Timing and Synchronization Configuration Guide, Cisco IOS XE 17 (Cisco NCS 4200 Series)

First Published: 2019-12-23

Last Modified: 2020-07-31

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.

CONTENTS

CHAPTER 8

CHAPTER 1

Feature History

Feature	Description
Cisco IOS XE Amsterdam 17.3.1	
Telemetry for GNSS Module	This feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language. Prior to this release, the traditional show commands were available to only view the GNSS statistic data. But, you could not use these show command outputs to manage network devices as demanded by centralized orchestration application such as Cisco Digital Network Architecture Center (DNAC). The introduction of this feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language to bring more visibility in the timing services operations. This feature is supported on Cisco RSP3 module.
Cisco IOS XE Amsterdam 17.1.1	
PTP Multiprofile	The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a network. The PTP Multiprofile support is configured on a PTP boundary clock by translating one PTP profile at PTP slave port to other PTP profile at PTP master port. To translate PTP properties from one profile to other, a special type of inter-op clock-port is introduced. This special clock-port is configured with the required profile and domain information.
Traps and Performance MIBs for GNSS	A new MIB, CISCO-GNSS-MIB, is introduced for GNSS.

CHAPTER 2

Configuring Clocking and Timing

This chapter explains how to configure timing ports on the Route Switch Processor (RSP) modules and includes the following sections:

Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the chassis:

- Interfaces carrying PTP traffic must be under the same VPN Routing and Forwarding (VRF). Misconfiguration will cause PTP packet loss.

  Use the 10 Gigabit Links to configure VRF on two Cisco RSP3 Routers.

- You can configure only a single clocking input source within each group of eight ports (0–7 and 8–15) on the T1/E1 interface module using the **network-clock input-source** command.
- Multicast timing is *not* supported.
- Out-of-band clocking and the **recovered-clock** command are *not* supported.
- Precision Time Protocol (PTP) is supported only on loopback interfaces.
- Synchronous Ethernet clock sources are *not* supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet except when configured as hybrid clock. However, you can use hybrid clocking to allow the chassis to obtain frequency using Synchronous Ethernet, and phase using PTP.
- Time of Day (ToD) and 1 Pulse per Second (1PPS) input is *not* supported when the chassis is in boundary clock mode.
- Multiple ToD clock sources are *not* supported.
- PTP redundancy is supported only on unicast negotiation mode; you can configure up to three server clocks in redundancy mode.

- In order to configure time of day input, you must configure both an input 10 Mhz and an input 1 PPS source.
- PTP over IPv6 is *not* supported.
- SyncE Rx and Tx is supported on uplink interfaces when using 8 x 1 GE Gigabit Ethernet SFP Interface Module.
- When PTP is configured, changing the configuration mode from LAN to WAN or WAN to LAN is *not* supported for following IMs:
    - 2x10G
    - 8x1G_1x10G_SFP
    - 8x1G_1x10G_CU
- PTP functionality is restricted by license type.

Note If you install the IEEE 1588-2008 BC/MC licenseIEEE 1588-2008 BC/MC license (available by default), you must reload the chassis to use the full PTP functionality.

Note By default, all timing licenses are already included on the Cisco NCS 4200 routers.

- End-to-end Transparent Clock is *not* supported for PTP over Ethernet.
- Transparent clock is not supported on the Cisco RSP3 Module.
- G.8265.1 telecom profiles are *not* supported with PTP over Ethernet.
- The chassis does *not* support a mix of IPv4 and Ethernet clock ports when acting as a transparent clock or boundary clock.

The following restrictions apply when configuring synchronous Ethernet SSM and ESMC:

- To use the **network-clock synchronization ssm option** command, ensure that the chassis configuration does *not* include the following:
    - Input clock source
    - Network clock quality level
    - Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is *not* a network clocking configuration applied to synchronous Ethernet interfaces, BITS interfaces, and timing port interfaces.

- SSM and ESMC are SSO-coexistent, but not SSO-compliant. The chassis goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.
- The chassis does not support ESMC messages on the S1 byte on SONET/SDH and T1/E1 interface modules.
- It is recommended that you do *not* configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).
- You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.
- When you configure the ports using the **synchronous mode** command on a copper interface, the port attempts to auto-negotiate with the peer-node copper port and hence the auto negotiation is incomplete as both the ports try to act as server clock, which in turn makes the port down. Hence, for a successful clock sync to happen, you should configure the ports using **network-clock input-source** *1* **interface** *interface id* command prior to the configuration using the **synchronous mode** command under the interfaces to ensure that one of the ports behaves as a server clock.

  It is not recommended to configure the copper ports using the **synchronous mode** command.

Restrictions on RSP3 Module

The following clocking and timing restrictions are supported on the RSP3 Module:

- Precision Time Protocol (PTP) is supported only on the routed interfaces.
- Transparent Clock over 1 Gigabit Ethernet port performance is *not good.*
- PTP is supported for LAN for the following IMs. WAN is not supported.
  - 2x40
  - 1x100 GE
  - 8x10 GE
- To shift from non hybrid clock configuration to hybrid clock configuration, you must first unconfigure PTP, unconfigure netsync, reconfigure netsync and configure hybrid PTP.

Clocking and Timing Overview

The chassis have the following timing ports:

- 1 PPS Input/Output
- 10 Mhz Input/Output
- ToD
- Building Integrated Timing Supply (BITS)

You can use the timing ports on the chassis to perform the following tasks:

- Provide or receive 1 PPS messages

- Provide or receive time of day (ToD) messages
- Provide output clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz
- Receive input clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz

Note Timing input and output is handled by the active RSP.

Note For timing redundancy, you can use a Y cable to connect a GPS timing source to multiple RSPs. For information, see the *Cisco NCS 4206 Series Hardware Installation Guide*.

SyncE is supported in both LAN and WAN mode on a 10 Gigabit Ethernet interface.

The following sections describe how to configure clocking and timing features on the chassis.

Understanding PTP

The Precision Time Protocol (PTP), as defined in the IEEE 1588 standard, synchronizes with nanosecond accuracy the real-time clocks of the devices in a network. The clocks in are organized into a server-member hierarchy. PTP identifies the switch 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 and are referred to as members. Constantly exchanged timing messages ensure continued synchronization.

PTP is particularly useful for industrial automation systems and process control networks, where motion and precision control of instrumentation and test equipment are important.

Table 1: Nodes within a PTP Network

Network Element	Description
Grandmaster (GM)	A network device physically attached to the server 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. • 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.
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 clock.

Network Element	Description
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.

Telecom Profiles

Cisco IOS XE Release 3.8 introduces support for telecom profiles, which allow you to configure a clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. For information about how to configure telecom profiles, see Configuring Clocking and Timing, on page 17.

Effective Cisco IOS-XE Release 3.18, the G.8275.1 telecom profile is also supported on the Cisco NCS 4206 Series with RSP2 module. For more information, see G.8275.1 Telecom Profile .

PTP Redundancy

PTP redundancy is an implementation on different clock nodes. This helps the PTP subordinate clock node achieve the following:

- Interact with multiple server ports such as grand server clocks and boundary clock nodes.
- Open PTP sessions.
- Select the best server from the existing list of server clocks (referred to as the primary PTP server port or server clock source).
- Switch to the next best server available in case the primary server clock fails, or the connectivity to the primary server fails.

Note The Cisco NCS 4206 Series chassis supports unicast-based timing as specified in the 1588-2008 standard.

For instructions on how to configure PTP redundancy, see Configuring PTP Redundancy, on page 37.

PTP Asymmetry Readjustment

Each PTP node can introduce delay asymmetry that affects the adequate time and phase accuracy over the networks. Asymmetry in a network occurs when one-way-delay of forward path (also referred as forward path delay or ingress delay) and reverse path (referred as reverse path delay or egress delay) is different. The magnitude of asymmetry can be either positive or negative depending on the difference of the forward and reverse path delays.

Effective Cisco IOS XE Gibraltar 16.10.1, PTP asymmetry readjustment can be performed on each PTP node to compensate for the delay in the network.

Restriction

In default profile configuration, delay-asymmetry value is provided along with the clock source command. This restricts it to change the delay-asymmetry value with a complete reconfiguration of **clock source** command. The delay-asymmetry value should be considered as static and cannot be changed at run-time.

PTP Redundancy Using Hop-By-Hop Topology Design

Real world deployments for IEEE-1588v2 for mobile backhaul requires the network elements to provide synchronization and phase accuracy over IP or MPLS networks along with redundancy.

In a ring topology, a ring of PTP boundary clock nodes are provisioned such that each boundary clock node provides synchronization to a number of PTP client clocks connected to it. Each such ring includes at least two PTP server clocks with a PRC traceable clock.

