SYS

How destination MAC address helps packet transmission using Cisco Smart SFP

In today's diverse networking environments, achieving seamless interoperability in diverse networking environments is essential. When Cisco Smart SFPs interact with third-party SFPs, packet drops may occur due to MAC address validation conflicts.

By default, Cisco Smart SFPs employ a destination MAC address of 00:00:00:00:00:00 that third-party SFPs reject during validation. To ensure interoperability, configure the MAC address of the third-party SFP as the destination MAC address on the Cisco Smart SFP.

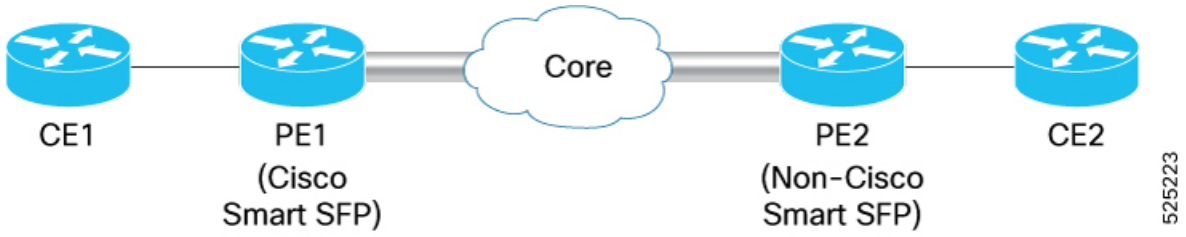
Summary

The key components involved in the packet transmission using Cisco Smart SFP with destination MAC address process are:

- **Customer Edge (CE) Routers**: These routers connect customer networks to provider networks.
- **Provider Edge (PE) Routers**: These routers manage traffic between the core network and customer networks.
- **Cisco Smart SFP**: Installed in PE1, such as Transparent PDH over Packet (tpop) and Channelized SDH over Packet (csop) Smart SFPs.
- **Non-Cisco Smart SFP**: Installed in PE2, the Non-Cisco Smart SFP validates the MAC address of incoming packets.
- **Core**: Intermediate routers in the provider network that forward data between PE routers.

Workflow

Figure 1: Packet transmission using Cisco Smart SFP with destination MAC address



The stages explain how packet transmission occurs using a destination MAC address in a Cisco Smart SFP.

1. **Destination MAC configuration**: Configure the MAC address of the peer SFP as the destination MAC address on the Cisco Smart SFP located on PE1. This ensures that all outgoing packets from PE1 carry a valid destination MAC address, meeting the requirements of the non-Cisco Smart SFP on PE2 and enabling proper packet delivery.
2. **Destination MAC verification**: The Cisco Smart SFP on PE1 uses the newly configured destination MAC address to validate the destination MAC address of incoming packets. If the destination MAC address is invalid, the Cisco Smart SFP discards these packets and records them as missing. This step ensures compliance with the MEF8 Standard 6.6.1 R.57, enhancing the reliability of packet transmission.
3. **Transmission and validation**: With the valid destination MAC address configured on PE1, the non-Cisco Smart SFP on PE2 successfully receives and processes the incoming packets. The non-Cisco Smart SFP validates the destination MAC address on the packets, confirming their correctness and enabling seamless data transmission between the two devices.

Guidelines for Cisco Smart SFP Destination MAC address

- The Cisco Smart SFPs destination MAC address feature is supported in:
  - TPOP (SFP-E1F-SATOP-I)
  - CSOP (SFP-CH-OC3STM1-I)
- The Cisco Smart SFPs destination MAC address feature is supported on:
  - N540-24Z8Q2C-M

    NCS540-ACC-SYS

    N540X-16Z4G8Q2C-A

    N540X-16Z8Q2C-D
- Configure the destination MAC address at the E1 controller level to ensure proper packet validation.
- Packets with a destination MAC address different from the configured address are dropped and counted as missing/underrun packets if incoming MAC address verification is enabled.
- When configuring the destination MAC address, always use the MAC address of the far-end device.
- **CSOP Smart SFP**

- Configuring the destination MAC address for one channel of the STM1 SFP automatically enables verification of incoming packet MAC addresses on all 63 channels
- To disable incoming packet MAC address verification, unconfigure the destination MAC address for each channel individually.
- When the destination MAC address is configured, the CSOP SFP can interoperate with only one device across all 63 channels.

Limitations for Cisco Smart SFP Destination MAC address

Incompatibility with MR-APS

The Cisco Smart SFP Destination MAC address feature is incompatible with Multi-Router Automatic Protection System (MR-APS). Since the MAC address must be reconfigured upon switchover (a process not handled automatically), avoid using this feature with MR-APS.

Configure the destination MAC Addresses on Cisco Smart SFPs

Configuring the destination MAC address on Cisco Smart SFPs to achieve seamless interoperability with peer non-Cisco SFPs that require MAC address validation.

Procedure

Step 1 Configure the MAC address of the peer Non-Cisco Smart SFP as the destination MAC address on the Cisco Smart SFP.

Example:

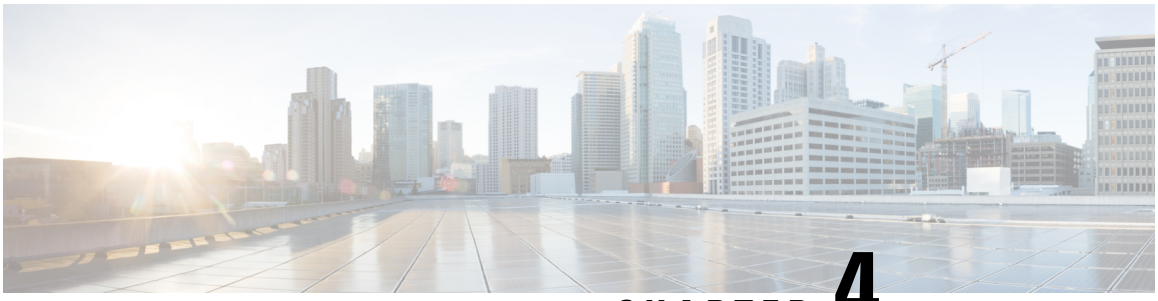
```
Router# config
Router(config)# controller e1 0/0/0/3
Router(config)# dmac-address 1111.2222.3333
```

This configuration enables the Cisco Smart SFP to receive packets from the Non-Cisco Smart SFP with the MAC address 1111.2222.3333.

Step 2 Use the show running configuration command to verify the controller configuration on E1 for a TPoP smart SFP.

Example:

```
Router# show run controller e1 0/0/0/3
controller E1 0/0/0/3
dmac-address 1111.2222.3333
vlan 70 ecid 7
```



CHAPTER 4

TSoP Smart SFP for SDH and SONET Encapsulation

Table 6: Feature History Table

Feature Name	Release	Description
TSoP Smart SFP for SDH and SONET Encapsulation	Release 7.11.1	This release introduces support for the Clear Channel Synchronous Transport Module Level-1 (STM1) Smart SFP (SFP-TS-OC3STM1-I) for the Transparent SONET or SDH over Packet (TSoP) protocol. This allows you to leverage your existing packet-switched network to transport traditional time-division multiplexing (TDM) traffic. TSoP Smart SFPs offer the following advantages: • Encapsulation of SDH or SONET bit streams into packet-switched network format • Improved suitability for pseudowire transport over an Ethernet network

The TSoP Smart SFP (SFP-TS-OC3STM1-I) is a special type of optical transceiver that allows for the transparent encapsulation of SDH or SONET bit streams into a packet format. This format is suitable for transporting pseudowires over an Ethernet network. The TSoP pseudowires can be manually configured or set up using the PWE3 control protocol [RFC4447].

TSoP provides packetization, de-packetization, and clock recovery. It translates the TDM bit stream into fixed-size data blocks (810 octets) and vice versa.

TSoP follows the SAToP method described in [RFC4553] for transporting E1/DS1 pseudowires over a packet-switched network. With TSoP, the entire OC-3 or STM-1 is encapsulated in a single circuit emulating pseudowire traffic. This traffic is then transported to a single destination across the Ethernet network.

Note The TSoP Smart SFP is used on any of the front panel ports of the 8-port Gigabit Ethernet SFP Interface Module (8x1GE).

- The Smart SFP transceivers are compatible with the Small Form Factor Pluggable 20-pin Multi-Source Agreement (MSA).
- TSoP Smart SFP (SFP-TS-OC3STM1-I) transports up to 155 Mbps on a L1.1 (40km) optical data link.

- Prerequisites for TSoP, on page 32
- Restrictions for TSoP, on page 32
- Guidelines for TSoP Smart SFP, on page 33
- De-jitter Buffer , on page 33
- Configuration for TSoP, on page 34

Prerequisites for TSoP

This section provides information about the prerequisites that apply to TSoP.

- Single mode optical fiber must be used to connect TSoP Smart SFP with the OC-3 port.
- The TSoP smart SFP pseudowire endpoints must use the same configuration parameters.

Restrictions for TSoP

This section provides information about the restrictions that apply to TSoP.

- TSoP is not supported on the 25GE ports, but it’s supported only on 1GE and 10GE ports.
- The RTP clock source value is Ethernet, by default. The **Clock source internal/line** under the **controller STM1** *r/s/i/p*, is not applicable.
- Ensure that there is at least 2 minutes time-delay between the swaps, during a quick OIR of TSoP smart SFP with other SFPs on the same port.
- Before you insert TSoP, always ensure that the Ethernet interface is in a **shutdown** state. If TSoP doesn't come up when the Ethernet interface is accidentally present in **no shut**, then remove TSoP and insert Gigabit Ethernet SFP to move it to the shutdown state, and then reinsert TSoP as a workaround.
- TSoP only supports Differential Clock Recovery (DCR) by default and doesn’t support any other clock configuration.
- Both sides of PE only support TSoP. Currently, interoperability with other devices is not supported.

Guidelines for TSoP Smart SFP

The TSoP is compatible with the following SFPs supported on the OC-3 interface module. We recommend using the specified attenuator:

- ONS-SI-155-I1 - For a cable length of 15km, use a 2 dB attenuator. Use an 8 dB attenuator for short distances to avoid receiver overload.
- ONS-SI-155-L1 - For a cable length of 40km, no attenuator is needed. Use a 10 dB attenuator for short distances to avoid receiver overload.
- ONS-SI-155-L2 - For a cable length of 40km, use a 2 dB attenuator. Use a 10 dB attenuator for short distances to avoid receiver overload.



Note Multimode SFP is not supported with TSoP.

De-jitter Buffer

A de-jitter buffer is a component in a packet-based network that helps mitigate the effects of jitter. Jitter refers to the variation in the arrival time of packets, which can lead to inconsistent delays and packet loss in real-time applications like voice or video.

The de-jitter buffer works by temporarily storing incoming packets and then releasing them at a regulated pace. It smooths out the variations in packet arrival times and ensures a more consistent and reliable stream of packets for playback.

The primary purpose of the de-jitter buffer is to ensure a steady and continuous playback of real-time data, such as voice packets in a voice-over-IP (VoIP) call. By absorbing and compensating for the variable delay, it helps maintain a stable voice quality without noticeable gaps or interruptions in the audio stream.

The size of the de-jitter buffer is a critical parameter to consider in network design. It should be large enough to handle the maximum expected delay variation (jitter) while still providing an acceptable level of delay. However, the buffer cannot be too large, as excessive buffering can introduce additional delay and affect the real-time nature of the application.

The de-jitter buffer for the TSoP can be configured to the following values:

- 292
- 627
- 810
- 1296
- 2633

Example configuration

This example shows how to configure De-jitter buffer.

```
sh controll cem 0/0/0/10 payload-dejitter-mapping
Thu Jan 19 12:40:16.206 UTC
Client type : STM1
Client rate (in kbps) : 155000
Client default payload (in bytes) : 810
Client default dejitter (in usec) : 1296

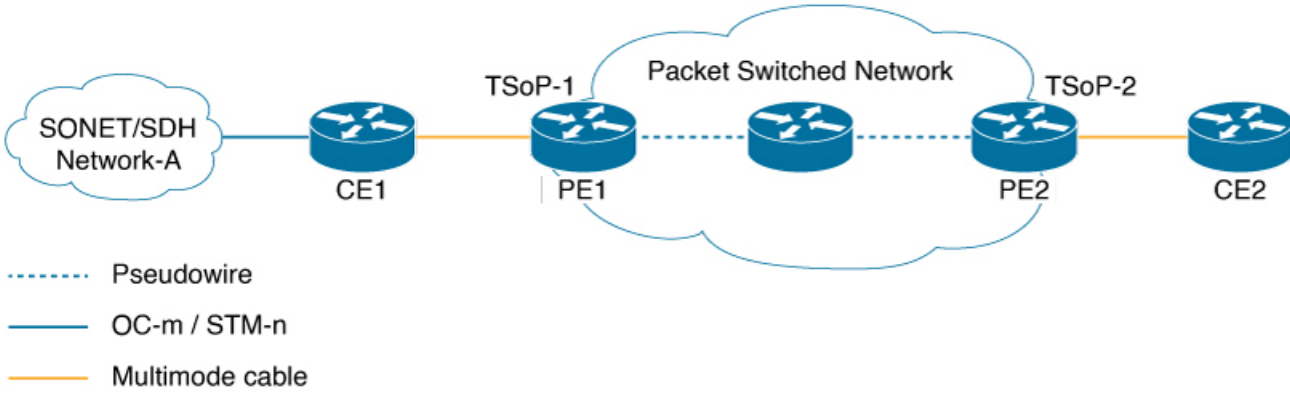
Payload (in bytes) Possible dejitter values (in microseconds)
------------------------------------------------------------
810 2633, 1296, 627, 292

For configuring out of range, we will get the below error:
Int CEM <>
cem payload 810 dejitter 696
!
```

Configuration for TSoP

Here is a sample configuration for TSoP:

Figure 2: TSoP in Packet Switched Network



Pre-requisites

These are the prerequisites for configuring PE routers and CE (SONET or SDH) routers for TSoP:

- The following are the pre-requisites on CE routers ASR 903:
  - The CE side routers must be ASR 903 operating on RSP4 or RSP3
  - SFP-OC3-SR must be plugged into ASR 903 for transmitting SONET or SDH packets
  - Supported Interface modules are:
    - NCS4200-1T8S-20CS
    - A900-IMA3G-1MSG
- The PE side routers must be NCS 5500 or NCS 540.
- PE and CE routers must be connected using multimode cable
- Only static L2VPN tunnel configuration is supported

- Sync-E should be operational

Note Traffic switch over is not supported even when multiple links are available. Traffic flow occurs as per the adjacent labels or hops defined by the user during static L2VPN tunnel configuration

Configuration for

1. This example shows how to configure clock synchronization on the PE routers.

   - Configuring Smart SFP in PE1

   ```
   Router(config)# frequency synchronization quality itu-t option 1
   Router(config)# interface GigabitEthernet0/0/0/5
   Router(config)# no shut
   Router(config)# frequency synchronization
   Router(config)# quality transmit exact itu-t option 1 PRC
   ```

   - Configuring Smart SFP in PE2

   ```
   Router(config)# frequency synchronization quality itu-t option 1
   Router(config)# interface GigabitEthernet0/0/0/18
   Router(config)# frequency synchronization
   Router(config)# selection input
   Router(config)# priority 1
   Router(config)# wait-to-restore 0
   ```

2. This example shows how to configure PE and CE interfaces.

   - Configuration at CE1

   ```
   Router(config)# interface CEM0/0/0/10
   Router(config)# l2transport
   ```

   - Configuration at PE1

   ```
   Router(config)# interface GigabitEthernet0/0/0/5
   Router(config)# ipv4 address 10.1.1.1 255.255.255.0
   Router(config)# no shut
   ```

   - Configuration at CE2

   ```
   Router(config)# interface CEM0/0/0/17
   Router(config)# l2transport
   ```

   - Configuration at PE2

   ```
   Router(config)# interface GigabitEthernet0/0/0/18
   Router(config)# ipv4 address 10.1.1.2 255.255.255.0
   Router(config)# no shut
   ```

3. This example shows how to configure loopback interface.

   - Configuration at PE1

   ```
   Router(config)# interface Loopback0
   Router(config)# ipv4 address 1.1.1.1 255.255.255.255
   ```

   - Configuration at PE2

```
Router(config)# interface Loopback0
Router(config)# ipv4 address 1.1.1.4 255.255.255.255
```

4. This example shows how to configure the ISIS IGP and advertise loopback and core interfaces.

   • Configuration at PE1

```
Router(config)# router isis core
Router(config)#is-type level-2-only
Router(config)#net 49.0000.0000.0000.0001.00
Router(config)#nsr
Router(config)#nsf cisco
Router(config)#log adjacency changes
Router(config)#address-family ipv4 unicast
Router(config)#metric-style wide
Router(config)#segment-routing mpls sr-prefer
Router(config)#segment-routing bundle-member-adj-sid
Router(config)#address-family ipv6 unicast
Router(config)#metric-style wide
Router(config)#segment-routing mpls sr-prefer
Router(config)#segment-routing bundle-member-adj-sid
Router(config)#interface Loopback0
Router(config)#point-to-point
Router(config)#address-family ipv4 unicast
Router(config)#prefix-sid index 1
Router(config)#address-family ipv6 unicast
Router(config)#interface GigabitEthernet0/0/0/5
Router(config)#point-to-point
Router(config)#address-family ipv4 unicast
Router(config)#adjacency-sid absolute 28121
Router(config)#address-family ipv6 unicast
```

   • Configuration at PE2

```
Router(config)#router isis core
Router(config)#is-type level-2-only
Router(config)#net 49.0000.0000.0000.0004.00
Router(config)#nsr
Router(config)#nsf cisco
Router(config)#log adjacency changes
Router(config)#address-family ipv4 unicast
Router(config)#metric-style wide
Router(config)#segment-routing mpls sr-prefer
Router(config)#segment-routing bundle-member-adj-sid
Router(config)#address-family ipv6 unicast
Router(config)#metric-style wide
Router(config)#segment-routing mpls sr-prefer
Router(config)#segment-routing bundle-member-adj-sid
Router(config)#interface Loopback0
Router(config)#point-to-point
Router(config)#address-family ipv4 unicast
Router(config)#prefix-sid index 4
Router(config)#address-family ipv6 unicast
Router(config)#interface GigabitEthernet0/0/0/18
Router(config)#point-to-point
Router(config)#address-family ipv4 unicast
Router(config)#adjacency-sid absolute 28211
Router(config)#address-family ipv6 unicast
```

5. This example shows how to configure Circuit-styled Segment routing traffic engineering tunnels.

   • Configuration at PE1

```
Router(config)#segment-routing
Router(config)#global-block 80000 111999
Router(config)#local-block 25000 28999
Router(config)#traffic-eng
Router(config)#segment-list pe1-pe2-forward-path
Router(config)#index 1 mpls label 28121
Router(config)#segment-list pe1-pe2-reverse-path
Router(config)#index 1 mpls label 28211
Router(config)#policy pe1-pe2-circuit-styled-srte
Router(config)#color 10 end-point ipv4 1.1.1.4
Router(config)#path-protection
Router(config)#candidate-paths
Router(config)#preference 10
Router(config)#explicit segment-list pe1-pe2-forward-path
Router(config)#reverse-path segment-list pe1-pe2-reverse-path
```

- Configuration at PE2

```
Router(config)#segment-routing
Router(config)#global-block 80000 111999
Router(config)#local-block 25000 28999
Router(config)#traffic-eng
Router(config)#segment-list pe1-pe2-forward-path
Router(config)#index 1 mpls label 28121
Router(config)#segment-list pe1-pe2-reverse-path
Router(config)#index 1 mpls label 28211
Router(config)#policy pe1-pe2-circuit-styled-srte
Router(config)#color 10 end-point ipv4 1.1.1.4
Router(config)#path-protection
Router(config)#candidate-paths
Router(config)#preference 10
Router(config)#explicit segment-list pe1-pe2-forward-path
Router(config)#reverse-path segment-list pe1-pe2-reverse-path
```

6. This example shows how to configure BGP EVPN neighbor session.

- Configuration at PE1

```
Router(config)#router bgp 100
Router(config)#bgp router-id 1.1.1.1
Router(config)#bgp graceful-restart
Router(config)#address-family ipv4 unicast
Router(config)#address-family l2vpn evpn
Router(config)#neighbor 1.1.1.4
Router(config)#remote-as 100
Router(config)#update-source Loopback0
Router(config)#graceful-restart
Router(config)#address-family l2vpn evpn
```