However, with this topology the following issues may occur:

- Node asymmetry and delay variation—In a ring topology, each boundary clock uses the same server, and the PTP traffic is forwarded through intermediate boundary clock nodes. As intermediate nodes do not correct the timestamps, variable delay and asymmetry for PTP are introduced based on the other traffic passing through such nodes, thereby leading to incorrect results.
- Clock redundancy—Clock redundancy provides redundant network path when a node goes down. In a ring topology with PTP, for each unicast PTP solution, the roles of each node is configured. The PTP clock path may not be able to reverse without causing timing loops in the ring.

No On-Path Support Topology

The topology (see Figure 1: Deployment in a Ring - No On-Path Support with IPv4, on page 8) describes a ring with no on-path support. S1 to S5 are the boundary clocks that use the same server clocks. GM1 and GM2 are the grandmaster clocks. In this design, the following issues are observed:

- Timestamps are not corrected by the intermediate nodes.
- Difficult to configure the reverse clocking path for redundancy.
- Formation of timings loops.

Figure 1: Deployment in a Ring - No On-Path Support with IPv4

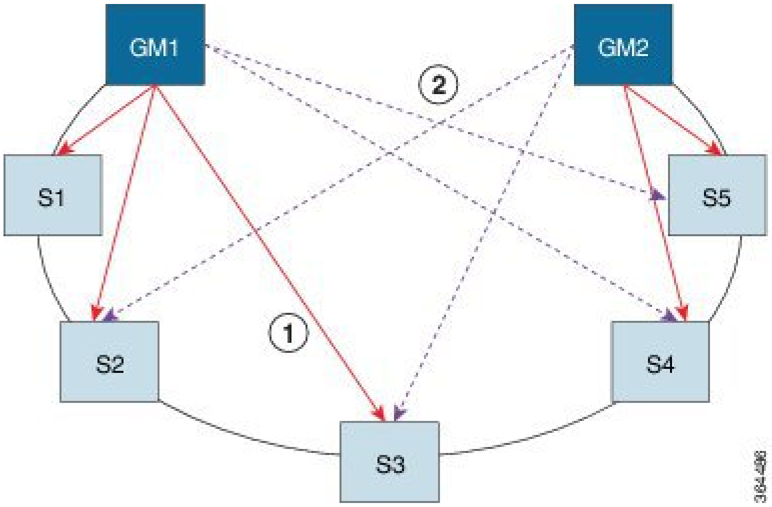


Table 2: PTP Ring Topology—No On-Path Support

Clock Nodes	Behavior in the PTP Ring
GM1	Grandmaster Clock
GM2	Grandmaster Clock
S1	Server Clocks: M1 (1st), M2 (2nd)
S2	Server Clocks: M1 (1st), M2 (2nd)
S3	Server Clocks: M1 (1st), M2 (2nd)
S4	Server Clocks: M2 (1st), M1 (2nd)
S5	Server Clocks: M2 (1st), M1 (2nd)

A solution to the above issue is addressed by using Hop-by-Hop topology configuration.

Hop-By-Hop Topology in a PTP Ring

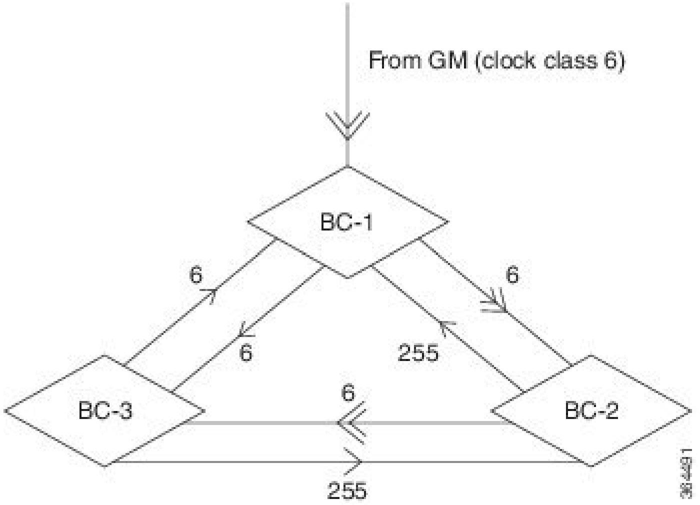
PTP Ring topology is designed by using Hop-By-Hop configuration of PTP boundary clocks. In this topology, each BC selects its adjacent nodes as PTP Server clocks, instead of using the same GM as the PTP server. These PTP BC server clocks are traceable to the GM in the network. Timing loop are not formed between adjacent BC nodes. The hot Standby BMCA configuration is used for switching to next the best server during failure.

Prerequisites

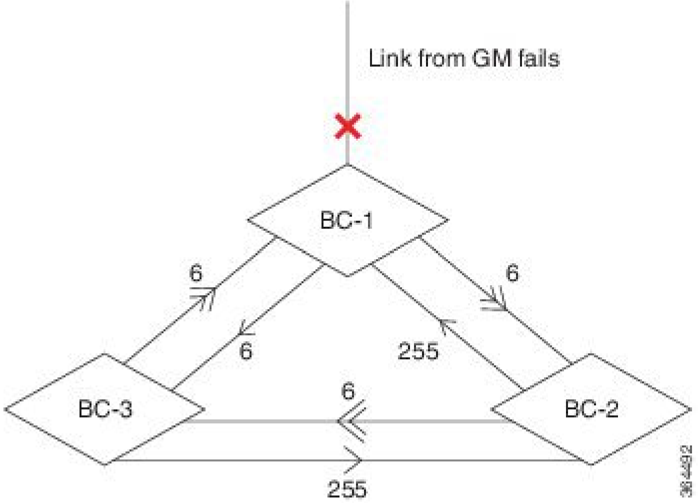
- PTP boundary clock configuration is required on all clock nodes in the ring, except the server clock nodes (GM), which provide the clock timing to ring. In the above example (see Figure 5-1) nodes S1 ... S5 must be configured as BC.
- The server clock (GM1 and GM2 in Figure 5-1) nodes in the ring can be either a OC server or BC server.
- Instead of each BC using same the GM as a PTP server, each BC selects its adjacent nodes as PTP server clocks. These PTP BC-server clocks are traceable to the GM in the network.
- Boundary clock nodes must be configured with the **single-hop** keyword in the PTP configuration to ensure that a PTP node can communicate with it’s adjacent nodes only.

Restrictions

- Timing loops should not exist in the topology. For example, if for a node there are two paths to get the same clock back, then the topology is not valid. Consider the following topology and configuration.



The paths with double arrows (>>) are the currently active clock paths and paths with single arrow (>) are redundant clock path. This configuration results in a timing loop if the link between the BC-1 and GM fails.



- In a BC configuration, the same loopback interface should never be used for both Server and Client port configuration.
- **Single-hop** keyword is not supported for PTP over MPLS with explicit null configuration. The Single-hop keyword is not supported when PTP packets are sent out with a MPLS tag.

On-Path Support Topology Scenario

Consider the topology as shown in Figure 5-1.

Figure 2: PTP Ring Topology—On-Path Support

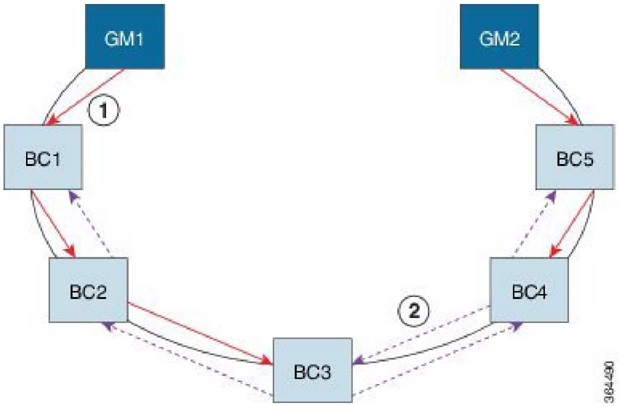


Table 3: PTP Ring Topology—On-Path Support

Clock Node	Behavior in the PTP Ring
GM1	Grandmaster Clock
GM2	Grandmaster Clock
BC1	Server Clocks: M1 (1st), BC2 (2nd) Client Clocks: BC2
BC2	Server Clocks: BC1(1st), BC3 (2nd) Client Clocks: BC1, BC3
BC3	Server Clocks: BC2 (1st), BC4 (2nd) Client Clocks: BC2, BC4
BC4	Server Clocks: BC5 (1st), BC3 (2nd) Client Clocks: BC3, BC5
BC5	Server Clocks: M2(1st), BC4 (2nd) Client Clocks: BC4

Now consider there is a failure between BC1 and BC2 (see Figure 5-3). In this case, the BC2 cannot communicate with GM1. Node BC2 receives the clock from BC3, which in turn receives the clock from GM2.

Figure 3: Deployment in a Ring—On-Path Support (Failure)

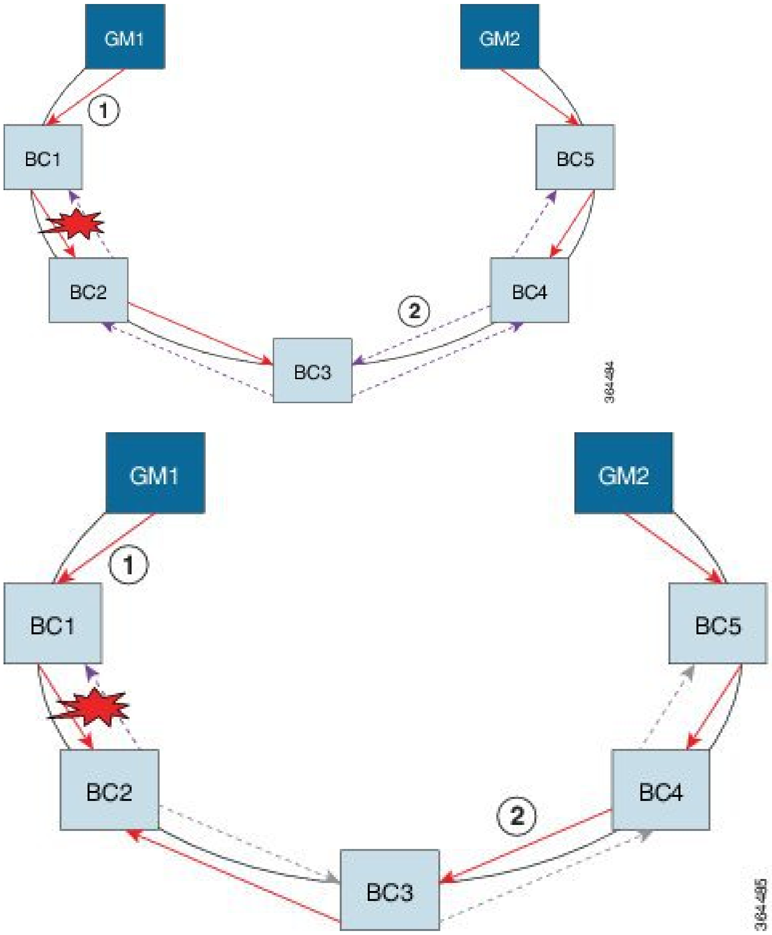


Table 4: PTP Ring Topology—On-Path Support (Failure)

Clock Node	Behavior in the PTP Ring[1]
GM1	Grandmaster Clock
GM2	Grandmaster Clock
BC1	Server Clocks: M1 (1st), BC2 (2nd) Client Clocks: BC2
BC2	Server Clocks: BC1(1st), BC3 (2nd) Client Clocks: BC1, BC3
BC3	Server Clocks: BC2 (1st), BC4 (2nd) Client Clocks: BC2, BC4
BC4	Server Clocks: BC5 (1st), BC3 (2nd) Client Clocks: BC3, BC5

Clock Node	Behavior in the PTP Ring[1]
BC5	Server Clocks: M2(1st), BC4 (2nd) Client Clocks: BC4

[1] Red indicates that GM is not traceable and there is no path to the client.

Configuration Example

PTP Ring boundary clocks must be configured with **single-hop** keyword in PTP configuration. The PTP node can communicate with its adjacent nodes only. This is required for PTP hop-by-hop ring topology.

```
ptp clock boundary domain 0
           clock-port client-port slave
               transport ipv4 unicast interface Lo0 negotiation single-hop
               clock source 10.0.0.1
               clock source 10.0.0.2 1
           clock-port server-port master
               transport ipv4 unicast interface Lo1 negotiation single-hop
.
.
```

Note The **single-hop** keyword is not supported for PTP over MPLS with explicit NULL configurations. The **single-hop** keyword is not supported when PTP packets are sent out with a MPLS tag.

For information on configuring PTP redundancy, see Configuring PTP Redundancy, on page 37.

BMCA

Starting Cisco IOS XE Release 3.15, BMCA is supported on the chassis.

The BMCA is used to select the server clock on each link, and ultimately, select the grandmaster clock for the entire Precision Time Protocol (PTP) domain. BCMA runs locally on each port of the ordinary and boundary clocks, and selects the best clock.

The best server clock is selected based on the following parameters:

- Priority—User-configurable value ranging from 0 to 255; lower value takes precedence
- Clock Class—Defines the traceability of time or frequency from the grandmaster clock
- Alarm Status—Defines the alarm status of a clock; lower value takes precedence

By changing the user-configurable values, network administrators can influence the way the grandmaster clock is selected.

BMCA provides the mechanism that allows all PTP clocks to dynamically select the best server clock (grandmaster) in an administration-free, fault-tolerant way, especially when the grandmaster clocks changes.

For information on configuring BMCA, see Configuring an Ordinary Clock, on page 17 and Configuring a Boundary Clock, on page 25.

Hybrid BMCA

In hybrid BMCA implementation, the phase is derived from a PTP source and frequency is derived from a physical lock source. More than one server clock is configured in this model and the best server clock is selected. If the physical clock goes down, then PTP is affected.

Configuration Example

Hybrid BMCA on Ordinary Clock

```
ptp clock ordinary domain 0 hybrid
 clock-port client-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 192.168.0.2
 clock source 172.16.0.2 1
 clock source 209.165.202.130 2

Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

Hybrid BMCA on Boundary Clock

```
ptp clock boundary domain 0 hybrid
 clock-port client-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 192.168.0.2
 clock source 172.16.0.2 1
 clock source 209.165.202.130 2
 clock-port server-port master
  transport ipv4 unicast interface Lo1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

Hybrid Clocking

The Cisco NCS 4206 Series Chassis support a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using the phase (ToD or 1 PPS) obtained using PTP. The combination of using physical source for frequency and PTP for time and phase improves the performance as opposed to using only PTP.

Note When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

For more information on how to configure hybrid clocking, see Configuring a Hybrid Clock, on page 29.

Transparent Clocking

A transparent clock is a network device such as 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 timing calculations. The transparent clock ports have no state because the transparent clock does not need to synchronize to the grandmaster clock.

There are two kinds of transparent clocks:

- End-to-end transparent clock—Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

- Peer-to-peer transparent clock— Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

Note The Cisco NCS 4206 Series Chassis does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco NCS 4206 Series Chassis as a transparent clock, see Configuring a Transparent Clock, on page 28.

Time of Day (TOD)

You can use the time of day (ToD) and 1PPS ports on the Cisco NCS 4206 Series Chassis to exchange ToD clocking. In server mode, the chassis can receive time of day (ToD) clocking from an external GPS unit; the chassis requires a ToD, 1PPS, and 10MHZ connection to the GPS unit.

In client mode, the chassis can recover ToD from a PTP session and repeat the signal on ToD and 1PPS interfaces.

For instructions on how to configure ToD on the Cisco NCS 4206 Series Chassis, see the Configuring an Ordinary Clock, on page 17.

Note On the RSP3 module, ToD port does not support the 1PPS feature. As a workaround, use the BNC connector in the ToD port to support the 1PPS feature.

Synchronizing the System Clock to Time of Day

You can set the chassis system time to synchronize with the time of day retrieved from an external GPS device. For information on how to configure this feature, see Synchronizing the System Time to a Time-of-Day Source, on page 42.

Timing Port Specifications

The following sections provide specifications for the timing ports on the Cisco NCS 4206 Series Chassis.

BITS Framing Support

The following table lists the supported framing modes for a BITS port.

Table 5: Framing Modes for a BITS Port on a Cisco NCS 4206 Chassis

BITS or SSU Port Support Matrix	Framing Modes Supported	SSM or QL Support	Tx Port	Rx Port
T1	T1 ESF	Yes	Yes	Yes
T1	T1 SF	No	Yes	Yes
E1	E1 CRC4	Yes	Yes	Yes

BITS or SSU Port Support Matrix	Framing Modes Supported	SSM or QL Support	Tx Port	Rx Port
E1	E1 FAS	No	Yes	Yes
2048 kHz	2048 kHz	No	Yes	Yes

The BITS port behaves similarly to the T1/E1 ports on the T1/E1 interface module; for more information about configuring T1/E1 interfaces, see the *Configuring T1/E1 Interfaces* document.

Understanding Synchronous Ethernet ESMC and SSM

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 chassis synchronizes to the best available clock source. If no better clock sources are available, the chassis remains synchronized to the current clock source.