- Configuration at PE2

```
Router(config)#bgp router-id 1.1.1.4
Router(config)#bgp graceful-restart
Router(config)#address-family ipv4 unicast
Router(config)#address-family l2vpn evpn
Router(config)#neighbor 1.1.1.1
Router(config)#remote-as 100
Router(config)#update-source Loopback0
Router(config)#graceful-restart
Router(config)#address-family l2vpn evpn
```

7. This example shows how to configure EVPN xconnect.

   - Configuration at PE1

```
Router(config)#l2vpn
Router(config)#pw-class pw-cs-srte
Router(config)#encapsulation mpls
Router(config)#preferred-path sr-te policy pe1-pe2-circuit-styled-srte
Router(config)#xconnect group evpn_vpws
Router(config)#p2p p1
Router(config)#interface CEM0/0/0/10
Router(config)#neighbor evpn evi 10 target 1 source 2
Router(config)#pw-class pw-cs-srte
```

   - Configuration at PE2

```
Router(config)#l2vpn
Router(config)#pw-class pw-cs-srte
Router(config)#encapsulation mpls
Router(config)#preferred-path sr-te policy pe1-pe2-circuit-styled-srte
Router(config)#xconnect group evpn_vpws
Router(config)#p2p p1
Router(config)#interface CEM0/0/0/17
Router(config)#neighbor evpn evi 10 target 2 source 1
Router(config)#pw-class pw-cs-srte
```

8. This example shows how to configure Dejitter.

   - Configuration at PE1

```
Router(config)#int cem0/0/0/10
Router(config)#cem payload 810 dejitter 696
```

   - Configuration at PE2

```
Router(config)#int cem0/0/0/17
Router(config)#cem payload 810 dejitter 696
```

Verification

Use the **show inventory** command to display all TSoP Smart SFPs installed on the router.

```
Router#show inventory
NAME: "GigabitEthernet0/0/0/17", DESCR: "Cisco SFP TSOP STM1 Pluggable Optics Module"
PID: SFP-TS-OC3STM1-I , VID: V01, SN: OEA2536001J
```

Use the **show hw-module fpd** command to display TSoP Smart SFPs FPD version.

```
Router#show hw-module fpd
Auto-upgrade:Disabled
FPD Versions
==============
Location Card type HWver FPD device ATR Status Running Programd
-------------------------------------------------------------------------------------------
0/RP0 NCS-55A2-MOD-SE-S 1.0 MB-MIFPGA CURRENT 0.21 0.21
0/RP0 NCS-55A2-MOD-SE-S 1.0 SSFP_OC3_STM1_6 CURRENT 12.01 12.01
0/RP0 NCS-55A2-MOD-SE-S 1.0 SSFP_STM1_TSOP_17 CURRENT 13.00 13.00  <<<<
0/RP0 NCS-55A2-MOD-SE-S 1.0 Bootloader CURRENT 1.18 1.18
0/RP0 NCS-55A2-MOD-SE-S 1.0 CPU-IOFPGA CURRENT 1.27 1.27
0/RP0 NCS-55A2-MOD-SE-S 1.0 MB-IOFPGA NEED UPGD 0.18 0.18
0/RP0 NCS-55A2-MOD-SE-S 1.0 SATA-INTEL_240G NEED UPGD 1120.00 1120.00
0/PM0 NC55-1200W-ACFW 1.0 LIT-PriMCU-ACFW CURRENT 2.09 2.09
```

```
0/PM1 NC55-1200W-ACFW LIT-PriMCU-ACFW NOT READY
RP/0/RP0/CPU0:ios#
```

Use the **show ipv4 interface brief** command to display the interface status.

```
Router#show ipv4 interface brief
Interface IP-Address Status Protocol Vrf-Name
MgmtEth0/RP0/CPU0/0 unassigned Shutdown Down default
TenGigE0/0/0/0 unassigned Shutdown Down default
GigabitEthernet0/0/0/1 unassigned Shutdown Down default
GigabitEthernet0/0/0/2 unassigned Shutdown Down default
TenGigE0/0/0/3 unassigned Shutdown Down default
TenGigE0/0/0/4 unassigned Shutdown Down default
GigabitEthernet0/0/0/5 unassigned Shutdown Down default
GigabitEthernet0/0/0/6 unassigned Up Up default
GigabitEthernet0/0/0/7 unassigned Shutdown Down default
GigabitEthernet0/0/0/8 unassigned Shutdown Down default
GigabitEthernet0/0/0/9 unassigned Shutdown Down default
GigabitEthernet0/0/0/10 unassigned Shutdown Down default
TenGigE0/0/0/11 unassigned Shutdown Down default
TenGigE0/0/0/12 unassigned Shutdown Down default
TenGigE0/0/0/13 unassigned Shutdown Down default
TenGigE0/0/0/14 unassigned Shutdown Down default
TenGigE0/0/0/15 unassigned Shutdown Down default
GigabitEthernet0/0/0/16 unassigned Up Up default
CEM0/0/0/17 unassigned Up Up default   <<<
GigabitEthernet0/0/0/18 unassigned Shutdown Down default
TenGigE0/0/0/19 unassigned Shutdown Down default
```

Use the **show controller cem** verifying TSoP smart SFP stats and Dejitter configuration.

```
Router#show controller cem 0/0/0/17
Interface : CEM0/0/0/17
Admin state : Up
Oper state : Up
Port bandwidth : 155000 kbps
Dejitter buffer (oper/in-use) : 1296/180064 usec   <<<<<<
Payload size (oper) : 810 bytes
PDV (min/max/avg) : 51589/142643/97116 usec
Dummy mode : last-frame
Dummy pattern : 0x0
Idle pattern : 0x0
Signalling : No CAS
RTP : Not Enabled
Clock type : Differential
Detected Alarms : None

Statistics Info
---------------
Ingress packets : 0, Ingress packets drop : 0
Egress packets : 0, Egress packets drop : 0
Total error : 1145472000
Missing packets : 572736000, Malformed packets : 0
Jitter buffer underrun : 572736000, Jitter buffer overrun : 0
Misorder drops : 0
Reordered packets : 0, Frames fragmented : 0
Error seconds : 0, Severely error seconds : 0
Unavailable seconds : 0, Failure counts : 0

Generated L bits : 0, Received L bits : 0
Generated R bits : 0, Received R bits : 0

Endpoint Info
-------------
Passthrough : No
```

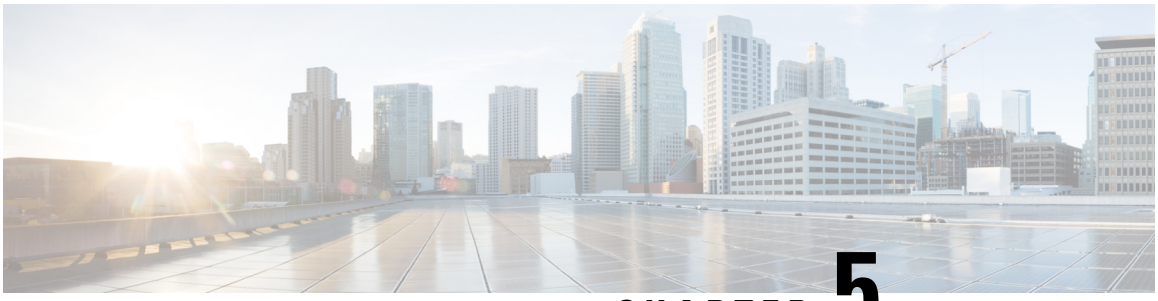
```
//Run the same command on CEm interface of PE1 router.

Router#show controll CEM0/0/0/10
Sat Mar 25 10:49:19.471 UTC
Interface                          : CEM0/0/0/6
Admin state                        : Up
Oper  state                        : Up
Port bandwidth                     : 155000 kbps
Dejitter buffer (oper/in-use)      : 1296/180645 usec
Payload size (oper)                : 810 bytes
PDV (min/max/avg)                  : 51589/142643/97116 usec
Dummy mode                         : last-frame
Dummy pattern                      : 0xab
Idle pattern                       : 0xff
Signalling                         : No CAS
RTP                                : Enabled
Clock type                         : Differential
Detected Alarms                    : None

Statistics Info
---------------
Ingress packets          : 0, Ingress packets drop     : 0
Egress packets           : 0, Egress packets drop      : 0
Total error              : 385536000
        Missing packets          : 192768000, Malformed packets        : 0
        Jitter buffer underrun   : 192768000, Jitter buffer overrun    : 0
        Misorder drops           : 0
Reordered packets        : 0, Frames fragmented        : 0
Error seconds            : 0, Severely error seconds   : 0
Unavailable seconds      : 0, Failure counts           : 0

Generated L bits         : 0, Received  L bits         : 0
Generated R bits         : 0, Received  R bits         : 0

Endpoint Info
-------------
Passthrough     : No
RP/0/RP0/CPU0:Router#
```



CHAPTER 5

Understanding PTP

The Precision Time Protocol (PTP), as defined in the IEEE 1588 standard, synchronizes withnanosecond accuracy the real-time clocks of the devices in a network. The clocks in are organized into a server-client hierarchy. PTP identifies the port that is connected to a device with the most precise clock. This clock is referred to as the server clock. All the other devices on the network synchronize their clocks with the server clock and are referred to as members. Constantly-exchanged timing messages ensure continued synchronization.

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.

Table 7: Nodes within a PTP Network

Network Element	Description
Grandmaster (GM)	A network device physically attached to the primary time source. All clocks are synchronized to the grandmaster clock.
Ordinary Clock (OC)	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 clock. • 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.

Network Element	Description
Boundary Clock (BC)	The device participates in selecting the best server clock and can act as the server clock if no better clocks are detected. Boundary clock starts its own PTP session with a number of downstream clients. The boundary clock mitigates the number of network hops and results in packet delay variations in the packet network between the Grandmaster and client.
Transparent Clock (TC)	A transparent clock is a device or a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of time calculations.

Note In Cisco IOS XR Release 7.3.1, on the Cisco N540-FH-CSR-SYS router, PTP is not supported on ports 0-14.

Note In Cisco IOS XR Release 7.3.2, PTP is enabled by default on all Ethernet ports of the following variants of the Cisco NCS 540 router. This support facilitates interoperability with FPGA ports.

- N540-FH-CSR-SYS
- N540-FH-AGG-SYS

- Why PTP?, on page 43
- Routers and Delays, on page 43
- Message-Based Synchronization, on page 43
- **PTP Event Message Sequences**, on page 44
- PTP Clocks, on page 46
- Restrictions for PTP, on page 46
- PTP Phase Difference Threshold Between Passive and Secondary Ports, on page 47
- Isolate Foreign Masters Causing Packet Timing Signal Fail, on page 49
- Advance monitoring, on page 52
- PTP Profiles, on page 55
- Monitor PTP virtual port using PTP timeReceiver ports, on page 74
- Slow Tracking, on page 79
- PTP Holdover Traceability Suppression, on page 80
- IEEE Default Profile , on page 81
- PTP Hybrid Mode, on page 82
- Verifying the PTP Hybrid Mode Configurations, on page 85
- Performance Monitoring for PTP Networks, on page 86

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 requirement for PTP data packets

Routers and Delays

In an IP network, routers provide a full-duplex communication path between network devices. Routers send data packets to packet destinations using IP address information contained in the packets. When the router attempts to send multiple packets simultaneously, the router buffers some packets so that they are not lost before they are sent. When the buffer is full, the router delays sending packets. This delay can cause device clocks on the network to lose synchronization with one another.

Additional delays can occur when packets entering a router are stored in its local memory while the router searches the address table to verify packet fields. This process causes variations in packet forwarding time latency, and these variations can result in asymmetrical packet delay times.

Adding PTP to a network can compensate for these latency and delay problems by correctly adjusting device clocks so that they stay synchronized with one another. PTP enables network routers to function as PTP devices, including boundary clocks (BCs) and transparent clocks (TCs).

For more information about PTP clock devices and their role in a PTP network, see the *PTP Clocks* section.

Message-Based Synchronization

To ensure clock synchronization, PTP requires an accurate measurement of the communication path delay between the time source (server) and the receiver (client). PTP sends messages between the server and client device 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. The local clocks are adjusted for this delay using a series of messages sent between servers and clients. 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, routed networks do not necessarily have symmetrical communication paths, due to the various asymmetries in the network.

Using transparent clocks, PTP provides a method to measure and account for the delay in a time-interval field in network timing packets. This makes the routers temporarily transparent to the server and client nodes on

the network. An end-to-end transparent clock forwards all messages on the network in the same way that a router does.

To read a detailed description of synchronization messages, see the *PTP Event Message Sequences* section. To learn more about how transparent clocks calculate network delays, refer to Transparent Clock, on page 7.

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

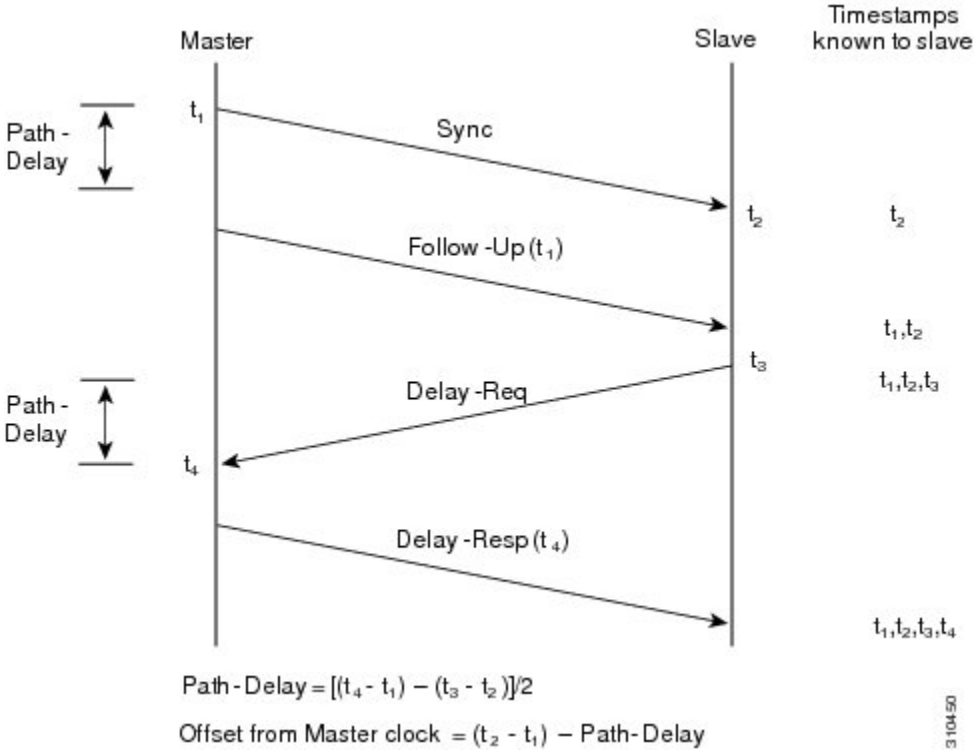
These messages are sent in the following sequence:

- The server sends a Sync message to the client and notes the time (t1) at which it was sent.
- The client receives the Sync message and notes the time of reception (t2).
- The server conveys to the client the timestamp t1 by embedding the timestamp t1 in a Follow_Up message.
- The client sends a Delay_Req message to the server and notes the time (t3) at which it was sent.
- The server receives the Delay_Req message and notes the time of reception (t4).
- The server conveys to the client the timestamp t4 by embedding it in a Delay_Resp message.

After this sequence, the client possesses all four timestamps. These timestamps can be used to compute the offset of the client clock relative to the server, 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 server to client is the same as the time required from client to server. This assumption is not always valid on an Ethernet/IP network due to asymmetrical packet delay times.

Figure 3: Detailed Steps—Boundary Clock Synchronization



Delay-Response Mechanism

The Delay Request-response mechanism (defined in section 11.3 of IEEE Std 1588-2008) lets a slave port estimate the difference between its own clock-time and the clock-time of its master. The following options are supported:

- One-step mechanism - The timestamp for a Sync message is received in the Sync message itself.
- Two-step mechanism - The timestamp for a Sync message is received later in a Follow-up message.

When running a port in Slave state, a router shall send Delay-request messages and handle incoming Sync, Follow-up, and Delay-response messages. The timeout periods for both Sync and Delay-response messages are individually configurable.

When running a port in Master state, only one-step is supported, and in slave state, both one-step and two-step are supported without configuration.

Synchronizing the Local Clock

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

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

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 PTP clock with a single PTP port. It functions as a node in a PTP network and can be selected by the BMCA as a server or client within a subdomain. 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. Ordinary clocks have various interfaces to external devices.

Boundary Clock

A boundary clock in a PTP network operates in place of a standard network 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 as a client. The server port synchronizes the clocks connected downstream, while the client port synchronizes with the upstream server 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.

Restrictions for PTP

- PTP over MPLS is not supported.
- On Cisco N540X-16Z4G8Q2C-D routers, use the dedicated copper ports 0 through 3 when copper connectivity is required. Do not install a copper SFP in an optical port. This configuration can cause SyncE problems.
- Configure one endpoint as a PTP server and the peer as a PTP client simultaneously. A PTP session does not establish when both endpoints are forced to the same role.

PTP Phase Difference Threshold Between Passive and Secondary Ports

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
PTP Phase Difference Threshold Between Passive and Secondary Ports	Release 25.1.1	Passive ports can participate in the Delay Request-Response Mechanism (DRRM), allowing for the observation of PTP phase differences between a passive port and a secondary port. This feature is now supported on: • N540-24Q2C2DD-SYS

Feature Name	Release Information	Feature Description
PTP Phase Difference Threshold Between Passive and Secondary Ports	Release 24.2.1	Introduced in this release on the following Cisco NCS 540L and NCS 540X router variants running on Cisco IOS XR: • N540X-12Z16G-SYS-A/D • N540-12Z20G-SYS-A/D • N540-28Z4C-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540-FH-CSR-SYS • N540-FH-AGG-SYS • N540-24Q8L2DD-SYS • N540X-6Z18G-SYS-A/D • N540X-8Z16G-SYS-A/D • N540X-4Z14G2Q-A/D • N540-6Z14S-SYS-A/D Passive ports can now be included in the Delay Request-Response Mechanism (DRRM), which allows for the monitoring of PTP phase differences between a passive port and a secondary port. If these PTP phase differences surpass a predefined limit, system logs are triggered. This feature enables you to detect potential errors such as fiber asymmetry or a clock failure in the PTP network. This feature introduces these changes: **CLI:** • **phase-difference-threshold-breach** • The **show ptp foreign-masters** command output is enhanced to include phase difference values and servo status. **YANG Data Models:** The following data models are enhanced: • `Cisco-IOS-XR-ptp-cfg.yang` • `Cisco-IOS-XR-um-ptp-cfg.yang`

The Precision Time Protocol (PTP), as defined in the IEEE 1588 standard, is designed for precise time synchronization across networked devices. It operates by having Foreign Masters (FMs) broadcast timing information to interfaces within the network. The selection of the Grandmaster (GM), the primary reference

clock, is determined by the Best Master Clock Algorithm (BMCA). Devices synchronize their clocks to the GM through a process known as the Delay Request-Response Mechanism (DRRM), wherein ports that are directly synchronizing with the GM enter a secondary state.

Historically, ports in a passive state—those that receive timing messages from FMs but aren't used for synchronization to the GM were not monitored by the router. Starting with Cisco IOS XR Software Release 24.2.1, these passive ports are enabled for the calculation of PTP phase differences between the FMs on passive ports and the GM.

This calculated PTP phase difference provides a valuable insight into the timing characteristics of other foreign masters in the network by using the grandmaster as a reference point. It can be utilized on any boundary clock or slave clock that has connections to at least one other foreign master.

You can access these measurements and the calculated PTP phase differences using show commands through the router's CLI. Also, the information can be retrieved programmatically through operational data models in YANG, providing flexibility in how you can access and utilize this synchronization data.

Phase Difference Alarm

PTP phase difference can also be used to monitor the timing properties of the network. You can configure a value at which a bistate alarm is triggered when the PTP phase difference of a FM exceeds the threshold. The PTP phase difference can have a negative or positive value, but the threshold can only be the absolute value. You can configure the PTP phase difference threshold using the **phase-difference-threshold-breach** command.