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

For more information about Ethernet ESMC and SSM, see Configuring Synchronous Ethernet ESMC and SSM, on page 44.

Note The chassis can only operate in one clock selection mode at a time.

Note PTP clock sources are not supported with synchronous Ethernet.

Clock Selection Modes

The chassis supports two clock selection modes, which are described in the following sections.

QL-Enabled Mode

In QL-enabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock quality level (QL)
- Clock availability
- Priority

QL-Disabled Mode

In QL-disabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock availability
- Priority

Note You can use override the default clock selection using the commands described in the Managing Clock Source Selection, on page 49.

Note 8275.1 profile does not support QL-disabled mode on RSP3.

Managing Clock Selection

You can manage clock selection by changing the priority of the clock sources; you can also influence clock selection by modifying modify the following clock properties:

- Hold-Off Time: If a clock source goes down, the chassis waits for a specific hold-off time before removing the clock source from the clock selection process. By default, the value of hold-off time is 300 ms.
- Wait to Restore: The amount of time that the chassis waits before including a newly active synchronous Ethernet clock source in clock selection. The default value is 300 seconds.
- Force Switch: Forces a switch to a clock source regardless of clock availability or quality.
- Manual Switch: Manually selects a clock source, provided the clock source has a equal or higher quality level than the current source.

For more information about how to use these features, see Managing Clock Source Selection, on page 49.

Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the chassis:

Configuring an Ordinary Clock

The following sections describe how to configure the chassis as an ordinary clock.

Configuring a Server Ordinary Clock

Follow these steps to configure the chassis to act as a Server ordinary clock.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters configuration mode.

Step 3 **platformptp masterprtc-only-enable**

Example:

```
Router(config)# platform ptp master prtc-only-enable
```

(Optional) Enable port deletion of the server clock.

Step 4 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number*

Example:

```
Router(config)# ptp clock ordinary domain 0
```

Example:

```
Router(config-ptp-clk)#
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream.
- e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at client.

Step 5 **priority1** *priorityvalue*

Example:

```
Router(config-ptp-clk)# priority1 priorityvalue
```

Sets the preference level for a clock. client devices use the priority1 value when selecting a server clock: a lower priority1 value indicates a preferred clock. The priority1 value is considered above all other clock attributes.

Valid values are from 0-255. The default value is 128.

Step 6 **priority2** *priorityvalue*

Example:

```
Router(config-ptp-clk)# priority2 priorityvalue
```

Sets a secondary preference level for a clock. client devices use the priority2 value when selecting a server clock: a lower priority2 value indicates a preferred clock. The priority2 value is considered only when the chassis is unable to use priority1 and other clock attributes to select a clock.

Valid values are from 0-255. The default value is 128.

Step 7 **utc-offset** *value* **leap-second** *“date time”* **offset** {**-1** | **1**}

Example:

```
Router(config-ptp-clk)# utc-offset 45 leap-second “01-01-2017 00:00:00” offset 1
```

(Optional) Starting with Cisco IOS-XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value.

Valid values are from 0-255. The default value is 36.

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before.

- *“date time”*—Leap second effective date in dd-mm-yyyy hh:mm:ss format.

Step 8 input [1pps] {R0 | R1}

Example:

```
Router(config-ptp-clk)# input 1pps R0
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

Step 9 **tod** {**R0** | **R1**} {**ubx** | **nmea** | **cisco** | **ntp** | **cmcc**}

Example:

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

Note It is mandatory that when electrical ToD is used, the **utc-offset** command is configured before configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

Note The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

Step 10 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port server-port master
```

Defines a new clock port and sets the port to PTP Server or Client mode; in server mode, the port exchanges timing packets with PTP client devices.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 11 Do one of the following:

- **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*
- **transport ethernet unicast** [**negotiation**]

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

Step 12 exit

Exits clock-port configuration.

Step 13 **network-clock synchronization automatic**

Example:

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

Enables automatic selection of a clock source.

Note This command must be configured before any input source.

Step 14 **network-clock synchronization mode ql-enabled**

Example:

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

Step 15 Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

Example:

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

Step 16 **clock destination** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id}* | **interface** *interface-name*}

Example:

```
Router(config-ptp-port)# clock-source 10.8.8.1
```

Specifies the IP address or MAC address of a clock destination when the chassis is in PTP server mode.

Step 17 **sync interval** *interval*

Example:

```
Router(config-ptp-port)# sync interval -4
```

Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows:

- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second
- -4—1 packet every 1/16 seconds, or 16 packets per second.
- -5—1 packet every 1/32 seconds, or 32 packets per second.
- -6—1 packet every 1/64 seconds, or 64 packets per second.
- -7—1 packet every 1/128 seconds, or 128 packets per second.

Step 18 **announce interval** *interval*

Example:

```
Router(config-ptp-port)# announce interval 2
```

Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows:

- 3—1 packet every 8 seconds
- 2—1 packet every 4 seconds
- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second

Step 19 **end**

Example:

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

Exit configuration mode.

Step 20 linecode {ami | b8zs | hdb3}

Example:

```
 Router(config-controller)# linecode ami
```

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Example

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the Server or Client clocks:

```
ptp clock ordinary domain 24

local-priority 1

priority2 128
utc-offset 37
tod R0 cisco
clock-port server-port-1 master profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0/1
```

Configuring a Client Ordinary Clock

Follow these steps to configure the chassis to act as a client ordinary clock.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config)# ptp clock ordinary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

Step 4 **output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*]

Example:

```
Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

Note Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microseconds.

Step 5 **tod** {**R0** | **R1}** {**ubx** | **nmea** | **cisco** | **ntp** | **cmcc**}

Example:

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

Note The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

Step 6 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 7 Do one of the following:

- **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*

-
- **transport ethernet unicast** [**negotiation**]

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

Step 8 **clock source** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id*} | **interface** *interface-name*} [*priority*] [**delay-asymmetry** *delay asymmetry value* **nanoseconds**]

Example:

```
Router(config-ptp-port)# clock-source 10.8.8.1
```

Specifies the IP or MAC address of a PTP server clock.

- *priority*—Sets the preference level for a PTP clock.
- *delay asymmetry value*—Performs the PTP asymmetry readjustment on a PTP node to compensate for the delay in the network.

Step 9 **announce timeout** *value*

Example:

```
Router(config-ptp-port)# announce timeout 8
```

Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10.

Step 10 **delay-req interval** *interval*

Example:

```
Router(config-ptp-port)# delay-req interval 1
```

Configures the minimum interval allowed between PTP delay-request messages when the port is in the server state.

The intervals are set using log base 2 values, as follows:

- 3—1 packet every 8 seconds
- 2—1 packet every 4 seconds
- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second

- -4—1 packet every 1/16 seconds, or 16 packets per second.
- -5—1 packet every 1/32 seconds, or 32 packets per second.
- -6—1 packet every 1/64 seconds, or 64 packets per second.
- -7—1 packet every 1/128 seconds, or 128 packets per second.

Step 11 **end**

Example:

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

Exit configuration mode.

Step 12 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring a Boundary Clock

Follow these steps to configure the chassis to act as a boundary clock.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **Router(config)# ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config)# ptp clock boundary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP server to client clocks downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

Step 4 **time-properties persist** *value*

Example:

```
Router(config-ptp-clk)#
time-properties persist 600
```

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.

When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server clock is used.

Step 5 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 6 **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]*

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

Step 7 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.2
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

Step 8 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-port)# clock-port server-port master
```

Sets the clock port to PTP Server or Client mode; in server mode, the port exchanges timing packets with PTP client devices.

Note The server clock-port does not establish a clocking session until the client clock-port is phase aligned.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 9 **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]*

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

Step 10 **end**

Example:

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

Exit configuration mode.

Step 11 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.

- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

What to do next

Configuring a Transparent Clock

Follow these steps to configure the chassis as an end-to-end transparent clock.

Note The Cisco NCS 4206 Series Chassis does not support peer-to-peer transparent clock mode.

Note The transparent clock ignores the domain number.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config)# ptp clock e2e-transparent domain 4
```

Configures the chassis as an end-to-end transparent clock.

Step 4 **exit**

Example:

```
Router(config)# exit
```

Exit configuration mode.

Step 5 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring a Hybrid Clock

The following sections describe how to configure the chassis to act as a hybrid clock.

Configuring a Hybrid Boundary Clock

Follow these steps to configure a hybrid clocking in boundary clock mode.