System Log for PTP Phase Difference

When the configured threshold is reached, system logs (syslogs) are displayed. The following syslog is triggered if the configured PTP phase difference threshold is passed through by any master.

```
Phase difference for clock ACDE48FFFE234567, steps removed 1, receiving-port 1, received
on interface GigabitEthernet0/2/0/3 is 40ns, configured threshold is 30ns. Raising phase
difference alarm.
```

Isolate Foreign Masters Causing Packet Timing Signal Fail

Table 9: Feature History Table

Feature Name	Release Information	Feature Description
Isolate foreign timeTransmitters causing packet timing signal failure	Release 25.1.1	The capability to isolate foreign timeTransmitters that lead to packet timing signal failures is available for: • N540-24Q2C2DD-SYS

Feature Name	Release Information	Feature Description
Isolate Foreign Masters Causing Packet Timing Signal Fail	Release 24.2.1	

Feature Name	Release Information	Feature Description
		Introduced in this release on the following Cisco NCS 540 router variants running on Cisco IOS XR: • N540X-12Z16G-SYS-A/D • N540-12Z20G-SYS-A/D • N540-28Z4C-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540-FH-CSR-SYS • N540-FH-AGG-SYS • N540-24Q8L2DD-SYS • N540X-6Z18G-SYS-A/D • N540X-8Z16G-SYS-A/D • N540X-4Z14G2Q-A/D • N540-6Z14S-SYS-A/D This feature permits the flexible selection of timing sources by filtering out Foreign Master (FM) clocks that exhibit unstable timing. This filtering causes the secondary clocks to produce a signal deemed Packet Timing Signal Fail (PTSF)-unusable, from consideration within the Best Master Clock Algorithm (BMCA). The system continuously monitors these clocks for timing stabilization, and upon detecting enhanced stability, it may reevaluate and possibly reintegrate them as suitable time sources. This feature introduces these changes: **CLI:** • **detect-ptsf-unusable** • The **show ptp foreign-masters** command output is enhanced to include phase difference values and servo status.

Feature Name	Release Information	Feature Description
		YANG Data Models: The following data models are enhanced: • `Cisco-IOS-XR-ptp-cfg.yang` • `Cisco-IOS-XR-um-ptp-cfg.yang`

Starting Cisco IOS XR Software Release 24.2.1, the servo mechanism now has the ability to detect unusable clocks due to packet timing signal fail by analyzing timestamps from foreign masters. This enhancement allows the system to identify foreign masters with unstable timing as unsuitable for use. A platform supports multiple masters, such a master can be excluded from the BMCA selection process while remaining under observation for potential recovery. Even after a master is deemed unusable, the DRRM continues to operate and timestamps from it are still provided to the servo. This ongoing monitoring enables PTP to detect and respond to any improvements in the primary's timing, allowing it to be reconsidered as usable.

System Log for PTSF-unusable

When the master becomes PTSF-unusable, and if its the current Grandmaster, the following system log (syslogs) is displayed:

```
Foreign master with clock ID ACDE48FFFE234567, steps removed 1, receiving-port 1, received
 on interface GigabitEthernet0/2/0/4 is now PTSF-unusable and disqualified from selection.
```

Advance monitoring

Advance monitoring is a network management tool that

- monitors alternative transmission paths within a network
- enhances the detection of network issues, such as clock failures or asymmetries, by providing comprehensive oversight, and
- analysis of network performance.

Table 10: Feature History Table

Feature Name	Release Information	Feature Description
Advance monitoring	Release 25.1.1	You can now enhance the detection of network issues, such as clock failures or asymmetries, by using advanced monitoring. This optional extension to the ITU-defined PTP G.8275.1 profile offers additional capabilities for monitoring alternative time transmitter information through the PTP port. This feature introduces these changes: **CLI:** • **monitor-receiver** • **monitor-sender**

Advance Monitoring monitors alternative transmission paths in the network and enhances the detection of network issues, such as clock failures or asymmetries.

You can enable advance monitoring using these configuration options `monitor-receiver` and `monitor-sender` enables the exchange of PTP packets beyond the typical port states.

These configuration options allows a port in the time-transmitter state to receive packets and allows a time-receiver to send packets.

When the port is configured with monitor-sender or monitor-receiver, the announce messages are sent with the correct alternateTimeTransmitter flag state.

Note With the introduction of the Phase Difference feature in version 24.2.1, platforms that support monitoring multiple sources will already send delay request packets from ports in the Passive state without needing additional configuration. But they do not set the alternate timeTransmitter flag.

packet exchange

You can monitor packet exchange by enabling these flags:

- monitor-receiver flag on the main port and monitor-sender flag on the passive port to understand the time error in the PTP network.
- monitor-receiver flag on the main port and PTP port, the PTP probe monitors PTP clock once both the ports initiate DRRM.

Note In some cases, monitoring the packet exchange may only require a single direction of exchange.

Configure advance monitoring

These configuration options can allow a port in the time-transmitter state to receive packets and allow a time-receiver to send packets.

Procedure

Step 1 Configure monitor-receiver or monitor-sender for advance monitoring.

- To configure monitor-receiver on the the main port through ptp profile:

```
Router# configure
Router(config)# ptp
Router(config-ptp)# profile demo
Router(config-ptp-profile)# monitor-receiver
Router(config-ptp-profile)# commit
```

- To configure monitor-sender on the the passive port through ptp profile:

```
Router# configure
Router(config)# ptp
Router(config-ptp)# profile demo
Router(config-ptp-profile)# monitor-sender
Router(config-ptp-profile)# commit
```

- To configure monitor-receiver on the the main port through interface ptp:

```
Router# configure
Router(config)# interface <name>
Router(config-if)# ptp
Router(config-if-ptp)# monitor-receiver
Router(config-if-ptp)# commit
```

- To configure monitor-sender on the the passive port through interface ptp:

```
Router# configure
Router(config)# interface <name>
Router(config-if)# ptp
Router(config-if-ptp)# monitor-sender
Router(config-if-ptp)# commit
```

Step 2 Execute the following command to verify the monitor-receiver and monitor-sender configuration.

- Execute the **show ptp interfaces** command to verify the monitor-receiver.

  In this example, the Time_transmitter is configured with monitor-receiver enabled, and the Monitor-Receiver is set to true.

```
Router# show ptp interfaces GigabitEthernet0/8/0/2
GigabitEthernet0/8/0/2 is in Master state
  PTP port number: 1
  Transport: Ethernet Multicast
  Address: b4a8.b905.4892
  Linestate: Up
  Monitor-Sender: False
  Monitor-Receiver: True
  Local Priority: 128
  Mechanism: Delay-request-response
  Sync rate: 16 per-second
  Announce rate: 8 per-second, timeout 3 intervals
```

```
Min Delay-Request rate: 16 per-second
CoS: General 6, Event 6, DSCP: General 46, Event 46
Profile interop: No
Platform capabilities (as Master):
  Supported:     L2 Encapsulation, Ethernet, IPv4, IPv6, Unicast,
                 Multicast, Master, Slave
  Not-supported: Source IP
  Max-Sync-rate: 128 per second
Master state only
0 Unicast peers
```

Step 3 Execute the **show ptp foreign-masters** command to verify the alternatemaster flag.

- In this example, the Time_transmitter is configured with monitor-receiverenabled and alternateMaster is set to true.

```
Router# show ptp foreign-masters GigabitEthernet0/8/0/2
Interface GigabitEthernet0/8/0/2 (PTP port number 1)
  Ethernet, Address 7426.acf7.4d9c, Multicast
    Configured priority: None (128)
    Configured clock class: None
    Configured delay asymmetry: None
    Is alternateMaster: True
    Qualified for 5 minutes, 24 seconds
    Clock ID: 7426acfffef74e80
    Received clock properties:
      Domain: 24, Priority1: 128, Priority2: 128, Class: 248
      Accuracy: 0xfe, Offset scaled log variance: 0xffff
      Steps-removed: 1, Time source: Internal, Timescale: PTP
      Frequency-traceable
      Current UTC offset: 37 seconds (valid)
    Parent properties:
      Clock ID: 7426acfffef74e80
      Port number: 1
```

PTP Profiles

Table 11: Feature History Table

Feature Name	Release Information	Description
PTP profiles support for N540X-6Z6G-SYS	Release 25.4.1	PTP Profiles are now supported on the following Cisco NCS 540 router variant: • N540X-6Z6G-SYS
PTP profiles support on N540-24Q8L2DD-SYS	Release 25.4.1	G8273.2 Class C PTP for 1G ports 2 to 9 are now supported on these NCS 540 Series router variant: • N540-24Q8L2DD-SYS

Feature Name	Release Information	Description
PTP profiles support for N540-24Q2C2DD-SYS	Release 25.1.1	PTP Profiles are now supported on the following Cisco NCS 540 router variant: • N540-24Q2C2DD-SYS
PTP and SyncE support on breakout ports for N540-24Q8L2DD-SYS and N540X-16Z4G8Q2C-A/D Routers	Release 7.11.1	With this release, timing support for PTP and SyncE is extended to the following NCS 540 routers: • N540-24Q8L2DD-SYS • N540X-16Z4G8Q2C-A/D Class B and Class C performances are supported on 4x10G and 4x25G breakout ports in N540X-16Z4G8Q2C-A/D Routers. Class B is supported on N540-24Q8L2DD-SYS for for 1G ports 10-33.
PTP Profiles Support for N540-6Z14S-SYS-D	Release 7.5.2	PTP Profiles are now supported on the following Cisco NCS 540 router variant: • N540-6Z14S-SYS-D
PTP Profiles Support for N540-24Q8L2DD-SYS	Release 7.4.1	PTP Profiles are specific selections of PTP configurations that allow organizations to achieve a performance that meets the requirement of a particular application. You can configure different PTP profiles for different applications, such as audio and media. PTP profiles ensure the application components stay in sync across multiple devices. PTP Profiles are now supported on the following Cisco NCS 540 router variant: • N540-24Q8L2DD-SYS

Feature Name	Release Information	Description
PTP and SyncE Support for N540X-8Z16G-SYS-D and N540X-8Z16G-SYS-A	Release 7.3.1	Cisco N540X-8Z16G-SYS-D and N540X-8Z16G-SYS-A routers support PTP and SyncE: • Class B timing on 1 G RJ-45 ports • Class C timing on all 1G and 10 G fiber ports
PTP Profiles Support for N540X-16Z4G8Q2C-A/D	Release 7.0.1	PTP Profiles are now supported on the following Cisco NCS 540 router variant: • N540X-16Z4G8Q2C-A/D

ITU-T Telecom Profiles for PTP

Cisco IOS XR software supports ITU-T Telecom Profiles for PTP as defined in the ITU-T recommendation. A profile consists of PTP configuration options applicable only to a specific application.

Separate profiles can be defined to incorporate PTP in different scenarios based on the IEEE 1588-2008 standard. A telecom profile differs in several ways from the default behavior defined in the IEEE 1588-2008 standard and the key differences are mentioned in the subsequent sections.

The following sections describe the ITU-T Telecom Profiles that are supported for PTP.

G.8265.1

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

- Clock advertisement: G.8265.1 profile specifies changes to values used in Announce messages for advertising PTP clocks. The clock class value is used to advertise the quality level of the clock, while the other values are not used.
- Clock Selection: G.8265.1 profile also defines an alternate 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 Server or Client 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-Request/Delay-Response Packets: Rates from 128 packets-per-second to 16 seconds-per-packet.
  - Announce Packets: Rates from 8 packets-per-second to 64 packets-per-second.

- Transport Mechanism: G.8265.1 profile only supports IPv4 PTP transport mechanism.
- Mode: G.8265.1 profile supports transport of data packets only in unicast mode.
- Clock Type: G.8265.1 profile only supports Ordinary Clock-type (a clock with only one PTP port).
- Domain Numbers: The domain numbers that can be used in a G.8265.1 profile network ranges from 4 to 23. The default domain number is 4.
- Port Numbers: Multiple ports can be configured; however, all ports must be of the same type, either Server or Client.

G.8275.1

G.8275.1 profile fulfills the time-of-day and phase synchronization requirements in telecom networks with all network devices participating in the PTP protocol. G.8275.1 profile with SyncE provides better frequency stability for the time-of-day and phase synchronization.

Features of G.8275.1 profile are:

- Synchronization Model: G.8275.1 profile adopts hop-by-hop synchronization model. Each network device in the path from Server to Client clock synchronizes its local clock to upstream devices and provides synchronization to downstream devices.
- Clock Selection: G.8275.1 profile also defines an alternate BMCA that selects a clock for synchronization and port state for the local ports of all devices in the network is defined for the profile. The parameters defined as a part of the BMCA are:
  - Clock Class
  - Clock Accuracy
  - Offset Scaled Log Variance
  - Priority 2
  - Clock Identity
  - Steps Removed
  - Port Identity
  - notSlave flag
  - Local Priority
- Port State Decision: The port states are selected based on the alternate BMCA algorithm. A port is configured to a server-only port state to enforce the port to be a server for multicast transport mode.
- Packet Rates: The nominal packet rate for Announce packets is 8 packets-per-second and 16 packets-per-second for Sync/Follow-Up and Delay-Request/Delay-Response packets.
- Transport Mechanism: G.8275.1 profile only supports Ethernet PTP transport mechanism.
- Mode: G.8275.1 profile supports transport of data packets only in multicast mode. The forwarding is done based on forwardable or non-forwardable multicast MAC address.
- Clock Type: G.8275.1 profile supports the following clock types:

- Telecom Grandmaster (T-GM)
- Telecom Time subordinate/client Clock (T-TSC)
- Telecom Boundary Clock (T-BC)

- Domain Numbers: The domain numbers that can be used in a G.8275.1 profile network ranges from 24 to 43. The default domain number is 24.

The G.8275.1 supports the following:

- T-GM: The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock (PRTC).
- T-BC: The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an 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, T-BC continues to provide its own timing information to its peers, although derived clock is not as accurate as the T-GM.
- T-TSC: The telecom time subordinate/client clock (T-TSC) synchronizes its local clock to another PTP clock (in most cases, the T-BC), and does not provide synchronization through PTP to any other device.

Performance Requirements

The router is compliant with Class B performance requirements for T-TSC and T-BC as documented in G.8273.2.

G.8275.2

The G.8275.2 is a PTP profile for use in telecom networks where phase or time-of-day synchronization is required. It differs from G.8275.1 in that it is not required that each device in the network participates in the PTP protocol. Also, G.8275.2 uses PTP over IPv4 in unicast mode.

The G.8275.2 profile is based on the partial timing support from the network. Hence nodes using G.8275.2 are not required to be directly connected.

The G.8275.2 profile is used in mobile cellular systems that require accurate synchronization of time and phase. For example, the fourth generation (4G) of mobile telecommunications technology.

Table 12: Feature History Table

Feature Name	Release Information	Description
ITU-T G.8275.2 and default PTP profiles over IPv6	Release 25.1.1	The capability of using the ITU-T G.8275.2 and the default PTP profiles, with IPv6 encapsulation for packet transport is now supported on: • N540-24Q2C2DD-SYS

Feature Name	Release Information	Description
ITU-T G.8275.2 and Default PTP profiles over IPv6	Release 7.7.1	For ITU-T G.8275.2 and the IEEE 1588 default PTP profiles, the encapsulation type for PTP packet transport is now extended to IPv6. The **transport** command now accepts the keyword **ipv6**. In this release, this feature is supported on the following Cisco NCS 540 router variants: • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS • N540-28Z4C-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540-12Z20G-SYS-A/D • N540X-12Z16G-SYS-A/D

Features of G.8275.2 profile are:

- Clock Selection: G.8275.2 profile also defines an alternate BMCA that selects a clock for synchronization and port state for the local ports of all devices in the network is defined for the profile. The parameters defined as a part of the BMCA are:
  - Clock Class
  - Clock Accuracy
  - Offset Scaled Log Variance
  - Priority 2
  - Clock Identity
  - Steps Removed
  - Port Identity
  - notSlave flag
  - Local Priority

Note See ITU-T G.8275.2 document to determine the valid values for Clock Class parameter.

- Port State Decision: The port states are selected based on the alternate BMCA algorithm. A port can be configured as "server-only", "client-only", or "any" mode.
- Packet Rates:
  - Synchronization/Follow-Up—minimum is one packet-per-second and maximum of 128 packets-per-second.
  - Packet rate for Announce packets—minimum of one packet-per-second and maximum of eight packets-per-second.
  - Delay-Request/Delay-Response packets—minimum is one packet-per-second and maximum of 128 packets-per-second.
- Transport Mechanism: G.8275.2 profile supports only IPv4 PTP transport mechanism.
- Mode: G.8275.2 profile supports transport of data packets only in unicast mode.
- Clock Type: G.8275.2 profile supports the following clock types:
  - Telecom Grandmaster (T-GM): Provides timing for other network devices and does not synchronize its local clock to other network devices. However, T-GM can be connected to a GPS or GNSS for deriving better clock information.
  - Telecom Time Subordinate/Client Clock (T-TSC) and Partial-Support Telecom Time Subordinate/Client Clocks (T-TSC-P): A client clock synchronizes its local clock to another PTP clock, but does not provide PTP synchronization to any other network devices.
  - Telecom Boundary Clock (T-BC) and Partial-Support Telecom Boundary Clocks (T-BC-P): Synchronizes its local clock to a T-GM or an upstream T-BC clock and provides timing information to downstream T-BC or T-TSC clocks.
- Domain Numbers: The domain numbers that can be used in a G.8275.2 profile network ranges from 44 to 63. The default domain number is 44.

PTP Virtual Port

Feature Name	Release Information	Feature Description
PTP virtual port support for N540-24Q2C2DD-SYS	Release 25.3.1	PTP virtual port is now supported on this Cisco NCS 540 router variant: • N540-24Q2C2DD-SYS

Feature Name	Release Information	Feature Description
PTP Virtual Port Support	Release 7.7.1	PTP Virtual Port is now supported on the following Cisco NCS 540L router variants: • N540X-12Z16G-SYS-A/D • N540-12Z20G-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540X-16Z8Q2C-D • N540-24Q8L2DD-SYS • N540-28Z4C-SYS-A/D
PTP Virtual Port Support for Cisco NCS 540 routers	Release 7.4.1	You can now select the best available timing source for your routers by using the PTP Virtual Port feature. This feature allows you to compare, select, and advertise the best clock source between a PTP server and other local timing sources connected to the routers. Vitual Port is an external frequency, phase, and time input interface on a Telecom Boundary Clock (T-BC), and thus participates in the timing source selection.

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.

Limitations

- Assisted Partial Timing Support (APTS) is supported only for the G8275.2 non hybrid mode.
- Virtual port is supported for G8275.1 and G8275.2 in hybrid and non-hybrid modes.
- Virtual port configuration is not allowed under Ordinary Clocks.
- Virtual port cannot be configured if the time of day (ToD) priority is not set under the global PTP configuration mode. Use the **time-of-day priority** command to set the ToD.

Assisted Partial Timing Support

Table 13: Feature History Table

Feature Name	Release Information	Description
Assisted partial timing support	Release 25.3.1	Assisted Partial Timing Support (APTS) is supported on: • N540-24Q2C2DD-SYS
Assisted Partial Timing Support	Release 7.7.1	Assisted Partial Timing Support (APTS) enables you to select timing and synchronization for mobile backhaul networks. APTS is now available on the following routers: • N540X-12Z16G-SYS-A/D • N540-12Z20G-SYS-A/D • N540X-16Z4G8Q2C-A/D • N540X-16Z8Q2C-D • N540-24Q8L2DD-SYS • N540-28Z4C-SYS-A/D APTS allows for proper distribution of phase and time synchronization in the network.

In a network having GNSS or GPS reference, all nodes (or secondary clocks) at the edge of the network follow the GNSS primary clock that runs at the core. When GNSS or GPS reference fails at the core, the secondary clocks running at the edge no longer receive accurate time stamps from the primary clock.

With the use of APTS, the nodes at the edge of the network identify GNSS or GPS as primary clock source, and PTP as the secondary source. So even if the GNSS reference is lost, the nodes fall back to the backup PTP session running between the primary clock at core and the nodes at the edge, and are thereby able to maintain an accurate time stamp.

Configuring the G.8265.1 Profile

Configuring the Client Global Configuration: Example

Master Node

```
ptp
 clock
 domain 4
 profile g.8265.1 clock-type master
 profile master
  transport ipv4
  sync frequency 16
```

```
  announce interval 1
  delay-request frequency 16
interface gi 0/1/0/0
 ptp
  profile master
  transport ipv4
  port state master-only
  ipv4 address 18.1.1.1/24
```

Slave Node

```
ptp
clock
domain 4
profile g.8265.1 clock-type slave

profile slave
transport ipv4
sync frequency 16
announce interval 1
delay-request frequency 16
interface gi 0/1/0/0
ptp
profile slave
transport ipv4
Master ipv4 18.1.1.1
port state slave-only
ipv4 address 18.1.1.2/24
```

Configuring the G.8275.1 Profile

Note The Sync 2 port and GNSS receiver configuration listed below are not supported simultaneously for network synchronization. Choose only one synchronization method at a time.

Configuring the Global Settings: Example

```
ptp
clock
 domain 24
 profile g.8275.1 clock-type [T-BC | TGM | TTSC]
!
profile profile1
 transport ethernet
 sync frequency 16
 announce frequency 8
 delay-request frequency 16
!
 profile profile2
 transport ethernet
 sync frequency 16
 announce frequency 8
 delay-request frequency 16
 !
 !
     physical-layer-frequency
 !
```

Configuring Client Port: Example

```
interface GigabitEthernet0/0/0/3
 ptp
  profile profile1
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  port state slave-only
  local-priority 10
!
  frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
 !
!
```

Configuring Server Port: Example

```
interface GigabitEthernet0/0/0/1
 ptp
  profile profile2
  multicast target-address ethernet 01-1B-19-00-00-00
  port state master-only
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
 !
!
```

Configuring the G.8275.2 Profile

Note The Sync 2 port and GNSS receiver configuration listed below are not supported simultaneously for network synchronization. Choose only one synchronization method at a time.

Global configuration for the telecom profile for Server clock:

```
ptp
 clock
  domain 44
  profile g.8275.2 clock-type T-GM
 !
 profile master
  transport ipv4
  sync frequency 64
  announce frequency 8
  unicast-grant invalid-request deny
  delay-request frequency 64
 !
!

interface GigabitEthernet0/0/0/11
 ptp
  profile master
 !
 ipv4 address 11.11.11.1 255.255.255.0
!
```

Global configuration for the telecom profile for Client clock:

Effective Cisco IOS XR Software Release 7.7.1, the encapsulation type for PTP packet transport is now extended to IPv6; you can now use the **transport ipv6** to set this encapsulation type.

```
ptp
 clock
  domain 44
  profile g.8275.2 clock-type T-TSC
 !
 profile slave
  transport ipv4
  port state slave-only
  sync frequency 64
  announce frequency 8
  delay-request frequency 64
 !
 log
  servo events
  best-master-clock changes
 !
!
interface GigabitEthernet0/0/0/12
 ptp
  profile slave
  master ipv4 10.10.10.1
   !
 !
 ipv4 address 10.10.10.2 255.255.255.0
!
```

Global configuration with clock type as T-Boundary Clock (T-BC) for the telecom profile:

Effective Cisco IOS XR Software Release 7.7.1, the encapsulation type for PTP packet transport is now extended to IPv6; you can use the **transport ipv6** to set this encapsulation type.

```
ptp
 clock
  domain 44
  profile g.8275.2 clock-type T-BC
 !
 profile slave
  transport ipv4
  port state slave-only
  sync frequency 64
  announce frequency 8
  unicast-grant invalid-request deny
  delay-request frequency 64
 !
 profile master
  transport ipv4
  sync frequency 64
  announce frequency 8
  unicast-grant invalid-request deny
  delay-request frequency 64
 !
 log
  servo events
  best-master-clock changes
 !
!


interface GigabitEthernet0/0/0/11
```

```
 ptp
  profile master
 !
 ipv4 address 10.10.10.2 255.255.255.0
!

interface GigabitEthernet0/0/0/12
 ptp
  profile slave
  master ipv4 10.10.10.1
  !
 !
 ipv4 address 10.10.10.3 255.255.255.0
!
```

Example: Configuring G.8275.2 in Hybrid Mode

1. Configuring Sync2

```
clock-interface sync 2 location 0/RP0/CPU0
port-parameters
gps-input tod-format cisco pps-input ttl <depending on the tod format incoming :
cisco/ntp4>
!
frequency synchronization
selection input
priority 1
wait-to-restore 0
quality receive exact itu-t option 1 PRC
```

2. Configuring the T-GM with GNSS as source

Note If the server clock receives front panel inputs, skip to step b.

   a. Enabling GNSS

```
gnss-receiver 0 location 0/RP1/CPU0
no shut
constellation auto
frequency synchronization
selection input
wait-to-restore 0
quality receive exact itu-t option 1 PRC
```

Note In Cisco IOS XR Release 7.0.1, GNSS is *not* supported on N540-28Z4C-SYS-A/D and N540-12Z20G-SYS-A/D variants.

Note In Cisco IOS XR Release 7.3.1, GNSS is *not* supported on N540X-6Z18G-SYS-A/D and N540X-8Z16G-SYS-AD variants.

Note In Cisco IOS XR Release 7.4.1, GNSS is *not* supported on the N540X-4Z14G2Q-SYS-A/D variants.

b. Configuring global PTP

```
ptp
          clock
          domain 44
          profile g.8275.2 clock-type T-GM
         !
         profile 8275.2
        transport ipv4
        port state any
        sync frequency 64
        announce frequency 8
        delay-request frequency 64
         !
         physical-layer-frequency
        !
```

c. Configuring global frequency

```
frequency synchronization
        quality itu-t option 1
        clock-interface timing-mode system
        !
```

d. Enabling GPS for phase and frequency input

```
clock-interface sync 2 location 0/RP0/CPU0
         port-parameters
         gps-input tod-format ntp4 pps-input ttl baud-rate 9600
         !
         frequency synchronization
         selection input
         priority 1
         wait-to-restore 0
         quality receive exact itu-t option 1 PRC
         !
         !
```

e. Configuring PTP and SyncE output on port for T-GM

```
interface HundredGigE0/0/0/1
    ptp
    profile 8275.2
    !
    frequency synchronization
    !
```

3. Configuring G.8275.2 on T-BC

a. Configuring global SyncE

```
frequency synchronization
     quality itu-t option 1
     clock-interface timing-mode system
     !
```

b. Configuring global PTP

```
ptp
clock
```

```
domain 44
profile g.8275.2 clock-type T-BC
!
profile 8275.2
  transport ipv4
  port state any
  sync frequency 64
  announce frequency 8
  delay-request frequency 64
!
physical-layer-frequency  <-- This is a mandatory command -->
!
```

c. Configuring Client port on Hybrid BC

```
interface HundredGigE0/0/0/0
ptp
profile 8275.2
!
frequency synchronization
selection input
priority 1
wait-to-restore 0
!
!
```

d. Configuring Server port on Hybrid BC

```
interface HundredGigE0/0/0/1
ptp
profile 8275.2
!
frequency synchronization
!
!
```

4. Configuring G8275.2 on T-TSC

a. Configuring global SyncE

```
frequency synchronization
     quality itu-t option 1
     clock-interface timing-mode system
     !
```

b. Configuring global PTP

```
ptp
clock
domain 44
profile g.8275.2 clock-type T-TSC
!
profile 8275.2
  transport ipv4
  port state any
  sync frequency 64
  announce frequency 8
  delay-request frequency 64
!
physical-layer-frequency  <-- This is a mandatory command -->
!
```

c. Configuring Client port on Hybrid BC

```
interface HundredGigE0/0/0/0
ptp
profile 8275.2
!
frequency synchronization
selection input
priority 1
wait-to-restore 0
!
!
```

Example: Configuring G.8275.2 in Non-Hybrid Mode

1. Configuring Sync2

```
clock-interface sync 2 location 0/RP0/CPU0
port-parameters
gps-input tod-format cisco pps-input ttl <depending on the tod format incoming :
cisco/ntp4>
!
frequency synchronization
selection input
priority 1
wait-to-restore 0
quality receive exact itu-t option 1 PRC
```

2. Configuring the T-GM with GNSS as source

Note If the server clock receives front panel inputs, skip to step b.

   a. Enabling GNSS

```
gnss-receiver 0 location 0/RP1/CPU0
frequency synchronization
selection input
wait-to-restore 0
quality receive exact itu-t option 1 PRC
```

Note In Cisco IOS XR Release 7.0.1, GNSS is *not* supported on N540-28Z4C-SYS-A/D and N540-12Z20G-SYS-A/D variants.

Note In Cisco IOS XR Release 7.3.1, GNSS is also *not* supported on N540X-6Z18G-SYS-A/D and N540X-8Z16G-SYS-AD variants.

Note In Cisco IOS XR Release 7.4.1, GNSS is *not* supported on the N540X-4Z14G2Q-SYS-A/D variants.

b. Configuring global PTP

```
ptp
          clock
          domain 44
          profile g.8275.2 clock-type T-GM
         !
         profile 8275.2
        transport ipv4
        port state any
        sync frequency 64
        announce frequency 8
        delay-request frequency 64
         !
        !
```

c. Enabling GPS for phase and frequency input

```
clock-interface sync 2 location 0/RP0/CPU0
         port-parameters
         gps-input tod-format ntp4 pps-input ttl baud-rate 9600
         !

         selection input
         priority 1
         wait-to-restore 0
         quality receive exact itu-t option 1 PRC
         !
         !
```

d. Configuring PTP and SyncE output on port for T-GM

```
interface HundredGigE0/0/0/1
    ptp
    profile 8275.2
    !
    !
```

3. Configuring G.8275.2 on T-BC

a. Configuring global PTP

```
ptp
clock
domain 44
profile g.8275.2 clock-type T-BC
!
profile 8275.2
  transport ipv4
  port state any
  sync frequency 64
  announce frequency 8
  delay-request frequency 64
!
```

b. Configuring Client port on Hybrid BC

```
interface HundredGigE0/0/0/0
ptp
profile 8275.2
!
selection input
priority 1
wait-to-restore 0
```

```
!
!
```

c. Configuring Server port on Hybrid BC

```
interface HundredGigE0/0/0/1
ptp
profile 8275.2
!
!
```

4. Configuring G8275.2 on T-TSC

a. Configuring global PTP

```
ptp
clock
domain 44
profile g.8275.2 clock-type T-TSC
!
profile 8275.2
  transport ipv4
  port state any
  sync frequency 64
  announce frequency 8
  delay-request frequency 64
!
```

b. Configuring Client port on Hybrid BC

```
interface HundredGigE0/0/0/0
ptp
profile 8275.2
!
selection input
priority 1
wait-to-restore 0
!
!
```

Configuring Virtual Port

Effective Cisco IOS XR Release 7.4.1, you can configure virtual port on the G8275.1 and G8275.2 profiles in hybrid and non-hybrid modes.

For virtual port configuration to work, GNSS or Sync2 must be configured.

```
ptp
clock
domain 44
profile g.8275.2 clock-type T-BC
!
profile profile1
transport ipv4
sync frequency 64
announce frequency 8
delay-request frequency 64
!
virtual-port
offset-scaled-log-variance 20061
priority2 128
clock-class 6
```

```
clock-accuracy 33
local-priority 127
!
frequency priority 254
time-of-day priority 90     <<--time-of-day priority is a required parameter if you want
to configure virtual port-->>
log
```

Configuring APTS

Effective Cisco IOS XR Release 7.4.1, you can configure APTS on the G8275.2 profile in non-hybrid mode.

```
ptp
apts
clock
domain 44
profile g.8275.2 clock-type T-BC
!
profile profile1
transport ipv4
sync frequency 64
clock operation one-step
announce frequency 8
delay-request frequency 64
!
virtual-port
  offset-scaled-log-variance 20061
  priority2 128
  clock-class 6
  clock-accuracy 33
  local-priority 127
 !
 frequency priority 254
 time-of-day priority 90
 log
```

Monitor PTP virtual port using PTP timeReceiver ports

Table 14: Feature History Table

Feature Name	Release Information	Feature Description
Monitor PTP virtual port using PTP timeReceiver ports	Release 24.4.1	You can now configure a threshold value for the Time of Day (ToD) difference or offset between the PTP virtual port Global Navigation Satellite System (GNSS) and the time received by the timeReceiver ports. The timeReceiver ports receive the timing signal from remote timeTransmitters. As part of the monitoring process, the servo mechanism in the router routinely calculates the ToD offset between the GNSS receiver and the best PTP timeTransmitter. When the offset value exceeds the configured threshold, the router raises a syslog message. Based on the generated syslog message, you can determine if you should switch from the virtual port GNSS to selecting the PTP timeTransmitter as a fallback source. Command introduced: **gm-threshold-breach** *threshold_value* YANG data models: • Cisco-IOS-XR-ptp-cfg, version 3.2.0 • Cisco-IOS-XR-um-ptp-cfg, version 2.0.0 • Cisco-IOS-XR-ptp-oper, version 2.3.0 See (GitHub, Yang Data Models Navigator)

Monitor PTP virtual port using PTP timeReceiver ports

The router achieves redundancy by having a primary and secondary timing source. For example, it can receive timing signals from a primary source, such as the Global Navigation Satellite System (GNSS) receiver, and secondary sources like PTP timeTransmitters.

When configuring a PTP virtual port to receive the GNSS timing signal, the router initially considers it the optimal local timing source. To monitor the quality of the virtual port signal, the servo mechanism in the router routinely calculates the Time of Day (ToD) difference, or offset, between the GNSS and the best timeReceiver port. You can now configure a ToD offset threshold value for the PTP virtual port GNSS. Threshold refers to a predefined limit or value set for the ToD offset. The router enforces the configured threshold value upon the absolute measured offset value, without any relative adjustments or considerations. If the offset exceeds the threshold, known as a threshold breach, the router sends alarm notifications as syslog messages.

Threshold configuration

Suppose you intend to configure a threshold of 1000 ns for the virtual port that receives the GNSS signal. You must configure the command as shown in the example:

```
Router(config-ptp-vp)#gm-threshold-breach 1000
```

Threshold breach

When the offset value exceeds the configured threshold value, it is referred to as a threshold breach. If the calculated offset value is 1100 ns, it exceeds the configured threshold. Upon detecting that the virtual port has breached the threshold value, the router sends a syslog message indicating a threshold breach. You can then analyze the syslog message and determine if you should switch from the virtual port GNSS to selecting the best PTP timeTransmitter as a fallback source.

The router enforces the configured threshold value of 1000 ns on the absolute measured offset value of 1100 ns, without any relative adjustments or considerations.

Sample syslog message

The alarm notification is sent as a syslog message, and it shows that the configured threshold value is 1000 ns. However, the offset value is 1100 ns, indicating a threshold breach.

```
Time of day offset between virtual port and best foreign master clock aaaafffeaaaa00,
steps removed 1, receiving port 1, received on interface GigabitEthernet0/2/0/0 is 1100 ns,
configured threshold is 1000 ns. Raising virtual port offset alarm due to threshold breach.
```

Supported platforms

- N540-ACC-SYS
- N540X-ACC-SYS
- N540-24Z8Q2C-SYS

Alarm conditions

The list provided explains the specific state or events that raise or clear the threshold alarm.

- An alarm is raised when
  - the configured threshold is exceeded, for reasons such as changing the timeTransmitter.
  - a new threshold value that is lesser than the current offset is configured.
- An alarm is cleared when
  - the offset value drops below the configured threshold.
  - the threshold value is unconfigured.

- the virtual port is no longer the best source of timing for reasons such as configuration or clock rank change.
- all timeTransmitters are lost.

Configure threshold to monitor PTP virtual port using PTP timeReceiver ports

Use this task to configure a threshold value to monitor the PTP Virtual Port using PTP timeReceiver timing sources.

Before you begin

Configure global SyncE and GNSS before you configure the virtual port. See the Configuration Example for more information.

Procedure

Step 1 Configure PTP.

```
Router(config)#ptp
```

Step 2 Configure the PTP virtual port.

```
Router(config-ptp)#virtual-port
```

Step 3 Configure the threshold for the PTP virtual port.

```
Router(config-ptp-vp)#gm-threshold-breach 1000
```

Note
The valid range is from 0 through 4,294,967,295 ns.

Configuration example

The example shows a Time-Based Clock (T-BC) consolidated configuration with Synchronous Ethernet (SyncE), GNSS, and PTP with the threshold value.

```
T-BC (Middle Router Configurations)
Global SyncE Configuration
Router#configure terminal
Router(config)#frequency synchronization
Router(config-freqsync)#quality itu-t option 1
Router(config-freqsync)#clock-interface timing-mode system
Router(config-freqsync)#commit

Source GNSS Configuration
Router#configure terminal
Router(config)#gnss-receiver 0 location 0/rp0/cpu0
Router(config-gnss)#frequency synchronization
Router(config-gnss-freqsync)#selection input
Router(config-gnss-freqsync)#priority 20
Router(config-gnss-freqsync)#time-of-day-priority 100
```

```
Router(config-gnss-freqsync)#quality receive exact itu-t option 1 PRC
Router(config-gnss-freqsync)#commit

Virtual Port and Global PTP Configuration
Router#configure terminal
Router(config)#ptp
Router(config-ptp)#physical-layer-frequency
Router(config-ptp)#time-of-day priority 90
Router(config-ptp)#clock
Router(config-ptp-clock)#domain 24
Router(config-ptp-clock)#profile G.8275.1 clock-type T-BC
Router(config-ptp-clock)#time-source GPS
Router(config-ptp-clock)#timescale PTP
Router(config-ptp-clock)#virtual-port
Router(config-ptp-vp)#clock-accuracy 0x21
Router(config-ptp-vp)#clock-class 6
Router(config-ptp-vp)#local-priority 128
Router(config-ptp-vp)#priority2 50
Router(config-ptp-vp)#offset-scaled-log-variance 0x4e5d
Router(config-ptp-vp)#gm-threshold-breach 1000
Router(config-ptp-vp)#ptp
Router(config-ptp)#profile master
Router(config-ptp-profile)#transport ethernet
Router(config-ptp-profile)#sync frequency 16
Router(config-ptp-profile)#delay-req frequency 16
Router(config-ptp-profile)#announce frequency 8
Router(config-ptp-profile)#ptp
Router(config-ptp)#profile slave
Router(config-ptp-profile)#transport ethernet
Router(config-ptp-profile)#sync frequency 16
Router(config-ptp-profile)#delay-req frequency 16
Router(config-ptp-profile)#announce frequency 8
Router(config-ptp-profile)#commit
Interface Configuration
Router#configure terminal
Router(config)#interface HundredGigE0/0/1/1
Router(config-if)#ptp
Router(config-if-ptp)#profile slave
Router(config-if-ptp)#transport ethernet
Router(config-if-ptp)#local-priority 30
Router(config-if-ptp)#port state slave-only
Router(config-if-ptp)#multicast target-address ethernet 01-1B-19-00-00-00
Router(config-if-ptp)#frequency synchronization
Router(config-if-freqsync)#selection input
Router(config-if-freqsync)#priority 30
Router(config-if-freqsync)#wait-to-restore 0
Router(config-if-freqsync)#commit
```

Verify PTP virtual port using PTP timeReceiver ports

These commands show that the offset value is 900 ns for the virtual port. The offset value does not exceed the configured threshold value of 1000 ns. The offset value indicates no threshold breach, implying consistent timing between the GNSS receiver and the best timeReceiver port.

Before you begin

Use these show commands to verify that the offset does not exceed the configured threshold value. You can execute these commands as needed and do not have to follow a specific sequence.

Procedure

Step 1 Verify local PTP clock information.

```
RP/0/0/CPU0#show ptp local-clock
    Clock ID: ACDE48FFFE234567
    Clock properties:
       Domain: 0, Priority1: 7, Priority2: 83, Class: 7
       Accuracy: 0x2B, Offset scaled log variance: 0x27FF
       Time Source: GPS
       Timescale: PTP
       Frequency-traceable, Time-traceable
       Current UTC offset: 35 seconds
    Virtual Port:
       Configured: True, Connected: True
       Offset from PTP best foreign master: 900ns
```

If no timeTransmitters send timestamps, the show command displays:

```
Offset from PTP best foreign master: none qualified
```

Step 2 Verify the best timeReceiver clock information.

```
RP/0/0/CPU0:demo#show ptp foreign-masters best
    Used to set system frequency and time
    Ipv4, Address 1.2.3.4
    Received on interface GigabitEthernet0/2/0/3 (port number 0x1007)
    Clock ID: ACDE48FFFE234567
    Best foreign-master for 5 days, 4 hours, 27 minutes
    Advertised for 5 days, 4 hours, 20 minutes
 Offset from Virtual Port: 900ns
    Clock properties:
       Domain: 0, Priority1: 7, Priority2: 83, Class: 6
       Accuracy: 0x2B, Offset scaled log variance: 0x27FF
       Steps-removed: 5, Time Source: GPS, Timescale: PTP
```

If the virtual port is not configured or connected, the show command displays:

```
Offset from Virtual Port: not configured/not connected
```

If the servo cannot provide offset, the show command displays:

```
Offset from Virtual Port: unavailable
```

Step 3 Verify the timeReceiver clock information.

```
RP/0/0/CPU0:demo#show ptp foreign-masters
    Used to set system frequency and time
    Ipv4, Address 1.2.3.4
    Received on interface GigabitEthernet0/2/0/3 (port number 0x1007)
    Clock ID: ACDE48FFFE234567
        Advertised for 5 days, 4 hours, 20 minutes
    Offset from Virtual Port: 900ns
    Received Clock properties:
       Domain: 0, Priority1: 7, Priority2: 83, Class: 6
       Accuracy: 0x2B, Offset scaled log variance: 0x27FF
       Steps-removed: 5, Time Source: GPS, Timescale: PTP
```

If the virtual port is not configured or connected, the show command displays:

```
Offset from Virtual Port: not configured/not connected
```

If the servo cannot provide offset, the show command displays:

```
Offset from Virtual Port: unavailable
```

Step 4 Verify the generated syslog.

```
Router#show logging
Router:Sep 21 06:42:39.995 UTC: ptp_ctrlr[1081]: %L2-PTP-4-VIRTUAL_PORT_OFFSET_EXCEEDED :
Time of day offset between virtual port
and best foreign master clock aaaafffeaaaa00, steps removed 1, receiving port 1,
received on interface GigabitEthernet0/2/0/0 is 1100 ns,
configured threshold is 1000 ns. Raising virtual port offset alarm due to threshold breach.
```

Restriction to monitor PTP virtual port using PTP timeReceiver ports

The main restriction to consider while enforcing the threshold:

- The threshold is only enforced on the best timeReceiver, even when the offset is reported for multiple timeReceivers.