Note When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**boundary**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config)# ptp clock boundary domain 0 hybrid
```

Configures the PTP clock. You can create the following clock types:

Note Hybrid mode is only supported with client clock-ports; server mode is not supported.

- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.

Step 4 **time-properties persist** *value*

Example:

```
Router(config-ptp-clk)# time-properties persist 600
```

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.

When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server is used.

Step 5 **utc-offset** *value* **leap-second** *"date time"* **offset** {**-1** | **1**}

Example:

```
Router(config-ptp-clk)# utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

(Optional) Starting with Cisco IOS XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value.

Valid values are from 0-255. The default value is 36.

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before.

- *"date time"*—Leap second effective date in dd-mm-yyyy hh:mm:ss format.

Step 6 **min-clock-class***value*

Example:

```
Router(config-ptp-clk)# min-clock-class 157
```

Sets the threshold clock-class value. This allows the PTP algorithm to use the time stamps from a upstream server clock, only if the clock-class sent by the server clock is less than or equal to the configured threshold clock-class.

Valid values are from 0-255.

Note Min-clock-class value is supported only for PTP with single server clock source configuration.

Step 7 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock.

Note Hybrid mode is only supported with client clock-ports; server mode is not supported.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 8 **transport ipv4** unicast **interface** *interface-type interface-number [***negotiationsingle-hop]**

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
or
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

negotiation—(Optional) configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

single-hop—(Optional)Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

Step 9 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.2
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

Step 10 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-port)# clock-port server-port master
```

Sets the clock port to PTP server or client mode; in server mode, the port exchanges timing packets with PTP client devices.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 11 **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***] [***single-hop]**

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation
or
Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

negotiation—(Optional)configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

single-hop—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

Step 12 **exit**

Exit clock-port configuration.

Step 13 **network-clock synchronization automatic**

Example:

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

Enables automatic selection of a clock source.

Note This command must be configured before any input source.

Step 14 **network-clock synchronization mode ql-enabled**

Example:

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

Step 15 Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

Example:

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

Step 16 **network-clock synchronization input-threshold** *ql value*

Example:

```
Router(config)# network-clock synchronization input-threshold <ql value>
```

(Optional) Starting with Cisco IOS-XE Release 3.18SP, this new CLI is used to set the threshold QL value for the input frequency source. The input frequency source, which is better than or equal to the configured threshold QL value, will be selected to recover the frequency. Otherwise, internal clock is selected.

Step 17 **network-clock hold-off** {**0** | *milliseconds*}

Example:

```
Router(config)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the chassis waits when a synchronous Ethernet clock source fails before taking action.

Note You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

For more information about this command, see Configuring Clocking and Timing, on page 3

Step 18 **platformptpmasteralways-on**

Example:

```
Router(config)# platform ptp master always-on
```

(Optional) Keeps the server port up all the time. So, when the frequency source has acceptable QL, the egress packets are sent to the downstream clients even when the server port is not phase aligned.

Step 19 **platformptphybrid-bcdownstream-enable**

Example:

```
Router(config)# platform ptp hybrid-bc downstream-enable
```

(Optional) Enables bust mode. When the difference between the forward timestamp of the previous packet and current packet is greater than 100ns, such timestamps are not provided to the APR. Due to this setting, the APR does not see unexpected and random time jumps in two sequential timestamps of the same PTP message-types. The same applies for the reverse path timestamps as well.

Step 20 **end**

Example:

```
Router(config)# end
```

Exit configuration mode.

Step 21 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.

- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring a Hybrid Ordinary Clock

Follow these steps to configure a hybrid clocking in ordinary clock client mode.

Note When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config)# ptp clock ordinary domain 0 hybrid
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.

  Note Hybrid mode is only supported with client clock-ports; server mode is not supported.

- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

Step 4 **output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*]

Example:

```
Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

Note Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microseconds.

Step 5 **tod** {**R0** | **R1**} {**ubx** | **nmea** | **cisco** | **ntp** | **cmcc**}

Example:

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

Note The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

Step 6 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

Note Hybrid mode is only supported with client clock-ports; server mode is not supported.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 7 **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

Step 8 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.2
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.

- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

Step 9 **exit**

Example:

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

Exit clock-port configuration.

Step 10 **network-clock synchronization automatic**

Example:

```
Router(config-ptp-clk)# network-clock synchronization automatic
```

Enables automatic selection of a clock source.

Note This command must be configured before any input source.

Step 11 **network-clock synchronization mode ql-enabled**

Example:

```
Router(config-ptp-clk)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

For more information about this command, see Configuring Clocking and Timing, on page 3

Step 12 Use one of the following options:

- network-clock input-source <priority> controller {SONET | wanphy}
- network-clock input-source <priority> external {R0 | R1} [10m | 2m]
- network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}]
- network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}}
- network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}]
- network-clock input-source <priority> interface <type/slot/port>

Example:

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

Step 13 **network-clock hold-off** {**0** | *milliseconds*}

Example:

```
Router(config-ptp-clk)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

Note You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

For more information about this command, see Configuring Clocking and Timing, on page 3

Step 14 **end**

Example:

```
Router(config-ptp-clk)# end
```

Exit configuration mode.

Step 15 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring PTP Redundancy

The following sections describe how to configure PTP redundancy on the chassis:

Configuring PTP Redundancy in Client Clock Mode

Follow these steps to configure clocking redundancy in client clock mode:

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

Example:

```
Router(config#) ptp clock ordinary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client clocks downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

Step 4 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 5 **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]**

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) **It ensures that the PTP node communicates only with the adjacent nodes.**

Step 6 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.2 1
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

Step 7 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.3 2
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

Step 8 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.4
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

Step 9 **end**

Example:

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

Exit configuration mode.

Step 10 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring PTP Redundancy in Boundary Clock Mode

Follow these steps to configure clocking redundancy in boundary clock mode:

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number*

Example:

```
Router(config)# ptp clock boundary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client clocks downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

Step 4 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 5 **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]**

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) Must beconfigured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

Step 6 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.2 1
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

Step 7 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.3 2
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

Step 8 **clock-source** *source-address [priority]*

Example:

```
Router(config-ptp-port)# clock source 192.168.0.4
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

Step 9 **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

Example:

```
Router(config-ptp-port)# clock-port server-port master
```

Specifies the address of a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

Note Using a telecom profile requires that the clock have a domain number of 4–23.

Step 10 **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]**

Example:

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

Note PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) Must be configured if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

Step 11 **end**

Example:

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

Exit configuration mode.

Step 12 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Synchronizing the System Time to a Time-of-Day Source

The following sections describe how to synchronize the system time to a time of day (ToD) clock source.

Synchronizing the System Time to a Time-of-Day Source (Server Mode)

Note System time to a ToD source (Server Mode) can be configured only when PTP server is configured. See Configuring a Server Ordinary Clock, on page 17. Select any one of the four available ToD format; cisco, nmea, ntp or ubx.10m must be configured as network clock input source.

Follow these steps to configure the system clock to a ToD source in server mode.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*}

Example:

```
Router(config)# TOD-clock 2 gps R0/R1
```

In server mode, specify a GPS port connected to a ToD source.

Step 4 **exit**

Example:

```
Router(config)# exit
```

Exit configuration mode.

Step 5 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Synchronizing the System Time to a Time-of-Day Source (Client Mode)

Note System time to a ToD source (Client Mode) can be configured only when PTP client is configured. See Configuring a Client Ordinary Clock, on page 22.

Follow these steps to configure the system clock to a ToD source in client mode. In client mode, specify a PTP domain as a ToD input source.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enter configuration mode.

Step 3 **tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*}

Example:

```
Router(config)# TOD-clock 10 ptp domain 0
```

In client mode, specify a PTP domain as a ToD input source.

Step 4 Router(config)# **end**

Exit configuration mode.

Step 5 Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

Configuring Synchronous Ethernet ESMC and SSM

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

The following sections describe ESMC and SSM support on the router.

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the router.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **network-clock synchronization automatic**

Example:

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

Enables the network clock selection algorithm. This command disables the Cisco-specific network clock process and turns on the G.781-based automatic clock selection process.

Note This command must be configured before any input source.

Step 4 **network-clock eec** {**1** | **2**}

Example:

```
Router(config)# network-clock eec 1
```

Specifies the Ethernet Equipment Clock (EEC) type. Valid values are

- 1—ITU-T G.8262 option 1 (2048)
- 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)

Step 5 **network-clock synchronization ssm option** {**1** | **2** {**GEN1** | **GEN2**}}

Example:

```
Router(config)# network-clock synchronization ssm option 2 GEN2
```

Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:

- Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.
- Option 2 refers to G.781 synchronization option 2, which is designed for the United States.

- GEN1 specifies option 2 Generation 1 synchronization.
- GEN2 specifies option 2 Generation 2 synchronization.

Step 6 Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

Example:

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.
- (Optional) To nominate PTP as network clock input source.