Slow Tracking

Under normal configured conditions, any change in offset triggers an immediate reaction in the servo. With the Slow Tracking feature enabled, the servo corrects the phase offset based on the configured value. If the phase offset exceeds the acceptable range, servo goes into Holdover state. In such a condition, the Slow Tracking feature becomes inactive and the servo corrects itself to the latest offset and goes into Phase locked state. Slow Tracking becomes active again.



Note

- The supported slow tracking rate range is from 8-894 nanoseconds per second and must be in multiples of 8.
- This feature is active only when servo is in Phase locked mode.

```
Router:# config
ptp
clock
domain 24
profile g.8275.1 clock-type T-BC
!
profile profile1
multicast target-address ethernet 01-1B-19-00-00-00
transport ethernet
sync frequency 16
announce frequency 8
delay-request frequency 16
!
physical-layer-frequency
servo-slow-tracking 16
!
```

PTP Holdover Traceability Suppression

Table 15: Feature History Table

Feature Name	Release Information	Feature Description
PTP frequency-assisted holdover	Release 26.3.1	The frequency-assisted holdover feature enhances network stability by allowing for an extended holdover duration when a Primary Reference Clock (PRC) frequency source remains available. This ensures that even if the GNSS or PTP time source is lost, the system can maintain timing stability for a longer, user-defined period without significant degradation. CLI: • holdover-spec-frequency-assisted-duration
PTP Holdover Traceability Suppression	Release 7.4.1	When a device which is configured as a Boundary clock (T-BC) loses synchronization with a quality Primary clock, to ensure that the downstream nodes continue to receive the configured clock class for a specified duration, and it's traceable you can configure this feature.
PTP Holdover Traceability Suppression for T-GM and T-GM with VP/APTS modes	Release 7.8.1	This feature extends the PTP holdover traceability suppression functionality to the devices which are in T-GM or T-GM with VP/APTS modes.

When the device loses synchronization with a quality Primary clock, to ensure that the downstream nodes continue to receive the configured clock class, and it's traceable you can configure this feature.

This feature enables the device which is configured as a boundary clock (T-BC) with PTP Profiles G.8275.1 or G.8275.2 to send out the configured clock-class as holdover clock-class and the time traceability flag to be set as TRUE for the specified duration. This is to ensure the down-stream nodes do not have an impact as this is a deviation from prescribed G.8275.1 ITU-T standards.

The Cisco IOS XR Software Release 7.8.1 introduces the holdover traceability suppression functionality to the devices which are in T-GM or T-GM with VP/APTS modes. Prior to this release, this feature was supported on T-BC mode only.

Note

- There are PTP flaps during switchovers or ISSU as the PTP holdover timer is running on the active RSP.
- Once the configured holdover override duration has lapsed and the device is unable to receive a quality Primary clock within this duration, the device sends the prescribed default clock class of 165, and the traceability flag will be set as FALSE to advertise loss of clock to downstream nodes.

Configuring PTP Holdover traceability suppression

This section describes how to configure the PTP holdover traceability suppression feature:

```
Router# config
Router(config)# ptp
Router(config-ptp)# holdover-spec-duration 1000
Router(config-ptp)# holdover-spec-clock-class 135
Router(config-ptp)# uncalibrated-traceable-override
Router(config-ptp)# holdover-spec-traceable-override
Router(config-ptp)# holdover-spec-frequency assisted-duration 410000
```

IEEE Default Profile

The IEEE default profile is a PTP configuration profile that

- defines the parameters for time-of-day distribution using the Precision Time Protocol (PTP) in accordance with IEEE 1588-2008 and IEEE 1588-2019 standards,
- supports Delay Request-Response mechanisms on Cisco IOS XR Release 24.1.1 or later, and
- enables both ordinary clock and boundary clock operation, allowing flexible roles for routers in hybrid synchronization networks.

The IEEE default PTP profile prescribes a domain number value of 0, or within a range of 4–127. You may configure PTP on multiple router ports, with best clock selection governed by the Best Master Clock Algorithm (BMCA). If no superior clocks are detected, the router assumes the role of grandmaster clock and synchronizes all connected devices. Alternatively, if a clock connected to the router is determined to be superior, the router acts as a client for synchronization, then serves as a clock source for other devices. After synchronizing initial time, routers and devices exchange timing messages to correct clock offsets and network delays.

This PTP profile is typically deployed in hybrid mode—PTP carries time-of-day information, while frequency synchronization is provided by physical-layer sources such as SyncE. The default profile supports IPv4 unicast negotiation and, on compatible platforms, IPv6. Ethernet and multicast transports are not supported.

Example: Global PTP Configuration

Global PTP Configuration:

```
ptp
 clock
  domain 0
 !
 profile ptp_node
  transport ipv4
```

```
  sync frequency 32
  announce frequency 1
  delay-request frequency 32
 !
 physical-layer-frequency
!
```

Example: PTP Master Configuration

PTP Master Configuration:

```
interface TenGigE0/0/0/19
 ptp
  profile ptp_node
  !
 !
frequency synchronization
  wait-to-restore 0
 !
 ipv4 address 192.0.2.0/24
!
```

Example:PTP Slave Configuration

PTP Slave Configuration:

```
interface TenGigE0/0/0/18
 ptp
  profile ptp_node
 master ipv4 192.0.2.0/24
  !
frequency synchronization
  selection input
  wait-to-restore 0
 !
 !
 ipv4 address 192.0.2.0/24
!
```

PTP Hybrid Mode

Your router allows the ability to select separate sources for frequency and time-of-day (ToD). Frequency selection can be between any source of frequency available to the router, such as: GPS, SyncE or IEEE 1588 PTP. The ToD selection is between the source selected for frequency and PTP, if available (ToD selection is from GPS or PTP). This is known as hybrid mode, where a physical frequency source (SyncE) is used to provide frequency synchronization, while PTP is used to provide ToD synchronization.

Frequency selection uses the algorithm described in ITU-T recommendation G.781, and is described in the Configuring Frequency Synchronization module in this document. The ToD selection is controlled using the time-of-day priority configuration. This configuration is found under the source interface frequency synchronization configuration mode and under the global PTP configuration mode. It controls the order for which sources are selected for ToD. Values in the range of 1 to 254 are allowed, with lower numbers.

Configuring PTP Hybrid Mode

Note You must configure the PTP hybrid mode when using the G.8275.1 PTP profile.

Configure hybrid mode by selecting PTP for the time-of-day (ToD) and another source for the frequency. This task summaries the hybrid configuration. See the other PTP configuration modules for more detailed information regarding the PTP configurations. For more information on SyncE configurations, see the *Configuring Ethernet Interfaces* section in the *Interface and Hardware Component Configuration Guide for Cisco NCS 540 Series Routers*.

Note Configure appropriate clock priorities when using synchronous Ethernet for frequency synchronization. This ensures the system selects the frequency source from the same interface as the PTP source. Aligning both frequency and time synchronization to the same interface helps maintain consistency and reduces configuration complexity.

To configure PTP Hybrid mode:

1. Configure Global Frequency Synchronization

```
RP/0/RP0/CPU0:router(config)# frequency synchronization
    RP/0/RP0/CPU0:router(config)# commit
    RP/0/RP0/CPU0:router(config)# quality itu-t option [1 | 2]
```

2. Configure Frequency Synchronization in Interface.

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0
RP/0/RP0/CPU0:router(config-if)# frequency synchronization
RP/0/RP0/CPU0:router(config-if-freqsync)# selection input
RP/0/RP0/CPU0:router(config-if-freqsync)# time-of-day-priority 100
RP/0/RP0/CPU0:router(config-if-freqsync)# commit
```

3. Configure Global PTP

```
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config-ptp)# time-of-day priority 1
RP/0/RP0/CPU0:router(config)# commit
```

4. Configure Client Port

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ptp
RP/0/RP0/CPU0:router(config-if)# profile slave
RP/0/RP0/CPU0:router(config-if)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config-if)# transport ethernet sync frequency 16
RP/0/RP0/CPU0:router(config-if)# announce frequency 8
RP/0/RP0/CPU0:router(config-if)# delay-request frequency 16
RP/0/RP0/CPU0:router(config-if)# frequency synchronization
RP/0/RP0/CPU0:router(config-if-freqsync)# selection input
RP/0/RP0/CPU0:router(config-if-freqsync)# priority 1
RP/0/RP0/CPU0:router(config-if-freqsync)# wait-to-restore 0
```

5. Configure Server Port

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/0/0/3
RP/0/RP0/CPU0:router(config)# ptp
RP/0/RP0/CPU0:router(config)# profile master
```

```
RP/0/RP0/CPU0:router(config)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config)# port state master-only
RP/0/RP0/CPU0:router(config)# transport ethernet
RP/0/RP0/CPU0:router(config)# sync frequency 16
RP/0/RP0/CPU0:router(config)# announce frequency 8
RP/0/RP0/CPU0:router(config)# delay-request frequency 16
RP/0/RP0/CPU0:router(config)# frequency synchronization
RP/0/RP0/CPU0:router(config-if-freqsync)# exit
```

Configure PTP for SyncE and PTP Traceability

In the hybrid mode of operation, if the SyncE and PTP clocks are coming from separate nodes and are not traceable to each other, and if the offset between the clocks is high, then the PTP-receiver may fail to synchronize with the PTP-transmitter node.

Starting with Cisco IOS XR Release 24.4.1, a new command, **synchronous-ethernet prefer-interface ptp-receiver**is introduced in the global frequency-synchronisation mode to ensure traceability between the PTP and SyncE clocks.

If you configure this CLI, note these points:

- A SyncE source among *equal sources* [1] is selected on the same interface on which PTP is selected by the router.
- If the SyncE source on the PTP receiver interface is inferior (in terms of QL and user configured priority) than any other available SyncE source, then the SyncE source is selected using the default criteria (based on the ITU-T G.781 requirements).
- In the event that the selected PTP source goes down or if the PTP source's quality degrades, the system may switch to another PTP source. In such case, use the **synchronous-ethernet prefer-interface ptp-receiver** command so that the SyncE source selection would also switch to the new PTP receiver interface. Here, the preferred switching of SyncE source to the new PTP receiver interface shall happen only if the new interface uses the same SyncE QL and the user configured priority as the previously selected interface.



Note The router can monitor only limited number of interfaces for SyncE selection. The **synchronous-ethernet prefer-interface ptp-receiver** command selects a SyncE source from the PTP receiver interface only if the interface is part of the list displayed using the **show frequency synchronization selection** command.

This example shows how to configure the **synchronous-ethernet prefer-interface ptp-receiver** command.

```
RP/0/RP0/CPU0:router(config)# frequency synchronization synchronous-ethernet prefer-interface
 ptp-receiver
RP/0/RP0/CPU0:router(config)# commit
```

This example verifies the **synchronous-ethernet prefer-interface ptp-receiver** configuration.

```
RP/0/RP0/CPU0:router(config)# show running-config frequency synchronization
Thu Aug 8 04:50:13.638 UTC
frequency-synchronization
 synchronous-ethernet prefer-interface ptp-receiver
!
```

[1] sources equal in their advertised QL and user configured priority

Verifying the PTP Hybrid Mode Configurations

Use the following show commands to verify the configurations:

- **show ptp platform servo**

```
RP/0/RP0/CPU0:ios# show ptp platform servo
Tue Mar  5 07:08:00.134 UTC
Servo status: Running
Servo stat_index: 2
Device status: PHASE_LOCKED
Servo Mode: Hybrid
Servo log level: 0
Phase Alignment Accuracy: 0 ns
Sync timestamp updated: 8631
Sync timestamp discarded: 0
Delay timestamp updated: 8631
Delay timestamp discarded: 0
Previous Received Timestamp T1: 22521.011765183  T2: 22521.011766745  T3: 22521.018061685
  T4: 22521.018063247
Last Received Timestamp T1: 22521.073747183  T2: 22521.073748745  T3: 22521.080054957
 T4: 22521.080056515
Offset from master:  0 secs, 2 nsecs
Mean path delay   :  0 secs, 1560 nsecs
setTime():1  stepTime():1 adjustFreq():0
Last setTime: 21984.000000000 flag:0  Last stepTime:-276573300 Last adjustFreq:0
RP/0/RP1/CPU0:ios#
```

- **show running-config ptp**

```
RP/0/RP0/CPU0:router# show running-config ptp
ptp
clock
domain 24
profile g.8275.1 clock-type T-BC
!
profile slave
transport ethernet
sync frequency 16
announce frequency 8
delay-request frequency 16
!
profile master
transport ethernet
sync frequency 16
announce frequency 8
delay-request frequency 16
!
!
physical-layer frequency
!
```

- **show running-config frequency synchronization**

```
RP/0/RP0/CPU0:router# show running-config frequency synchronization
Tue Feb 6 06:36:26.472 UTC
frequency synchronization
quality itu-t option 1
clock-interface timing-mode system
!
```

- **show frequency synchronization interface brief**

```
RP/0/RP0/CPU0:P3# show frequency synchronization interface brief

Tue Feb 6 06:37:49.234 UTC
Flags: > - Up D - Down S - Assigned for selection
d - SSM Disabled x - Peer timed out i - Init state
s - Output squelched
Fl Interface QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
>S GigabitEthernet0/0/0/2 PRC PRC 1 DNU GigabitEthernet0/0/0/2
>x GigabitEthernet0/0/0/3 Fail n/a 100 PRC GigabitEthernet0/0/0/2
>x GigabitEthernet0/0/0/4 Fail n/a 100 PRC GigabitEthernet0/0/0/2
RP/0/RP0/CPU0:P3#
```

Performance Monitoring for PTP Networks

Table 16: Feature History Table

Feature Name	Release Information	Feature Description
Performance Monitoring	Release 24.3.1	You can now get statistical information with Performance Monitoring in PTP networks, such as clock accuracy, synchronization status, and network delays by defining Performance Monitoring Parameters and Port Specific Parameters. This feature empowers operators with comprehensive performance monitoring and precise time-stamp analysis, offering enhanced granularity for time synchronization in telecommunication networks. By providing detailed insights, it enables operators to make well-informed decisions and take proactive actions to ensure optimal network performance. The feature introduces these changes: **CLI:** **YANG Data Models:** • `Cisco-IOS-XR-ptp-cfg.yang` • `Cisco-IOS-XR-ptp-oper.yang` • `Cisco-IOS-XR-um-ptp-cfg.yang` (see GitHub, YANG Data Models Navigator)

Performance Monitoring in PTP involves tracking and analyzing the performance of PTP networks to ensure accurate time synchronization across devices. This includes monitoring various metrics such as clock accuracy, synchronization status, and network delays. The goal is to identify and address any issues that may affect the precision and reliability of time synchronization in the network.

Performance Monitoring now has the ability to provide performance monitoring and time-stamp analysis information in a PTP network as per Annex J IEEE 1588-2019. This feature also includes additional monitoring

granularity for time synchronization in telecommunication networks as per Annex F from the G8275 standard. For more information on PTP, Best TimeTransmitter Clock Algorithm (BTCA), see PTP Overview.

You can use the following parameters to define the Performance Monitoring in a PTP Network:

- Performance Monitoring Parameters
- Port Specific Parameters

Performance Monitoring Parameters

In addition to using the timestamps received from the grandmaster to sync to the grandmaster's clock, the timestamps can now be used to calculate parameters that are of your interest in performance monitoring:

- **TimeTransmitter - TimeReceiver Delay**: corrected propagation time from TimeTransmitter to TimeReceiver.
- **TimeReceiver - TimeTransmitter Delay**: corrected propagation time from TimeReceiver to TimeTransmitter.
- **Mean Path Delay**: mean propagation time over the PTP Communication Path.
- **Offset from TimeTransmitter**: time difference between a TimeTransmitter PTP instance and a TimeReceiver PTP instance as computed by the TimeReceiver PTP instance.

For each of these parameters, you can measure the average, minimum, maximum, and standard deviation for each measurement. These values are calculated and maintained for the following time intervals over the specified time periods:

- **3-minute**: maintained for the current 1-hour period.
- **15-minute**: maintained for the current 24-hour period.
- **1-hour**: maintained for the current 2-hour period.
- **24-hour**: maintained for the current 48-hour period.

The platform actively calculates the end-to-end latency between the TimeTransmitter and TimeReceiver through the Delay-Request-Response-Mechanism (DRRM), allowing Precision Time Protocol (PTP) to seamlessly operate across networks equipped with Transparent clocks, non-PTP aware switches, or a mix of both. Upon a request, PTP dynamically extracts these calculated values from the servo using a platform specific API, allowing you to make proactive changes to the network to ensure precise time synchronization essential for applications that depend on accurate timing.

Additional Port Specific Parameters

The parameters mentioned above apply to the entire Precision Time Protocol (PTP) instance, and there is an additional set of parameters specific to individual ports. These parameters include the counters for various packet types,

- received (rx) and
- transmitted (tx)

It is important to collect and maintain these counters for performance monitoring purposes, which follows the same time intervals and periods as those used for monitoring clock performance.

Port-specific parameters play a crucial role in ensuring accurate time synchronization. These packet types are essential for maintaining the accuracy and reliability of time synchronization in a PTP network:

- **Sync Packets**: These packets are sent by the master clock to the slave clocks to synchronize their time. They contain the precise time at which the packet was sent.
- **Delay Request Packets**: Sent by the slave clock to the master clock, these packets measure the delay between the master and slave clocks. The master clock responds with a Delay Response packet.
- **Follow-Up Packets**: These packets are sent by the master clock immediately after the Sync packet. They contain the exact time the Sync packet was sent, which helps in correcting any delays introduced by the network.
- **Announce Packets**: These packets are used by the master clock to announce its presence and capabilities to the slave clocks. They help in the selection of the best master clock in the network.
- **Management Packets**: These packets are used for configuration and management purposes within the PTP network. They allow for the adjustment of various parameters and settings.

Record format

Record format refers to the structure or layout of data within a record, which is used to store information about time synchronization events and measurements. This format can include various fields such as timestamps, event types, and other relevant data that PTP uses to maintain accurate time synchronization across a network. It is a single buffer for both annexes.

The format is the same for both clock and port performance monitoring parameters that is presented in the operational data. The data is stored over a 48-hour period, resulting in a list of records as per Annex J 1588-2019, composed of the following:

- 1 record for the current 15-minute set of statistics (stored at position 0 in the buffer).
- 96 records for the 15-minute sets of statistics over the last 24-hour period (stored between positions 1-96 in the buffer).
- 1 record for the current 24-hour set of statistics (stored at position 97 in the buffer).
- 1 record for the previous 24-hour set of statistics (stored at position 98 in the buffer).

The data buffer records data at 3-minute intervals over the most recent 1-hour period, creating a list of records that includes:

- 1 record for the current 3-minute set of statistics (stored at position 100 in the buffer).
- 20 records for the 3-minute set of statistics over the last 1-hour period (stored between positions 101-120).
- 1 record for the current 1-hour set of statistics (stored at position 121 in the buffer).
- 1 record for the previous 1-hour set of statistics (stored at position 122 in the buffer).

Configure PTP Performance Monitoring

The purpose of this task is to configure and verify PTP performance monitoring.

Procedure

Step 1 Configure the **performance-monitoring** command to enable collection of performance monitoring statistics and for the users to make performance monitoring requests.

Example:

```
Router(config)# ptp
Router(config-ptp)# performance-monitoring
Router(config-ptp)# commit
```

Step 2 Verify that PTP performance monitoring is enabled.

Example:

```
Router# show running-config ptp
```

Step 3 Run the **sh ptp platform performance-counters** command to display the details of all 123 records.

The existing command **show ptp platform** is extended to include the performance monitoring data for the local clock. The detail mode of the command displays all 123 records while the brief mode displays only the current windows for 15 minutes, 24 hours, 3minutes, and 1hour.

Example:

```
Router#sh ptp platform performance-counters detail

PTP Current record index 15 min: 96
PTP Current record index 3 min: 119

PTP performance monitoring statistics:
================================================================================
15 min stats
[0]     12 August 2024 07:08:59 UTC 15 min statistics
--------------------------------------------------------------------------------

                Stat    Min(sec.nsec)        Max(sec.nsec)       Mean(sec.nsec)     Std
deviation           Samples
--------------------------------------------------------------------------------

  Master-slave-delay -000000000.15937      000000000.333       -000000000.1780
000000000.71191      154
  Slave-master-delay  000000000.319        000000000.16593      000000000.2437
000000000.74103      154
     mean-path-delay  000000000.322        000000000.334        000000000.327
000000000.4057       154
  offset-from-master -000000000.16263      000000000.6         -000000000.2108
000000000.72546      154

--------------------------------------------------------------------------------

            Complete      Valid      PmRef      ServoAtStart     ServoAtEnd
LastServoFlapTime
--------------------------------------------------------------------------------

              FALSE      FALSE       TRUE        PHASE_LOCKED   HOLDOVER              12
 Apr 2024 07:09:09 UTC
```

```
==============

….
```

Step 4 Run the **show ptp dataset performance clock** command to display the performance monitoring data-set details in 15 minutes intervals.

Example:

```
Router#show ptp dataset performance clock

performanceMonitoringDS for the current 15-minute window:
Clock ID ccccfffecccc00, steps removed 1, receiving-port 2:
    Start of time window: Thursday, April 11, 2024 14:18:59
    Measurement is valid
    Period is complete
    Measurement has been taken with reference to system clock
    Master slave delay:
        Average: 50ns
        Min: 50ns
        Max: 70ns
        Std: 1ns
    Slave master delay:
        Average: 51ns
        Min: 51ns
        Max: 71ns
        Std: 2ns
    Mean path delay:
        Average: 52ns
        Min: 52ns
        Max: 72ns
        Std: 3ns
    Offset from master:
        Average: 53ns
        Min: 53ns
        Max: 73ns
        Std: 4ns

Clock ID aaaabbbecccc00, steps removed 1, receiving-port 2:
    Start of time window: Thursday, April 11, 2024 14:18:59
    Measurement is not valid
    Period is not complete
    Measurement has been taken with reference to system clock
    Master slave delay:
        Average: 50ns
        Min: 50ns
        Max: 70ns
        Std: 1ns
    Slave master delay:
        Average: 51ns
        Min: 51ns
        Max: 71ns
        Std: 2ns
    Mean path delay:
        Average: 52ns
        Min: 52ns
        Max: 72ns
        Std: 3ns
    Offset from master:
        Average: 53ns
        Min: 53ns
        Max: 73ns
        Std: 4ns
```

Step 5 Run the **show ptp dataset performance port** to display the Performance Monitoring Port Data-set in 15 minutes intervals.

Example:

```
Router#show ptp dataset performance port GigabitEthernet 0/0/0/1

performanceMonitoringPortDS for the current 15-minute window:
Interface GigabitEthernet 0/0/0/1
    Start of time window: Thursday, April 11, 2024 14:18:59
    Measurement is valid
    Period is not complete
    Measurement has been taken with reference to system clock
    Packets                      Sent        Received         Dropped
    ------------------------------------------------------------------
    Announce                        3              83              11
    Sync                            0              32               5
    Follow-Up                       0              31               0
    Delay-Req                      22               0               0
    Delay-Resp                      0              21               7
    Pdelay-Req                      0               7               0
    Pdelay-Resp                     0               0               0
    Pdelay-Resp-Follow-Up           0               0               0
    Signaling                       2               1               0
    Management                      0               0               0
    Other                           0               3              12
                                 -----           -----           -----
    TOTAL                          27             178              35
```

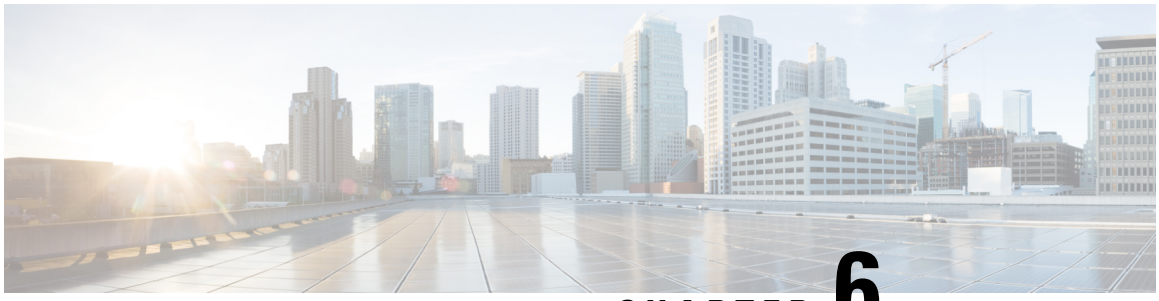
What to do next

To disable PTP performance monitoring, remove the global configuration and commit the change:

```
Router# configure
Router(config)# ptp
Router(config-ptp)# no performance-monitoring
Router(config-ptp)# commit
```

To verify the removal:

```
Router# show running-config ptp
```



CHAPTER 6

External Timing Source

Clock interfaces are external connectors for connecting other timing signals, such as, GPS, BITS.

- GPS, on page 93
- Building Integrated Timing Supply (BITS), on page 95

GPS

The router can receive 1PPS, 10 MHz, and ToD signals from an external clocking and timing source. The three inputs are combined as a Sync-2 interface to form the external timing source or the GPS input.

The GPS front panel connector details are:

- ToD—RS422 format as input
- 1PPS—1.0/2.3 DIN connector as input
- 10MHz—1.0/2.3 DIN connector as input

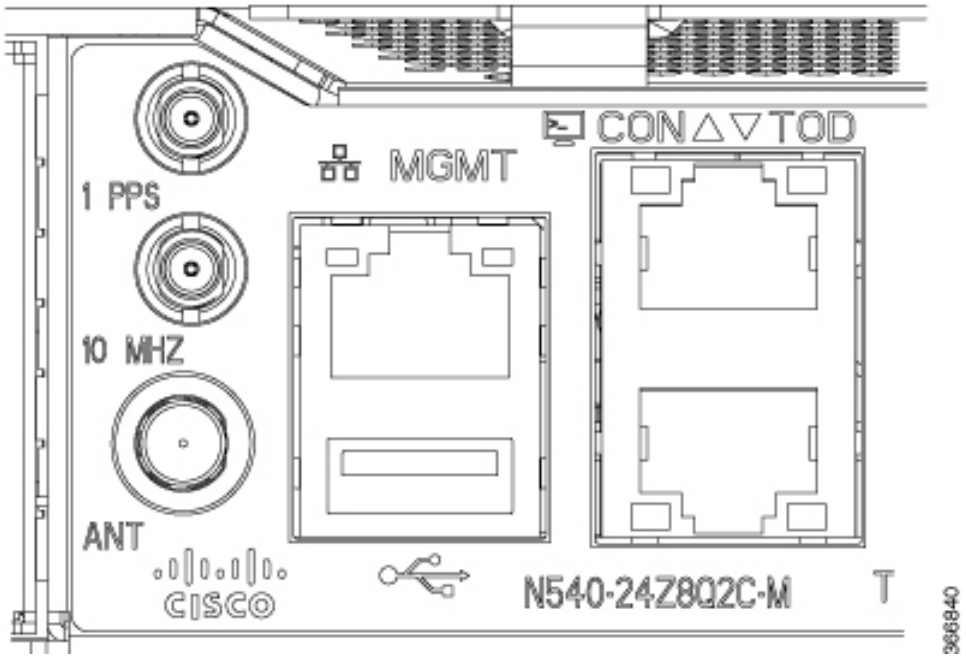
GPS input starts only when all the three signals – 1PPS, 10MHz, and ToD are UP.

Note Unlike the Ethernet interface, the Sync-2 interface cannot receive or transmit QL. Ensure that you assign a QL value to the Sync-2 interface.

By default, 1PPS and 10MHz are in output mode. ToD output mode is not configurable.

For these variants - N540-24Z8Q2C-SYS, N540X-ACC-SYS, N540-ACC-SYS, N540-28Z4C-SYS, 10MHZ and 1PPS can operate in output mode only when PTP Client or BC mode are configured.

Figure 4: 1PPS, 10MHz, and the ToD ports on the Router's Front Panel



Configuring GPS Settings for the Grandmaster Clock

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# clock-interface sync 2 location 0/RP0/CPU0
RP/0/RP0/CPU0:router(config-clock-if)# port-parameters
RP/0/RP0/CPU0:router(config-clk-parms)# gps-input tod-format cisco pps-input ttl
RP/0/RP0/CPU0:router(config-clk-parms)# exit
RP/0/RP0/CPU0:router(config-clock-if)# frequency synchronization
RP/0/RP0/CPU0:router(config-clk-freqsync)# selection input
RP/0/RP0/CPU0:router(config-clk-freqsync)# wait-to-restore 0
RP/0/RP0/CPU0:router(config-clk-freqsync)# quality receive exact itu-t option 1 PRC
RP/0/RP0/CPU0:router(config-clk-freqsync)# exit
RP/0/RP0/CPU0:router(config-clock-if)# frequency synchronization
RP/0/RP0/CPU0:router(config-clk-freqsync)# quality itu-t option 1
RP/0/RP0/CPU0:router(config-clk-freqsync)# clock-interface timing-mode system
RP/0/RP0/CPU0:router(config-clk-freqsync)# end
or
RP/0/RP0/CPU0:router(config-clk-freqsync)# commit
```

Verifying the GPS Input

```
RP/0/RP0/CPU0:R1# show controllers timing controller clock

SYNCC Clock-Setting: -1 -1 6 -1
  Port 0  Port 1  Port 2  Port 3
Config :      No      No      Yes     No
Mode :  -       -       GPS     -
Submode1 :    -       -       CISCO   -
Submode2 :    -       -       UTC     -
Submode3 :    0       0       0       0
Shutdown :    0       0       0       0
Direction :   RX/TX   RX/TX   RX      RX/TX
```

```
Baud-Rate :   -       -       9600    -
QL Option :   O1      O1      -       -
RX_ssm(raw):  -       -       -       -
TX_ssm :      -       -       -       -
If_state :    DOWN    DOWN    UP      DOWN  << Port 2 is UP when GPS input is
valid.

RP/0/RP0/CPU0:R1#
```

When the front panel timing LED is Green, it indicates that the GPS is configured and 1PPS, ToD, and 10M inputs are valid.

Timing LED Behavior:

- Timing LED is off: Indicates that no GPS is configured or the GPS port is down.
- Timing LED is green: Indicates that the GPS port is up.

SYNC LED Behavior:

- SYNC LED is applicable: Only when the timing configuration is applied.
- SYNC LED is green: Indicates that SyncE is locked.
- SYNC LED is amber: Indicates a holdover or free-running state.
- SYNC LED is off: Indicates that the configuration is removed.

Building Integrated Timing Supply (BITS)

Router supports receiving (Rx) and transmitting (Tx) of frequency via BITS interface. To receive and transmit BITS signals, configuration is done under the clock-interface sync 0 on the route processor (RP).

Prerequisite for BITS

Frequency synchronization must be configured with the required quality level option at the global level.

```
RP/0/RP0/CPU0:ios#show running-config frequency synchronization
Wed Aug 21 12:37:32.524 UTC
frequency synchronization
 quality itu-t option 1
!
```

Note BITS-In and BITS-Out on the peer nodes must be configured with the same mode and format.

Configuring BITS-IN

```
RP/0/RP0/CPU0:ios#configure
Wed Aug 21 12:29:59.162 UTC
RP/0/RP0/CPU0:ios(config)#clock-interface sync 0 location 0/RP0/CPU0
RP/0/RP0/CPU0:ios(config-clock-if)#port-parameters
RP/0/RP0/CPU0:ios(config-clk-parms)#bits-input e1 crc-4 sa4 ami
RP/0/RP0/CPU0:ios(config-clk-parms)#exit
```

```
RP/0/RP0/CPU0:ios(config-clock-if)#frequency synchronization
RP/0/RP0/CPU0:ios(config-clk-freqsync)#selection input
RP/0/RP0/CPU0:ios(config-clk-freqsync)#wait-to-restore 0
RP/0/RP0/CPU0:ios(config-clk-freqsync)#priority 1
RP/0/RP0/CPU0:ios(config-clk-freqsync)#commit
Wed Aug 21 12:30:53.296 UTC

RP/0/RP0/CPU0:ios#show running-config clock-interface sync 0 location 0/RP0/CPU0
Wed Aug 21 12:31:43.350 UTC
clock-interface sync 0 location 0/RP0/CPU0
 port-parameters
  bits-input e1 crc-4 sa4 ami
 !
 frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
 !
!
```

Configuring BITS-OUT

```
RP/0/RP0/CPU0:ios#configure
Wed Aug 21 12:53:24.189 UTC
RP/0/RP0/CPU0:ios(config)#clock-interface sync 0 location 0/RP0/CPU0
RP/0/RP0/CPU0:ios(config-clock-if)#port-parameters
RP/0/RP0/CPU0:ios(config-clk-parms)#bits-output e1 crc-4 sa4 ami
RP/0/RP0/CPU0:ios(config-clk-parms)#commit
Wed Aug 21 12:53:39.411 UTC

RP/0/RP0/CPU0:ios#show running-config clock-interface sync 0 location 0/RP0/CPU0
Wed Aug 21 12:54:02.853 UTC
clock-interface sync 0 location 0/RP0/CPU0
 port-parameters
  bits-output e1 crc-4 sa4 ami
 !
!
```

Note Based on the quality level chosen in global configuration, E1/T1 modes can be changed as required. But in all the cases, both TX and RX side modes and submodes must be the same.

For non-CRC-4/D4 modes, SSM is not present in BITS and manual receive quality level must be configured.

Verifying BITS-IN Configuration

```
RP/0/RP0/CPU0:ios#show controllers timing controller clock
Wed Aug 21 12:38:20.394 UTC

SYNCC Clock-Setting: 1 -1 -1 -1

          Port 0          Port 1          Port 2          Port 3
Config     : Yes            No              No              No
Mode       : E1             -               -               -
Submode1   : CRC-4          -               -               -
Submode2   : AMI            -               -               -
Submode3   : 0              0               0               0
Shutdown   : 0              0               0               0
```

```
Direction  : RX             RX/TX          RX/TX          RX/TX
Baud-Rate  : -              -              -              -
QL Option  : O1             O1             -              -
RX_ssm(raw): 99             -              -              -
TX_ssm     : -              -              -              -
If_state   : UP           DOWN           DOWN           DOWN
```

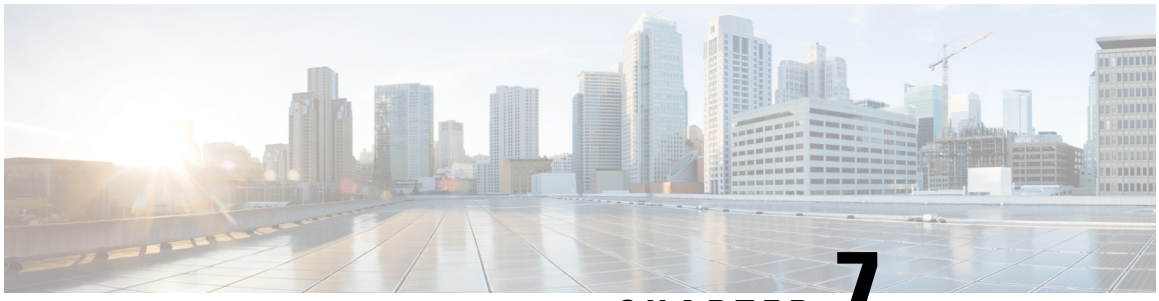
Verifying BITS-OUT Configuration

```
RP/0/RP0/CPU0:ios#show controllers timing controller clock
Wed Aug 21 12:49:32.923 UTC
SYNCC Clock-Setting: 1 -1 -1 -1

          Port 0          Port 1          Port 2          Port 3
Config     : Yes            No              No              No
Mode       : E1             -               -               -
Submode1   : CRC-4          -               -               -
Submode2   : AMI            -               -               -
Submode3   : 0              0               0               0
Shutdown   : 0              0               0               0
Direction  : TX             RX/TX           RX/TX           RX/TX
Baud-Rate  : -              -               -               -
QL Option  : O1             O1              -               -
RX_ssm(raw): -              -               -               -
TX_ssm     : 22             -               -               -
If_state   : UP             DOWN            DOWN            DOWN
```

Verify Quality Level Received and Clock Interfaces

```
RP/0/RP0/CPU0:ios#show frequency synchronization clock-interfaces brief
Sat Mar 16 07:35:08.351 UTC
Flags:  > - Up               D - Down              S - Assigned for selection
        d - SSM Disabled     s - Output squelched  L - Looped back
Node 0/RP0/CPU0:
==============
  Fl    Clock Interface     QLrcv  QLuse  Pri QLsnd  Output driven by
  ===== ================== ====== ====== === ====== ========================
  >S    Sync0               PRS    PRS      5 n/a    n/a
  D     Sync1               n/a    n/a    n/a n/a    n/a
  D     Sync2               n/a    n/a    n/a n/a    n/a
  >S    Internal0           n/a    ST3    255 n/a    n/a
```



CHAPTER 7

Implementing NTP

Network Time Protocol (NTP) is a protocol designed to time-synchronize devices within a network. Cisco IOS XR software implements NTPv4. NTPv4 retains backwards compatibility with the older versions of NTP, including NTPv3 and NTPv2 but excluding NTPv1, which has been discontinued due to security vulnerabilities.

- Information About Implementing NTP, on page 99
- Best Practices for NTP configuration , on page 100
- Configuring NTP, on page 101

Information About Implementing NTP

NTP synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur.

NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communication uses Coordinated Universal Time (UTC). An NTP network usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP distributes this time across the network. NTP is efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

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

NTP avoids synchronizing to a machine whose time may not be accurate, in two ways. First, NTP never synchronizes to a machine that is not synchronized itself. Second, NTP compares the time reported by several machines and does not synchronize to a machine whose time is significantly different than the others, even if its stratum is lower. This strategy effectively builds a self-organizing tree of NTP servers.

The Cisco implementation of NTP does not support stratum 1 service; in other words, it is not possible to connect to a radio or atomic clock (for some specific platforms, however, you can connect a GPS time-source device). We recommend that 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.

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

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

The Cisco implementation of NTP supports two ways that a networking device can obtain NTP time information on a network:

- By polling host servers
- By listening to NTP broadcasts

In a LAN environment, NTP can be configured to use IP broadcast messages. As compared to polling, IP broadcast messages reduce configuration complexity, because each machine can simply be configured to send or receive broadcast or multicast messages. However, the accuracy of timekeeping is marginally reduced because the information flow is one-way only.

An NTP broadcast client listens for broadcast messages sent by an NTP broadcast server at a designated IPv4 address. The client synchronizes the local clock using the first received broadcast message.

The time kept on a machine is a critical resource, so we strongly recommend 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 (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.



Note NTP-PTP interworking is not supported on Cisco NCS 540 Series routers till IOS XR Software Release 24.1.1.

Best Practices for NTP configuration

Follow these best practices when configuring NTP :

- Configure multiple redundant NTP time sources to avoid reliance on a single server and improve reliability.
- Use a loopback interface as the NTP source for consistency across device reboots and interface changes.
- Enable NTP authentication to secure communications and prevent malicious time alterations.
- Monitor NTP status and logs regularly; implement detection and alerting mechanisms using commands like **show ntp status** and **show ntp associations.**
- Use the **ntp panic-threshold-apply** command to check the configuration sanity checks, which reject large clock changes and prevent network instability.
- Address failure modes related to time-based authentication keychains by configuring overlapping key lifetimes to avoid routing disruptions.
- Regularly monitor and validate NTP synchronization status with monitoring tools and SNMP traps.