Step 7 **network-clock synchronization mode ql-enabled**

Example:

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

Step 8 **network-clock hold-off** {**0** | *milliseconds*}

Example:

```
Router(config)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

Note You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

Step 9 **network-clock wait-to-restore** *seconds*

Example:

```
Router(config)# network-clock wait-to-restore 70
```

(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process.

Valid values are 0 to 86400 seconds. The default value is 300 seconds.

Note You can also specify a wait-to-restore value for an individual interface using the **network-clock wait-to-restore** command in interface mode.

Step 10 **network-clock revertive**

Example:

```
Router(config)# network-clock revertive
```

(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the **no** form of this command.

Step 11 **esmc process**

Example:

```
Router(config)# esmc process
```

Enables the ESMC process globally.

Step 12 **network-clock external** *slot/card/port* **hold-off** {**0** | *milliseconds*}

Example:

```
Router(config)# network-clock external 0/1/0 hold-off 0
```

Overrides the hold-off timer value for the external interface.

Step 13 **network-clock quality-level** {**tx** | **rx**} *value* {**controller** [**E1**| **BITS**] *slot/card/port* | external [**2m** | **10m** | **2048k** | **t1** | **e1**] }

Example:

```
Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4
```

Specifies a quality level for a line or external clock source.

The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:

- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
- Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

Step 14 **interface** *type number*

Example:

```
Router(config)# interface GigabitEthernet 0/0/1
```

Example:

```
Router(config-if)#
```

Enters interface configuration mode.

Step 15 **synchronous mode**

Example:

```
Router(config-if)# synchronous mode
```

Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.

Step 16 network-clock source quality-level *value* {**tx** | **rx**}

Example:

```
Router(config-if)# network-clock source quality-level QL-PrC tx
```

Applies quality level on sync E interface.

The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:

- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
- Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

Step 17 **esmc mode** [**ql-disabled** | **tx** | **rx**] *value*

Example:

```
Router(config-if)# esmc mode rx QL-STU
```

Enables the ESMC process at the interface level. The **no** form of the command disables the ESMC process.

Step 18 **network-clock hold-off** {*0* | *milliseconds*}

Example:

```
Router(config-if)# network-clock hold-off 0
```

(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.

Step 19 **network-clock wait-to-restore** *seconds*

Example:

```
Router(config-if)# network-clock wait-to-restore 70
```

(Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.

Step 20 **end**

Example:

```
Router(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

You can use the **show network-clocks** command to verify your configuration.

Managing Clock Source Selection

The following sections describe how to manage the selection on the chassis:

Specifying a Clock Source

The following sections describe how to specify a synchronous Ethernet clock source during the clock selection process:

Selecting a Specific Clock Source

To select a specific interface as a synchronous Ethernet clock source, use the network-clock switch manual command in global configuration mode.

Note The new clock source must be of higher quality than the current clock source; otherwise the chassis does not select the new clock source.

Command	Purpose
network-clock switch manual external R0 | **R1** {{**E1** {**crc4** | **cas** |**fas**}} {**T1** {**d4** | **sf** | **esf**}} } `Router# network-clock switch manual external r0 e1 crc4`	Manually selects a synchronization source, provided the source is available and is within the range.

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Forcing a Clock Source Selection

To force the chassis to use a specific synchronous Ethernet clock source, use the **network-clock switch force** command in global configuration mode.

Note This command selects the new clock regardless of availability or quality.

Note Forcing a clock source selection overrides a clock selection using the **network-clock switch manual command.**

Command	Purpose
network-clock switch force external R0 | **R1** {{**E1** {**crc4** | **cas** |**fas**}} {**T1** {**d4** | **sf** | **esf**}} } `Router# network-clock switch force r0 e1 crc4`	Forces the chassis to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Disabling Clock Source Specification Commands

To disable a **network-clock switch manual** or **network-clock switch force** configuration and revert to the default clock source selection process, use the **network-clock clear switch** command.

Command	Purpose

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Disabling a Clock Source

The following sections describe how to manage the synchronous Ethernet clock sources that are available for clock selection:

Locking Out a Clock Source

To prevent the chassis from selecting a specific synchronous Ethernet clock source, use the network-clock set lockout command in global configuration mode.

Command	Purpose

network-clock set lockout {**interface** *interface_name slot/card/port* | **external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**]}}
`Router# network-clock set lockout interface GigabitEthernet 0/0/0`
	Prevents the chassis from selecting a specific synchronous Ethernet clock source.

network-clock clear lockout {**interface** *interface_name slot/card/port* | **external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**] }
`Router# network-clock clear lockout interface GigabitEthernet 0/0/0`
	Disable a lockout configuration on a synchronous Ethernet clock source.

Restoring a Clock Source

To restore a clock in a lockout condition to the pool of available clock sources, use the **network-clock clear lockout** command in global configuration mode.

Command	Purpose

network-clock clear lockout {**interface** *interface_name slot/card/port* | **external external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**] }
`Router# network-clock clear lockout interface GigabitEthernet 0/0/0`
	Forces the chassis to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

Verifying the Configuration

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

- show esmc—Displays the ESMC configuration.
- **show esmc detail**—Displays the details of the ESMC parameters at the global and interface levels.
- show network-clock synchronization—Displays the chassis clock synchronization state.
- show network-clock synchronization detail—Displays the details of network clock synchronization parameters at the global and interface levels.
- **show ptp clock dataset**
- **show ptp port dataset**
- **show ptp clock running**
- **show platform software ptpd statistics**
- **show platform ptp all**
- **show platform ptp tod all**

Troubleshooting

Table 6: SyncE Debug Commands , on page 51 list the debug commands that are available for troubleshooting the SyncE configuration on the chassis:

Caution We recommend that you do not use **debug** commands without TAC supervision.

Table 6: SyncE Debug Commands

Debug Command	Purpose
debug platform network-clock	Debugs issues related to the network clock including active-standby selection, alarms, and OOR messages.

Debug Command	Purpose
debug network-clock	Debugs issues related to network clock selection.
debug esmc error **debug esmc event** debug esmc packet [interface *interface-name*] debug esmc packet rx [interface *interface-name*] debug esmc packet tx [interface *interface-name*]	These commands verify whether the ESMC packets are transmitted and received with proper quality-level values.

Table 7: Troubleshooting Scenarios , on page 52 provides the information about troubleshooting your configuration

Table 7: Troubleshooting Scenarios

Problem	Solution
Clock selection	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Ensure that the nonrevertive configurations are in place. • Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists.
Incorrect QL values	• Ensure that there is no framing mismatch with the SSM option. • Reproduce the issue using the debug network-clock errors and debug network-clock event commands.
Alarms	• Reproduce the issue using the debug platform network-clock command enabled in the RSP. Alternatively, enable the debug network-clock event and debug network-clock errors commands.
Incorrect clock limit set or queue limit disabled mode	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations. • Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm RSP commands.

Problem	Solution
Incorrect QL values when you use the **show network-clock synchronization detail** command.	• Use the **network clock synchronization SSM** (*option 1* |*option 2*) command to confirm that there is no framing mismatch. Use the **show run interface** command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1. • Reproduce the issue using the debug network-clock errors and debug network-clock event RSP commands.

Note Effective from Cisco IOS XE Everest 16.6.1, on RSP3 module, alarm notification is enabled on 900 watts DC power supply. There are 2 input feeds for 900 watts DC power supply, if one of the input voltage is lesser than the operating voltage, critical alarm is generated for that particular feed and clears (stops) once the voltage is restored but the power supply state remains in OK state as the other power supply is operationally up.

Configuration Examples

This section contains sample configurations for clocking features on the chassis.

Note This section contains partial chassis configurations intended to demonstrate a specific feature.

Note Effective from Cisco IOS XE 16.12.3, you can configure the warning and critical thresholds for offset between 1 nanosecond and 400 nanoseconds. Ensure that you configure the warning threshold lower than the critical threshold.

Ordinary Clock—Client

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 10.8.8.1
announce timeout 7
delay-req interval 100
```

Ordinary Clock —Client Mode (Ethernet)

```
ptp clock ordinary domain 0
clock-port Client slave
transport ethernet unicast
clock-source 1234.5678.90ab bridge-domain 2 5
```

Ordinary Clock—Server

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0 negotiation
```

Ordinary Clock—Server (Ethernet)

```
ptp clock ordinary domain 0
clock-port Server master
transport ethernet unicast
clock destination interface GigabitEthernet0/0/1
```

Unicast Configuration—Client Mode

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0
clock-source 10.8.8.1
```

Unicast Configuration—Client Mode (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Client slave
    transport ethernet unicast
      clock source 1234.5678.90ab bridge-domain 5 2
```

Unicast Configuration—Server Mode

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0
clock-destination 10.8.8.2
sync interval 1
announce interval 2
```

Unicast Configuration—Server Mode (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Server master
    transport ethernet unicast
      clock destination 1234.5678.90ab bridge-domain 5
```

Unicast Negotiation—Client

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 10.8.8.1
```

Unicast Negotiation—Client (Ethernet)

```
ptp clock ordinary domain 0
```

```
  clock-port Client slave
    transport ethernet unicast negotiation
      clock source 1234.5678.90ab bridge-domain 5 5
  clock-port Client1 slave
    transport ethernet unicast negotiation
      clock source 1234.9876.90ab interface gigabitethernet 0/0/4 2
```

Unicast Negotiation—Server

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0 negotiation
sync interval 1
announce interval 2
```

Unicast Negotiation—Server (Ethernet)

```
ptp clock ordinary domain 0
clock-port Server master
transport ethernet unicast negotiation
```

Boundary Clock

```
ptp clock boundary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 192.168.0.2
 clock-port Server master
  transport ipv4 unicast interface Loopback 1 negotiation
```

Transparent Clock

```
ptp clock e2e-transparent domain 0
```

Hybrid Clock—Boundary

```
ptp clock boundary domain 0 hybrid
 clock-port Client slave
  transport ipv4 unicast interface Loopback0 negotiation
  clock source 192.168.0.2
 clock-port Server master
  transport ipv4 unicast interface Loopback1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

Hybrid Clock—Client

```
ptp clock ordinary domain 0 hybrid
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 192.168.0.2

Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

PTP Redundancy—Client

```
ptp clock ordinary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 192.168.0.2 1
   clock source 10.55.55.55 2
   clock source 10.5.5.5
```

PTP Redundancy—Boundary

```
ptp clock boundary domain 0
clock-port Client slave
transport ipv4 unicast interface Loopback 0 negotiation
clock source 192.168.0.2 1
clock source 10.55.55.55 2
clock source 10.5.5.5
clock-port Server master
transport ipv4 unicast interface Lo1 negotiation
```

Hop-By-Hop PTP Redundancy—Client

```
ptp clock ordinary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation single-hop
  clock source 192.168.0.2 1
   clock source 10.55.55.55 2
   clock source 10.5.5.5
```

Hop-By-Hop PTP Redundancy—Boundary

```
ptp clock boundary domain 0
clock-port Client slave
transport ipv4 unicast interface Loopback 0 negotiation single-hop
clock source 192.168.0.2 1
clock source 10.55.55.55 2
clock source 10.5.5.5
clock-port Server master
transport ipv4 unicast interface Lo1 negotiation single-hop
```

Time of Day Source—Server

```
TOD-clock 10 gps R0/R1
```

Time of Day Source—Client

```
TOD-clock 10 ptp domain 0
```

Clock Selection Parameters

```
network-clock synchronization automatic
network-clock synchronization mode QL-enabled
network-clock input-source 1 ptp domain 3
```

ToD/1PPS Configuration—Server

```
network-clock input-source 1 external R010m
ptp clock ordinary domain 1
tod R0 ntp
input 1pps R0
clock-port Server master
transport ipv4 unicast interface loopback 0
```

ToD/1PPS Configuration—Client

```
ptp clock ordinary domain 1
tod R0 ntp
output 1pps R0 offset 200 pulse-width 20 μsec
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 33.1.1.
```

Show Commands

```
Router# show ptp clock dataset ?
  current          currentDS dataset
  default          defaultDS dataset
  parent           parentDS dataset
  time-properties  timePropertiesDS dataset
Router# show ptp port dataset ?
 foreign-master  foreignMasterDS dataset
 port            portDS dataset
Router# show ptp clock running domain 0
                      PTP Ordinary Clock [Domain 0]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         ACQUIRING      1              98405          296399         Track one
                               PORT SUMMARY
   PTP Master
Name               Tx Mode      Role         Transport    State        Sessions     Port
Addr
Client        unicast      slave              Lo0          Slave              1
10.8.8.8
                             SESSION INFORMATION
SLAVE [Lo0] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 10.8.8.8            296399     98405      0          0
Router#
Router# show platform software ptpd stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval 0
  Tx packets : 0,  Rx Packets : 169681
  Last Seq Number : 0,  Error Packets : 1272
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval : 0
  Tx packets : 84595, Rx Packets : 0
  Last Seq Number : 19059, Error Packets : 0
!output omitted for brevity
Current Data Set
  Offset from master :  0.4230440
  Mean Path Delay :  0.0
  Steps Removed 1
General Stats about this stream
```

```
  Packet rate : 0, Packet Delta (ns) : 0
  Clock Stream handle : 0, Index : 0
  Oper State : 6, Sub oper State : 7
  Log mean sync Interval : -5, log mean delay req int : -4
Router# show platform ptp all
Slave info  : [Loopback0][0x38A4766C]
--------------------------------
clock role          : SLAVE
Slave Port hdl      : 486539266
Tx Mode             : Unicast-Negotiation
Slave IP            : 10.4.4.4
Max Clk Srcs        : 1
Boundary Clock      : FALSE
Lock status         : HOLDOVER
Refcnt              : 1
Configured-Flags    : 0x7F - Clock Port Stream
Config-Ready-Flags  : Port Stream
-----------
PTP Engine Handle   : 0
Master IP           : 10.8.8.8
Local Priority      : 0
Set Master IP       : 10.8.8.8
Router#show platform ptp tod all
--------------------------------
ToD/1PPS Info for 0/0
--------------------------------
ToD CONFIGURED        : YES
ToD FORMAT            : NMEA
ToD DELAY             : 0
1PPS MODE             : OUTPUT
OFFSET                : 0
PULSE WIDTH           : 0
ToD CLOCK             : Mon Jan 1  00:00:00 UTC 1900
Router# show ptp clock running domain 0
                      PTP Boundary Clock [Domain 0]
State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  2              32355          159516         Hot standby
PORT SUMMARY

  PTP Master
Name               Tx Mode      Role         Transport State        Sessions Port Addr

SLAVE              unicast      slave        Ethernet                             1
  10.9.9.1
MASTER             unicast      master       Ethernet  -                 2            -
                             SESSION INFORMATION

SLAVE [Ethernet] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs

 10.9.9.1            159083     31054      0          0

MASTER [Ethernet] [Sessions 2]
 Peer addr                             Pkts in    Pkts out   In Errs    Out Errs
 aabb.ccdd.ee01 [Gig0/2/3]                 223        667        0          0
 aabb.ccdd.ee02 [BD 1000]                    210        634        0          0
```

Input Synchronous Ethernet Clocking

The following example shows how to configure the chassis to use the BITS interface and two Gigabit Ethernet interfaces as input synchronous Ethernet timing sources. The configuration enables SSM on the BITS port.

```
!
```

```
Interface GigabitEthernet0/0
    synchronous mode
    network-clock wait-to-restore 720
!
Interface GigabitEthernet0/1
    synchronous mode
!
!
network-clock synchronization automatic
network-clock input-source 1 External R0 e1 crc4
network-clock input-source 1 gigabitethernet 0/0
network-clock input-source 2 gigabitethernet 0/1
network-clock synchronization mode QL-enabled
no network-clock revertive
```

CHAPTER 3

Configuring Synchronous Ethernet ESMC and SSM

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

The following sections describe ESMC and SSM support on the Cisco ASR 903 Series Router.

Understanding Synchronous Ethernet ESMC and SSM

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

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

When configured to use synchronous Ethernet, the Cisco ASR 903 Series Router synchronizes to the best available clock source. If no better clock sources are available, the router remains synchronized to the current clock source.

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

Note The router can only operate in one clock selection mode at a time.

Note Conversely, PTP clock sources are not supported with synchronous Ethernet. However, you can use hybrid clocking to allow the router to obtain frequency using Synchronous Ethernet and phase using PTP.

Clock Selection Modes

The Cisco ASR 903 Series Router supports two clock selection modes, which are described in the following sections.

QL-Enabled Mode

In QL-enabled mode, the router considers the following parameters when selecting a clock source:

- Clock quality level (QL)
- Clock availability
- Priority

QL-Disabled Mode

In QL-disabled mode, the router considers the following parameters when selecting a clock source:

- Clock availability
- Priority

Note You can use override the default clock selection using the commands described in the Managing Clock Source Selection, on page 67.

Note 8275.1 profile does not support QL-disabled mode on RSP3.