- Ensure operational practices include multiple NTP sources and configuration checks to prevent routing disruptions caused by time inaccuracies.

These practices help maintain accurate time synchronization, improve NTP security, and minimize the risk of network instability caused by incorrect time settings.

Configuring NTP

PTP-NTP Interworking

Table 17: Feature History Table

Feature Name	Release Information	Feature Description
PTP-NTP Interworking	Release 24.1.1	Introduced in this release on the following Cisco NCS 540 router variants running on Cisco IOS XR: • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS We have improved NTP synchronization and reliability to achieve nanosecond-level accuracy for applications that require high-precision timing. This is achieved by enabling NTP-PTP interworking which allows the use of PTP as the reference clock. As in previous releases, the NTP client continues to support polling NTP protocol-based external time servers to synchronize the local system clock and achieve accuracy within the millisecond range.

Before the support of PTP-NTP interworking, NTP worked with NTP server to get the clock.

PTP-NTP interworking provides the ability to use PTP, and other valid time of day (TOD) sources such as Data over Cable Service Interface Specification (DOCSIS) Timing Interface (DTI) and global positioning system (GPS), as the time source for the operating system in the units of nanosecond-level accuracy. PTP is capable of achieving nanosecond-level accuracy, while NTP is typically only accurate to within milliseconds. By using PTP as a reference clock, NTP can improve its accuracy and meet the needs of applications that require high precision timing.

PTP-NTP interworking also provides the means to communicate status changes between PTP and NTP processes. It also supports the unambiguous control of the operating system time and backplane time in the event of bootup, switchovers, or card and process failures.

With PTP-NTP interworking, NTP is less likely to lose synchronization. As, PTP is more robust to network delays and disruptions than NTP. Hence, PTP can still maintain accurate synchronization even if there's a problem with the network.

Enable PTP-NTP Interworking

Prerequisites for PTP-NTP Interworking

Ensure that PTP is enabled, before configuring PTP-NTP Interworking.

Configuration Example for PTP-NTP Interworking

You can configure PTP-NTP Interworking in any of the following ways:

- Setting NTP Primary Reference Clock as PTP

```
Router # Configure
Router(config) # ntp
Router(config-ntp) # master primary-reference-clock
Router(config-ntp) # commit
```

- Configuring NTP Server with IP address

  The following example shows an NTP configuration to allow the system clock to be synchronized by time server hosts at IP address 198.51.100.1. You can take IP address of a neighbouring PTP interface.

```
Router # Configure terminal
Router(config)# ntp server 198.51.100.1
Router(config-ntp) # commit
```

Verification

```
Router#show ntp status

Clock is synchronized, stratum 1, reference is 198.51.100.1
nominal freq is 1000000000.0000 Hz, actual freq is 101341889.2967 Hz, precision is 2**24
reference time is 8497CD13.A6AEB9DA (00:02:27.651 UTC Tue Jun 30 1970)
clock offset is -0.077 msec, root delay is 0.000 msec
root dispersion is 3937.89 msec, peer dispersion is 3937.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.0000088676 s/s
system poll interval is 64, last update was 4 sec ago
authenticate is disabled, panic handling is disabled,
hostname resolution retry interval is 1440 minutes

Router#Show ntp associations
  address         ref clock     st  when  poll reach  delay  offset    disp
*~198.51.100.1    .PTP.          0     -    64    0   0.00   0.000   16000
```

Configuring Poll-Based Associations

The following example shows an NTP configuration in which the router's system clock is configured to form a peer association with the time server host at IP address 192.168.22.33, and to allow the system clock to be synchronized by time server hosts at IP address 10.0.2.1 and 172.19.69.1:

```
ntp
  server 10.0.2.1 minpoll 5 maxpoll 7
  peer 192.168.22.33
  server 172.19.69.1
```

Configuring Broadcast-Based Associations

The following example shows an NTP client configuration in which interface 0/2/0/0 is configured to receive NTP broadcast packets, and the estimated round-trip delay between an NTP client and an NTP broadcast server is set to 2 microseconds:

```
ntp
 interface tengige 0/2/0/0
  broadcast client
  exit
broadcastdelay 2
```

The following example shows an NTP server configuration where interface 0/2/0/2 is configured to be a broadcast server:

```
ntp
 interface tengige 0/2/0/0
  broadcast
```

Configuring NTP Access Groups

The following example shows a NTP access group configuration where the following access group restrictions are applied:

Peer restrictions are applied to IP addresses that pass the criteria of the access list named peer-acl. Serve restrictions are applied to IP addresses that pass the criteria of access list named serve-acl.

Serve-only restrictions are applied to IP addresses that pass the criteria of the access list named serve-only-acl.

Query-only restrictions are applied to IP addresses that pass the criteria of the access list named query-only-acl.

```
ntp
  peer 10.1.1.1
  peer 10.1.1.1
  peer 10.2.2.2
  peer 10.3.3.3
  peer 10.4.4.4
  peer 10.5.5.5
  peer 10.6.6.6
  peer 10.7.7.7
  peer 10.8.8.8
  access-group peer peer-acl
  access-group serve serve-acl
  access-group serve-only serve-only-acl
  access-group query-only query-only-acl
  exit
ipv4 access-list peer-acl
  10 permit ip host 10.1.1.1 any
  20 permit ip host 10.8.8.8 any
  exit
ipv4 access-list serve-acl
  10 permit ip host 10.4.4.4 any
  20 permit ip host 10.5.5.5 any
  exit
ipv4 access-list query-only-acl
  10 permit ip host 10.2.2.2 any
```

```
  20 permit ip host 10.3.3.3 any
  exit
ipv4 access-list serve-only-acl
  10 permit ip host 10.6.6.6 any
  20 permit ip host 10.7.7.7 any
  exit
```

Configuring NTP Authentication

The following example shows an NTP authentication configuration. In this example, the following is configured:

NTP authentication is enabled.

Two authentication keys are configured (key 2 and key 3).

The router is configured to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 10.3.32.154 using authentication key 2.

The router is configured to allow its software clock to be synchronized with the clock by the device at IP address 10.32.154.145 using authentication key 3.

The router is configured to synchronize only to systems providing authentication key 3 in their NTP packets.

```
ntp
 authenticate
 authentication-key 2 md5 encrypted 06120A2D40031D1008124
 authentication-key 3 md5 encrypted 1311121E074110232621
 trusted-key 3
 server 10.3.32.154 key 3
 peer 10.32.154.145 key 2
```

Disabling NTP on an Interface

The following example shows an NTP configuration in which 0/2/0/0 interface is disabled:

```
ntp
 interface tengige 0/2/0/0
   disable
   exit
authentication-key 2 md5 encrypted 06120A2D40031D1008124
authentication-key 3 md5 encrypted 1311121E074110232621
authenticate
trusted-key 3
server 10.3.32.154 key 3
peer 10.32.154.145 key 2
```

Configuring the System as an Authoritative NTP Server

The following example shows a NTP configuration in which the router is configured to use its own NTP server clock to synchronize with peers when an external NTP source becomes unavailable:

```
ntp
  master 6
```

Updating the Hardware Clock

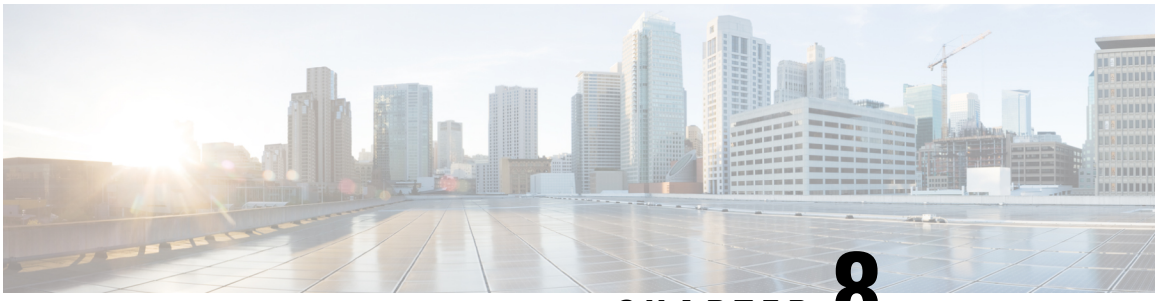
The following example shows an NTP configuration in which the router is configured to update its hardware clock from the software clock at periodic intervals:

```
ntp
  server 10.3.32.154
  update-calendar
```

Configuring NTP Server Inside VRF Interface

Note No specific command enables NTP; the first NTP configuration command that you issue enables NTP.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ntp
RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A
RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A source bvi 70
RP/0/RP0/CPU0:router(config-ntp)# end
or
RP/0/RP0/CPU0:router(config-ntp)# commit
```

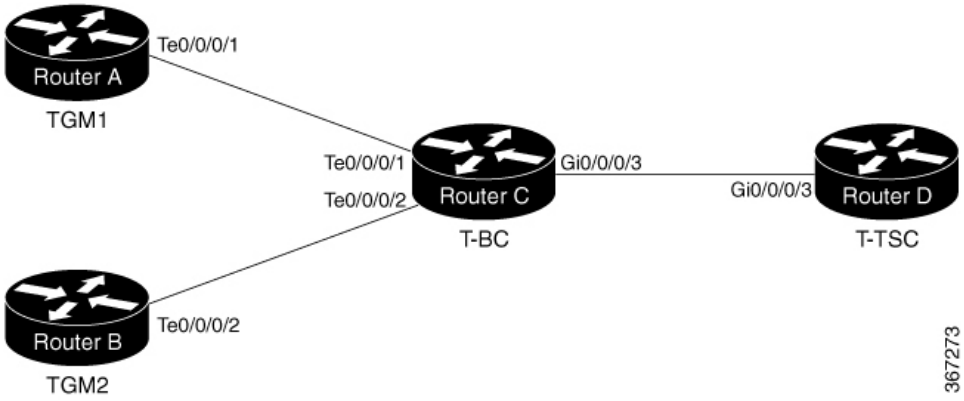


CHAPTER 8

Workflow and Use Case

Consider the following topology for configuring the G.8275.1:

Figure 5: Sample G.8275.1 Topology



Configuration on TGM1

```
frequency synchronization
 quality itu-t option 1
 clock-interface timing-mode system
!
clock-interface sync 2 location 0/RP0/CPU0
 port-parameters
  gps-input tod-format cisco pps-input ttl
  !
 frequency synchronization
  selection input
  wait-to-restore 0
  quality receive exact itu-t option 1 PRC
!
ptp clock
domain 24
  profile g.8275.1 clock-type T-GM
 !
 profile master
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
interface GigabitEthernet0/0/0/1
```

```
 ptp
  profile master
  multicast target-address ethernet 01-1B-19-00-00-00
  port state master-only
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
 !
```

Configuration on TGM2

```
frequency synchronization
 quality itu-t option 1
 clock-interface timing-mode system
!
clock-interface sync 2 location 0/RP0/CPU0
 port-parameters
  gps-input tod-format cisco pps-input ttl
  !
 frequency synchronization
  selection input
  wait-to-restore 0
  quality receive exact itu-t option 1 PRC
!
ptp clock
domain 24
  profile g.8275.1 clock-type T-BC
 !
 profile master
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
!
interface GigabitEthernet0/0/0/2
 ptp
  profile master
  multicast target-address ethernet 01-1B-19-00-00-00
  port state master-only
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
 !
```

Configuration on T-BC

```
frequency synchronization
 quality itu-t option 1
 clock-interface timing-mode system
!
ptp clock
domain 24
  profile g.8275.1 clock-type T-BC
 !
 profile slave
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
```

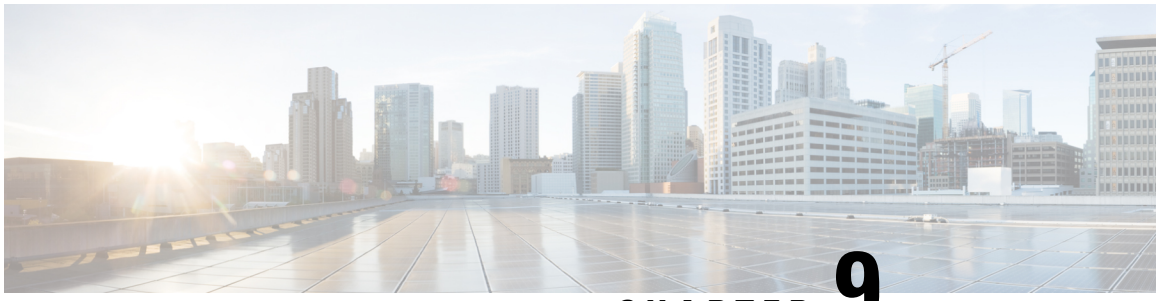
```
 !
physical-layer frequency
!

 profile master
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
! !
interface TenGigE0/0/0/1
 ptp
  profile slave
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  sync frequency 16
  local-priority 10
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
! !
interface TenGigE0/0/0/2
 ptp
  profile slave
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  port state any
  sync frequency 16
  local-priority 20
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
! !
interface GigabitEthernet0/0/0/3
 ptp
  profile master
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  port state any
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 frequency synchronization
! !
```

Configuration on T-TSC

```
frequency synchronization
 quality itu-t option 1
 clock-interface timing-mode system
! ptp
 clock
  domain 24
  profile g.8275.1 clock-type T-TSC
 !
 profile slave
```

```
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
!
physical-layer frequency
!
!
interface GigabitEthernet0/0/0/3
 ptp
  profile slave
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  port state slave-only
  local-priority 10
 !
 frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
!
```



CHAPTER 9

Configure the Global Navigation Satellite System

Effective Cisco IOS XR Release 7.5.1, GNSS is supported on the following router variants:

- N540-FH-CSR-SYS
- N540-FH-AGG-SYS

This chapter describes the Global Navigation Satellite System (GNSS) and how to configure it.

In typical telecom networks, network synchronization works in a hierarchal manner where the core network is connected to a stratum-1 clock. The timing from the stratum-1 clock is then distributed along the network in a tree-like structure. However, with a GNSS receiver, clocking is changed to a flat architecture, where access networks can directly take clock from the satellites by using an on-board GPS chip.

Router now uses a satellite receiver, also called the Global Navigation Satellite System (GNSS), as the new timing interface.

This capability simplifies network synchronization planning and provides flexibility and resilience in resolving network synchronization issues in the hierarchical network.

- Overview of GNSS, on page 111
- Operation of GNSS Module , on page 113
- Prerequisites for GNSS, on page 114
- Restrictions for GNSS, on page 115
- Configure GNSS, on page 115

Overview of GNSS

Effective Cisco IOS XR Release 7.1.1, the following Cisco NCS 540 variants support GNSS receiver:

- N540X-16Z4G8Q2C-A
- N540X-16Z4G8Q2C-D
- N540X-12Z16G-SYS-A
- N540X-12Z16G-SYS-D
- N540-12Z20G-SYS-A
- N540-12Z20G-SYS-D

- N540-24Z8Q2C-SYS
- N540-28Z4C-SYS-A
- N540-28Z4C-SYS-D
- N540-ACC-SYS
- N540X-ACC-SYS

Effective Cisco IOS XR Release 7.3.1, the following Cisco NCS 540 variants support GNSS receiver:

- N540-24Z8Q2C-SYS
- N540-28Z4C-SYS
- N540-ACC-SYS
- N540X-ACC-SYS

Effective Cisco IOS XR Release 7.4.1, the following Cisco NCS 540 variant supports GNSS receiver:

- N540-24Q8L2DD-SYS

Effective Cisco IOS XR Release 7.5.2, the following Cisco NCS 540 variant supports GNSS receiver:

- N540X-16Z8Q2C-D

No license is required to enable the GNSS module. The GNSS LED on the front panel indicates the status of the module. The following table describes the different status of GNSS LED:

LED Status	Description
Green	GNSS NormalState.Selfsurvey is complete.
Amber	GNSS not shut and not locked
OFF	If GNSS is not configured or is shut.

When connected to an external antenna, the module can acquire satellite signals and track up to 32 GNSS satellites, and compute location, speed, heading, and time. GNSS provides an accurate one pulse-per-second (PPS), a stable 10 MHz frequency output to synchronize broadband wireless, aggregation and pre-aggregation routers, and an accurate time-of-day (ToD).

Note NCS540X can also receive 1PPS, 10 MHz, and ToD signals from an external clocking and timing source. However, the timing signals from the GNSS module (when enabled) take precedence over those of the external source.

Note We do not recommend that you configure both the front panel (10M, 1PPS and ToD) input configuration and the GNSS input configuration.

By default, anti-jamming is enabled on the GNSS module.

Operation of GNSS Module

Operation of GNSS Module on the N540-24Z8Q2C-SYS, N540-28Z4C-SYS, N540-ACC-SYS, and N540X-ACC-SYS Routers

The GNSS module has the following stages of acquiring and providing timing signals to the Cisco router:

- Self-survey mode - When the router is reset, the GNSS module comes up in self-survey mode. It tries to lock on to a minimum of four different satellites and computes approximately 2000 different positions of the satellites to obtain a 3-D location (Latitude, Longitude, and Height) of its current position. This operation takes about 35 to 40 minutes. During this stage, the module is also able to generate accurate timing signals and achieve a Normal or Phase-locked state.

  When GNSS moves into Normal state, you can start using the 1PPS, 10 MHz, and ToD inputs from GNSS. The quality of the signal in self-survey mode with Normal state is considered good enough to lock to GNSS.

- Over determined clock mode - The router switches to over determined (OD) mode when the self-survey mode is complete, and the position information is stored in non-volatile memory on the router. In this mode, the module only processes the timing information based on satellite positions captured in self-survey mode.

The router saves the tracking data, which is retained even when the router is reloaded.

The GNSS module stays in OD mode until one of the following conditions occur:

- A position relocation of the antenna of more than 100 meters is detected. This detection causes an automatic restart of the self-survey mode.
- A manual restart of the self-survey mode or when the stored reference position is deleted.
- A worst-case recovery option after a jamming-detection condition that cannot be resolved with other methods.

You can configure the GNSS module to automatically track any satellite or configure it to explicitly use a specific constellation. However, the module uses configured satellites in only the OD mode.



Note GLONASS and BeiDou satellites cannot be enabled simultaneously.

When the router is reloaded, it always comes up in OD mode unless:

- the router is reloaded when the self-survey mode is in progress.
- the physical location of the router is changed to more than 100 meters from its pre-reloaded condition.

When the system restarts the GNSS self-survey by using the default gnss slot R0/R1 command in config mode, the 10MHz, 1PPS, and ToD signals are not changed and remain up.

Operation of GNSS Module on the N540X-16Z4G8Q2C-A, N540X-16Z4G8Q2C-D, N540X-12Z16G-SYS-A, and N540X-12Z16G-SYS-D Routers, N540X-6Z18G-SYS-A, N540X-6Z18G-SYS-D, N540X-8Z16G-SYS - A, N540X-8Z16G-SYS - D

The GNSS module has the following stages of acquiring and providing timing signals to the Cisco router:

- Self-survey mode - Self-survey is the procedure that is performed prior to using time mode. It determines the position of a stationary receiver by building a weighted mean of all valid 3D position solutions.

  To stop self-survey mode, the following two requirements must be met:

  - The minimum observation time defines a minimum amount of observation time regardless of the actual number of valid fixes that are used for position calculation. Reasonable values range from one day for high accuracy position calculation to a few minutes for coarse position determination.
  - The required 3D position standard deviation defines a limit on the spread of positions that contribute to the calculated mean. As the position error translates into a time error when using time mode, you should carefully evaluate the time accuracy requirements and choose an appropriate value.

  Self-survey ends when both requirements are met. After self-survey is completed successfully, the receiver automatically enters time-fix mode.

  Recommendations

  - Self-survey must run for at least twenty-four hours because it is important to cover a full constellation run and a day-night cycle.
  - CNO or signal strength for achieving time-fix during self-survey is 35dB.

- Time-fix mode - In order to use the time-fix mode, the exact position of the receiver must be known. The exact position of the receiver is determined by using self-survey. Errors in the fixed position translate into time errors depending on the satellite constellation.

  There is no minimum and maximum value (Time) in the self-survey process and the receiver makes the best effort to achieve the time-fix mode.

  For achieving the time-fix mode, a minimum of four satellites are required and it may take several days to get into the time-fix mode.

  If the position is already known, the module can achieve time-fix mode even if there is only one satellite received.

You can configure the GNSS module to automatically track any satellite or configure it to explicitly use a specific constellation.

When the router is reloaded, it always comes up in the time-fix mode unless the router is reloaded when the self-survey mode is in progress.

Prerequisites for GNSS

To use GNSS, the antenna must see as much as possible from the sky. For proper timing, a minimum of four satellites must be locked. For more information, see the *Cisco NCS 540 Series Router Hardware Installation Guide*.

Restrictions for GNSS

- The GNSS module is not supported through SNMP; all configurations are performed through commands.
- The GNSS holdover performance is one microsecond in two hours of holdover after twelve hours of GNSS lock time.
- GNSS module is not supported in default profile mode.

Configure GNSS

Configuration Example

This section describes how you can configure GNSS for a router.

```
/* Enable the GNSS receiver and enter the gnss-receiver submode */

Router(config)# gnss-receiver 0 location 0/RP0/CPU0
Router(config-gnss)# no shutdown
Router(config-gnss)# frequency synchronization
Router(config-gnss-freqsync)# selection input
Router(config-gnss-freqsync)# commit
```

Optional Configuration Example

```
Router(config)# gnss-receiver 0 location 0/RP0/CPU0
Router(config-gnss)# anti-jam disable
Router(config-gnss)# constellation GPS
Router(config-gnss)# snr threshold 10
Router(config-gnss)# frequency synchronization
Router(config-gnss-freqsync)# selection input
Router(config-gnss-freqsync)# priority 5  >>>Values can range from 1 (highest priority) to
 254 (lowest priority). The default value is 100.
Router(config-gnss-freqsync)# wait-to-restore 0
```

Running Configuration

```
gnss-receiver 0 location 0/RP0/CPU0
frequency synchronization
  selection input
  priority 1
  wait-to-restore 0
  quality receive exact itu-t option 1 PRC
 !
!
```

Verification

The following is the output of the **show gnss-receiver** command on the router models.

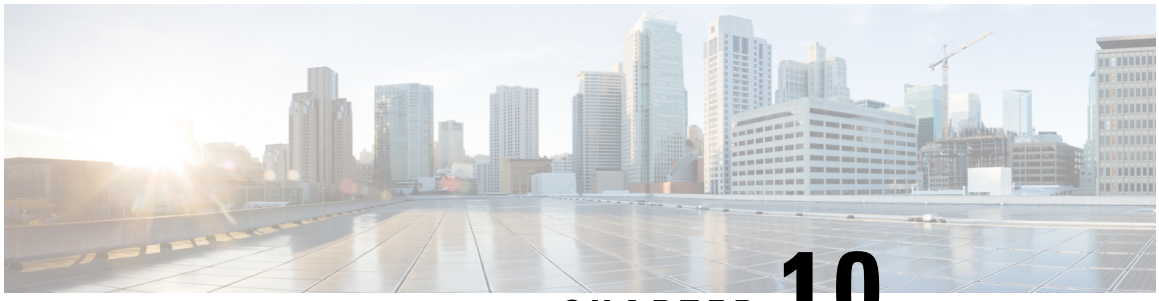
The following is the output of the **show gnss-receiver** command on the router models - N540-24Z8Q2C-SYS, N540-28Z4C-SYS, N540-ACC-SYS, and N540X-ACC-SYS.

```
RP/0/RP0/CPU0:R6# show gnss-receiver
Fri Jan 17 07:27:34.804 UTC
GNSS-receiver 0 location 0/RP0/CPU0
    Status: Available, Up
    Position: 12:56.18 N 77:41.77 E 0.823km
    Time: 2020:01:17 07:31:41 (UTC offset: 0s)
    Locked at: 2020:01:15 17:15:28
    Firmware version: TIM 1.10
    Lock Status: Phase Locked, Receiver Mode: Time fix only
    Survey Progress: 100, Holdover Duration: Unknown
    Major Alarms: Unknown
    Minor Alarms: Unknown
    Anti-jam: Enabled, Cable-delay compensation: 0
    1PPS polarity: Positive
    PDOP: 99.990, HDOP: 99.990, VDOP: 99.990, TDOP: 0.240
    Constellation: GPS, Satellite Count: 17
    Satellite Thresholds:
        SNR - 0 dB-Hz, Elevation - 0 degrees, PDOP - 0, TRAIM - 0 us
    Satellite Info:
        CHN: Channel, AQUN: Aquisition, EPH: Ephemeris
        PRN   CHN   AQUN   EPH    SV            Signal
        No.   No.   Flag   Flag   Type          Strength   Elevat'n   Azimuth
        ---   ---   ----   ----   -----------   --------   --------   --------
          1   n/a   On     On     GPS             44.000     19.000    220.000
          3   n/a   On     On     GPS             48.000     62.000    299.000
          4   n/a   On     On     GPS             46.000     30.000    338.000
          7   n/a   On     On     GPS             47.000      9.000    261.000
          8   n/a   On     On     GPS             41.000     17.000    172.000
          9   n/a   On     On     GPS             44.000      7.000    317.000
         11   n/a   On     On     GPS             42.000     10.000    202.000
         14   n/a   On     On     GPS             42.000     22.000     90.000
         16   n/a   On     On     GPS             46.000     66.000     59.000
         22   n/a   On     On     GPS             47.000     71.000    238.000
         23   n/a   On     On     GPS             46.000     27.000    332.000
         26   n/a   On     On     GPS             48.000     40.000     40.000
```

The following is the output of the **show gnss-receiver** command on the router models - N540X-16Z4G8Q2C-A, N540X-16Z4G8Q2C-D, N540X-12Z16G-SYS-A, N540X-12Z16G-SYS-D, N540X-6Z18G-SYS-A, N540X-6Z18G-SYS-D, N540X-8Z16G-SYS - A, N540X-8Z16G-SYS - D.

```
RP/0/RP0/CPU0:ios#show gnss-receiver
Sun Sep 29 09:25:29.477 UTC
GNSS-receiver 0 location 0/RP0/CPU0
    Status: Available, Up
    Position: 12:56.18 N 77:41.77 E 0.823km
    Time: 2019:10:24 11:32:21 (UTC offset: 0s)
    Locked at: 2019:09:29 09:19:20
    Firmware version: TIM 1.10
    Lock Status: Phase Locked, Receiver Mode: Time fix only
    Survey Progress: 100, Holdover Duration: Unknown
    Major Alarms: Unknown
    Minor Alarms: Unknown
    Anti-jam: Enabled, Cable-delay compensation: 0
    1PPS polarity: Positive
    PDOP: 99.990, HDOP: 99.990, VDOP: 99.990, TDOP: 0.450
    Constellation: Auto, Satellite Count: 5
    Satellite Thresholds:
        SNR - 0 dB-Hz, Elevation - 0 degrees, PDOP - 0, TRAIM - 0 us
    Satellite Info:
        CHN: Channel, AQUN: Aquisition, EPH: Ephemeris
        PRN   CHN   AQUN   EPH    SV            Signal
        No.   No.   Flag   Flag   Type          Strength   Elevat'n   Azimuth
        ---   ---   ----   ----   -----------   --------   --------   --------
```

```
  1   n/a   On      On      GLONASS         28.000     19.000    342.000
  7   n/a   On      On      GLONASS         25.000     30.000     91.000
  8   n/a   On      On      GLONASS         25.000     42.000     28.000
 10   n/a   On      On      GLONASS         33.000     54.000    211.000
 11   n/a   On      On      GLONASS         33.000     78.000    217.000
```



CHAPTER 10

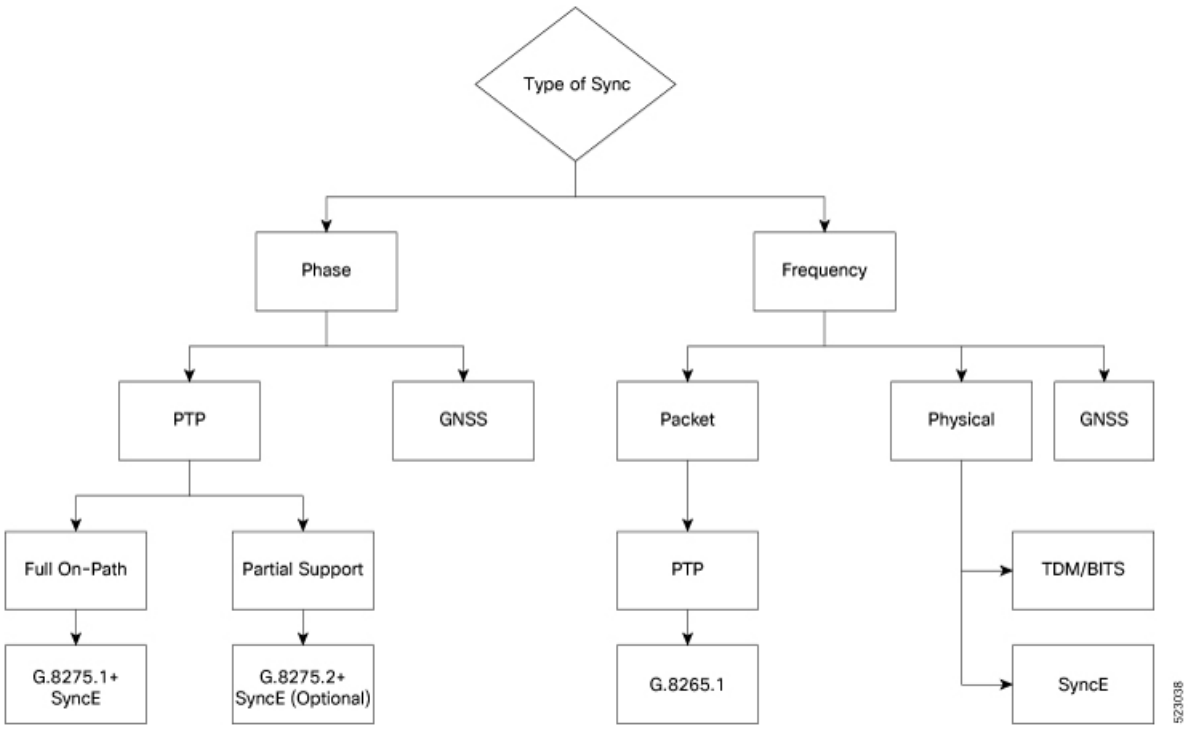
Network Synchronization Design Best Practices

The synchronization of a network is essential for ensuring that all devices in a network run on the same clock time. It also ensures that the applications in the network function correctly. To design your network synchronization accurately, you must have a clear understanding of your network requirements, timing budget, application requirements, and the desired level of synchronization accuracy. This section describes some best practices to follow when designing your network synchronization.

- Network Synchronization Decision Tree, on page 119
- Restrictions for Network Synchronization , on page 120
- General Guidelines for Successful Synchronization Deployments, on page 120
- Guidelines for Phase Synchronization Deployments, on page 122
- PTP over IP Network Design, on page 123
- Selecting the Correct Profile For Network Synchronization, on page 123
- Reducing Asymmetry, on page 124
- Reducing Packet Delay Variation, on page 124
- Remediating Transport Asymmetry, on page 125
- Synchronizing Across Networks, on page 125

Network Synchronization Decision Tree

Use the network synchronization decision tree for determining the appropriate synchronization solution for your network deployment. Network synchronization helps in ensuring that the network operates with accurate and synchronized time.



Restrictions for Network Synchronization

- Do not configure MACsec with Sync-E or PTP on the same interface, as this combination is not supported.
- When using PTP with MACsec can result in time delay inconsistencies because MACsec header processing affects precise timestamping, which may reduce synchronization accuracy.

General Guidelines for Successful Synchronization Deployments

Network synchronization is crucial for maintaining reliable and efficient network operations, ensuring data integrity, complying with regulations, and facilitating troubleshooting and management tasks. The following guidelines help in deploying successful network synchronization for your network:

- Ensure that you use a standards-based solution designed for your need. For example, use the correct profile.
- Configure the appropriate clock source for your network. It can be Global Navigation Satellite System (GNSS) based such as a Global Positioning System (GPS) clock, or a Precision Time Protocol (PTP) grandmaster clock.
  - Frequency synchronization requires Building Integrated Timing Supply (BITS) or synchronous Ethernet, and Phase synchronization requires PTP and/or GNSS.
  - Use a combination of GNSS over the air and/or PTP or synchronous Ethernet over transport.

For more information on SyncE and PTP, refer to *Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers*.

- Set up the synchronization protocols that are required, which includes PTP, Network Time Protocol (NTP), or synchronous Ethernet.
  - NTP uses the system clock for logging events in the system, or to show clock output, whereas PTP and GNSS work on the IEEE 1588 hardware clock in the system.
  - The NTP clock of a node can't be used to synchronize the downstream network using PTP. However, a node can synchronize its NTP clock with the available PTP or GNSS clock.



Note Most NTP implementations are software-based. Software-based time synchronization is less accurate than hardware-based synchronization, but it's still useful for applications where low levels of accuracy, such as 10's or 100's of milliseconds, are acceptable.

  - Use PTP for phase synchronization in the absence of a GNSS.
  - Synchronous Ethernet (SyncE) is a recommendation from ITU Telecommunication Standardization Sector (ITU-T) on how to deliver a frequency in a network. If you require a frequency-only synchronization solution, use SyncE instead of PTP.

- Configure the appropriate synchronization profiles and preferences for your network. It might include the accuracy, priority, and other parameters that determine how your network handles synchronization events.
- Design your network for phase synchronization with optimal time error budgets.
  - Use boundary clocks to reduce time error and to reset Packet Delay Variation (PDV).
  - Ensure that PTP awareness is implemented consistently throughout, including the transport system, and that boundary clocks accurately transmit time to minimize accumulated time error.
- For phase synchronization, use a hybrid clock that incorporates both SyncE and PTP.

  For more information on PTP Hybrid Mode, refer to *Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers*.
- Reduce the number of hops:
  - Distribute sources of time to meet the budget. If you have too many hops, install a GNSS receiver further out into the network.
  - Don't centralize two Primary Reference Time Clocks (PRTC) and Telecom Grandmasters (T-GM) in two different locations and try to run a synchronization signal accurately across the whole network.
- Minimize Packet Delay Variation (PDV) and jitter. Ensure that microwaves, Gigabit-capable Passive Optical Networks (GPON), Digital Subscriber Line (DSL), and Dense Wavelength Division Multiplexing (DWDM) are PTP aware.
- Monitor your synchronization deployment to ensure that it's functioning correctly and meeting your desired level of accuracy.

For more information, refer to Verifying the Frequency Synchronization Configuration in the *Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers*.

- Be aware of any relevant industry standards and practices when deploying synchronization.

Guidelines for Phase Synchronization Deployments

Follow these guidelines for phase synchronization deployments.

- Set up the necessary network infrastructure to support phase synchronization. It includes installing timing devices such as GPS receivers, synchronous Ethernet interfaces, and timing servers.
- Configure the phase synchronization protocols such as setting up PTP as appropriate.
- As best practice, use the G.8275.1 telecommunication profile standard with complete on-path support, including Layer-2 multicast in combination with SyncE.
- Minimize phase time error by performing the following tasks:
  - Remove asymmetric routing issues.
  - Reduce the number of hops, unless telecommunication grandmaster (T-GM) clocks are deployed in the preaggregation network.
  - Decrease PDV or packet jitter.
- If you use IP protocols for PTP, you can run into issues with rerouting, asymmetric routing, Equal Cost Multi-Path (ECMP), bundles, and so on.
- If you need tight timing budgets over many hops, ensure that your hardware supports the highest levels of clock accuracy.
- For GNSS deployments:
  - Meet all the requirements for cable and antenna installations.
  - Consult with a professional if you don’t have experience with GNSS installation and calibration.
- Make sure that your deployment is working as intended. Monitor it regularly to identify any potential issues.
- Consult with Cisco technical support if you encounter any issues or have questions.



Note When PTP is used with MACsec, achieving high accuracy can be challenging. PTP requires exact timestamping to maintain tight network synchronization. MACsec affixes and detaches a header that is between 24–32 bytes in size. This process can lead to significant inconsistencies in the time delays between where the link is connected and the location where the egress timestamps are applied.

PTP over IP Network Design

When using networks to carry frequency over Precision Time Protocol over Internet Protocol (PTPoIP), the goal is to minimize Packet Delay Variation (PDV) by reducing the number of hops. Use the following guidelines:

- The placement of the telecom grandmaster (T-GM) clock plays an important role in ensuring that the network operates within your timing budget. For example, place a pair of T-GM clocks in a centralized location only if the network has a small number of hops. In larger networks with multiple hops, it may be necessary to distribute T-GM clocks throughout the network to ensure proper timing management at each hop.
- Use a dedicated frequency synchronization protocol such as synchronous Ethernet or 1588v2, which is designed specifically to maintain precise frequency synchronization between devices.
- Use the G.8265.1 standard. Frequency synchronization using the G.8265.1 standard is a way to make sure multiple devices on a network are operating at the same frequency, allowing for more accurate and reliable communication.
- Configure Quality of Service (QoS) policies to prioritize network traffic and reduce delays. This can be done by using traffic shaping, traffic policing, and queue management.

Selecting the Correct Profile For Network Synchronization

G.8275.1 PTPoE

G.8275.1 is a technical specification standard for Precision Time Protocol over Ethernet (PTPoE). It defines how you can use the Precision Time Protocol (PTP) to synchronize clocks over Ethernet networks with layer 2 multicast. PTPoE is an extension of PTP that allows it to be used over Ethernet networks. It's used in applications where precise time synchronization is required.

For more information, refer to G.8275.1 in the *Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers*.

G.8275.2 PTPoIP

G.8275.2 is a technical specification standard for Precision Time Protocol over Internet Protocol (PTPoIP). It defines the use of the Precision Time Protocol (PTP) over packet-based networks such as Internet Protocol (IP) networks, to provide precise time synchronization of network devices.

For more information, refer to G.8275.2 in the *Network Synchronization Configuration Guide for Cisco NCS 540 Series Routers*.

Feature Adaptability on Each Profile

The following table lists the adaptability of features on each profile:

Feature	G.8275.1 PTPoE	G.8275.2 PTPoIP
Network Model	Full on-path support	Partial on-path support

Feature	G.8275.1 PTPoE	G.8275.2 PTPoIP
IP Routing	Not applicable	Can cause issues in rings and asymmetry from a number of causes
Transit Traffic	Not allowed	Can result in jitter and asymmetry
Performance	Optimal	Variable
Configuration Model	Physical port	L3 device
PTP over Bundles	No issues	Work in progress for Telecom Boundary Clocks (T-BC)
Asymmetry	Reduced due to T-BC on every node	Optimal when deployed as a Partial Support Telecom Boundary Clock (T-BC-P)
PDV/Jitter	Reduced due to T-BC on every node	Optimal when deployed as a T-BC-P

Reducing Asymmetry

Asymmetry occurs in a PTP unaware network for the following scenarios:

- When routing large networks, complex topologies, rings, and Equal-cost multi-path (ECMP)
- When using PTP unaware transit nodes, especially with varying traffic patterns
- In the transport layer such as Passive Optical Network (PON), cable, DWDM, and complex optics

Note Every 2 seconds of asymmetry results in 1 microsecond of time error.

To reduce asymmetry in a PTP unaware network:

- Use QoS: QoS can help reduce asymmetry in an unaware network.
- Implement Telecom Boundary Clocks (T-BC): T-BCs can handle asymmetry in the nodes when implemented correctly.

Reducing Packet Delay Variation

To reduce the effects of Packet Delay Variation (PDV) on PTP clock recovery, you must have a steady layer of packets that arrive in minimum time.

- Implement Telecom Boundary Clocks (T-BC) in the PTP unaware node. T-BC introduces a time reference to the PTP unaware node, which then synchronizes its clock with the T-BC.

- Use a high-quality network connection between the T-BC and the PTP unaware node. A high-quality network connection, such as a dedicated fiber link, can help reduce PDV due to network impairments.

Remediating Transport Asymmetry

Transport asymmetry occurs when data is transported at varying rates in different directions over a communication link, leading to an imbalance in transport. To correct this issue:

- Ensure that your transport layer is PTP aware.

  In optical devices, use a wavelength division multiplexing (WDM) technology such as Optical Service Channel (OSC) for managing your fiber optic infrastructure effectively.

Synchronizing Across Networks

To avoid synchronization issues when connecting to other mobile networks:

- Make sure to align all mobile networks to a common source of time. For example, align mobile networks to the Coordinated Universal Time (UTC) from a Global Navigation Satellite System (GNSS) such as Global Positioning System (GPS).
- Monitor your clocks at the interconnect points.



Note In 5G networks, using standalone GNSS receivers at every radio site may not provide the sub-100 nanosecond accuracy required for the timing requirements of Fronthaul radio systems.