Managing Clock Selection

You can manage clock selection by changing the priority of the clock sources; you can also influence clock selection by modifying modify the following clock properties:

- Hold-Off Time: If a clock source goes down, the router waits for a specific hold-off time before removing the clock source from the clock selection process. By default, the value of hold-off time is 300 ms.
- Wait to Restore: The amount of time that the router waits before including a newly active synchronous Ethernet clock source in clock selection. The default value is 300 seconds.
- Force Switch: Forces a switch to a clock source regardless of clock availability or quality.

- Manual Switch: Manually selects a clock source, provided the clock source has a equal or higher quality level than the current source.

For more information about how to use these features, see Managing Clock Source Selection, on page 67.

Restrictions and Usage Guidelines

The following restrictions apply when configuring synchronous Ethernet SSM and ESMC:

- To use the **network-clock synchronization ssm option** command, ensure that the router configuration does not include the following:
    - Input clock source
    - Network clock quality level
    - Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is not a network clocking configuration applied to sychronous Ethernet interfaces, BITS interfaces, and timing port interfaces.
- SSM and ESMC are SSO-coexistent, but not SSO-compliant. The router goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.
- It is recommended that you do not configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).
- You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.
- Copper SFP is *not* supported for SyncE Rx and Tx on the uplink interfaces. SyncE Rx and Tx is supported on the uplink interfaces only for fiber SFP only.

The following restrictions apply when configuring synchronous Ethernet and PTP:

- We recommend configuring SyncE and PTP on the same interface to prevent endless timing loops.
- When you have not configured a redundant secondary node for SyncE, we recommend that you explicitly configure the SyncE source node as master.

Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the Cisco ASR 903 Series Router.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **network-clock synchronization automatic**

Example:

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

Enables the network clock selection algorithm. This command disables the Cisco-specific network clock process and turns on the G.781-based automatic clock selection process.

Note This command must be configured before any input source.

Step 4 **network-clock eec** {**1** | **2**}

Example:

```
Router(config)# network-clock eec 1
```

Specifies the Ethernet Equipment Clock (EEC) type. Valid values are

- 1—ITU-T G.8262 option 1 (2048)
- 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)

Step 5 **network-clock synchronization ssm option** {**1** | **2** {**GEN1** | **GEN2**}}

Example:

```
Router(config)# network-clock synchronization ssm option 2 GEN2
```

Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:

- Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.
- Option 2 refers to G.781 synchronization option 2, which is designed for the United States.
- GEN1 specifies option 2 Generation 1 synchronization.
- GEN2 specifies option 2 Generation 2 synchronization.

Step 6 **network-clock input-source** *priority* {**interface** *interface_name slot*/*card*/*port* | **ptp domain** *domain_num* | {**external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**} **line-build-out** *length*} | **e1** [**crc4** | **fas**] [**125ohm** | **75ohm**] **linecode** [**hdb3** | **ami**] } | **10m**] }}

Example:

```
Router(config)# network-clock input-source 1 interface GigabitEthernet 0/0/1
```

Enables you to select an interface as an input clock for the router. You can select the BITS, Gigabit Ethernet 0/0, Gigabit Ethernet 0/1 interfaces, or GPS interfaces, or an external interface.

Note Before configuring ethernet intreface as clock source, you should configure synchronous mode under interface configuration.

Step 7 **network-clock synchronization mode ql-enabled**

Example:

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

Note This command is disabled by default.

Step 8 **network-clock hold-off** {**0** | *milliseconds*} *global*

Example:

```
Router(config)# network-clock hold-off 0 global
```

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

Note You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

Step 9 **network-clock wait-to-restore** *seconds global*

Example:

```
Router(config)# network-clock wait-to-restore 70 global
```

(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process.

Valid values are 0 to 86400 seconds. The default value is 300 seconds.

Note You can also specify a wait-to-restore value for an individual interface using the **network-clock wait-to-restore** command in interface mode.

Step 10 **network-clock revertive**

Example:

```
Router(config)# network-clock revertive
```

(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the **no** form of this command.

Step 11 **esmc process**

Example:

```
Router(config)# esmc process
```

Enables the ESMC process globally.

Step 12 **network-clock external** [*r0* / *r1* **hold-off** {**0** | **milliseconds**}

Example:

```
Router(config)# network-clock external r0 hold-off 0
```

Overrides the hold-off timer value for the external interface.

Step 13 **network-clock quality-level** {**tx** | **rx**} *value* {**interface** *interface-name slot/card/port* | **controller** [**E1**| **BITS**] *slot/card/port* | external [**2m** | **10m**] }

Example:

```
Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4
```

Specifies a quality level for a line or external clock source.

The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:

- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
- Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

Step 14 **interface** *type number*

Example:

```
Router(config)# interface GigabitEthernet 0/0/1
```

Example:

```
Router(config-if)#
```

Enters interface configuration mode.

Step 15 **synchronous mode**

Example:

```
Router(config-if)# synchronous mode
```

Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.

Step 16 **esmc mode** [**ql-disabled** | **tx** | **rx**] *value*

Example:

```
Router(config-if)# esmc mode rx QL-STU
```

Enables the ESMC process at the interface level. The **no** form of the command disables the ESMC process.

Step 17 **network-clock hold-off** {*0* | *milliseconds*}

Example:

```
Router(config-if)# network-clock hold-off 0
```

(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.

Step 18 **network-clock wait-to-restore** *seconds*

Example:

```
Router(config-if)# network-clock wait-to-restore 70
```

(Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.

Step 19 **end**

Example:

```
Router(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

You can use the **show network-clocks** command to verify your configuration.

Managing Clock Source Selection

The following sections describe how to manage the selection on the Cisco ASR 903 Series Router:

Specifying a Clock Source

The following sections describe how to specify a synchronous Ethernet clock source during the clock selection process:

Selecting a Specific Clock Source

To select a specific interface as a synchronous Ethernet clock source, use the network-clock switch manual command in global configuration mode.

Note The new clock source must be of higher quality than the current clock source; otherwise the router does not select the new clock source.

Command	Purpose
network-clock switch manual external R0 | **R1** {{**E1** {**crc4** | **cas** |**fas**}} {**120ohms** | **75ohms** | **t0**}} } `Router# network-clock switch manual external r0 e1 crc4 120ohms t0`	Manually selects a synchronization source, provided the source is available and is within the range.

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Forcing a Clock Source Selection

To force the router to use a specific synchronous Ethernet clock source, use the **network-clock switch force** command in global configuration mode.

Note This command selects the new clock regardless of availability or quality.

Note Forcing a clock source selection overrides a clock selection using the **network-clock switch manual command.**

Command	Purpose
network-clock switch force external R0 | **R1** {{**E1** {**crc4** | **cas** |**fas**}} {**120ohms** {**75ohms** | **t0** }} } `Router# network-clock switch force r0 e1 crc4 120ohms t0`	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Disabling Clock Source Specification Commands

To disable a **network-clock switch manual** or **network-clock switch force** configuration and revert to the default clock source selection process, use the **network-clock clear switch** command.

Command	Purpose

network-clock clear switch {**t0** | **external** *slot/card/port* [**10m** | **2m**]}
`Router# network-clock clear switch t0`
	Disable a clock source selection.

Disabling a Clock Source

The following sections describe how to manage the synchronous Ethernet clock sources that are available for clock selection:

Locking Out a Clock Source

To prevent the router from selecting a specific synchronous Ethernet clock source, use the network-clock set lockout command in global configuration mode.

Command	Purpose

network-clock set lockout {**interface** *interface_name slot/card/port* | **external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**]}}
`Router# network-clock set lockout interface GigabitEthernet 0/0/0`
	Prevents the router from selecting a specific synchronous Ethernet clock source.

network-clock clear lockout {**interface** *interface_name slot/card/port* | **external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**] }
`Router# network-clock clear lockout interface GigabitEthernet 0/0/0`
	Disable a lockout configuration on a synchronous Ethernet clock source.

Restoring a Clock Source

To restore a clock in a lockout condition to the pool of available clock sources, use the **network-clock clear lockout** command in global configuration mode.

Command	Purpose

network-clock clear lockout {**interface** *interface_name slot/card/port* | **external external** {**R0** | **R1** [{ **t1** {**sf** | **esf** } **linecode** {**ami** | **b8zs**}} | **e1** [**crc4** | **fas**] **linecode** [**hdb3** | **ami**] }
`Router# network-clock clear lockout interface GigabitEthernet 0/0/0`
	Forces the router to use a specific synchronous Ethernet clock source, regardless of clock quality or availability.

Verifying the Configuration

You can use the following commands to verify your configuration:

- show esmc—Displays the ESMC configuration.
- **show esmc detail**—Displays the details of the ESMC parameters at the global and interface levels.

- show network-clock synchronization—Displays the router clock synchronization state.
- show network-clock synchronization detail—Displays the details of network clock synchronization parameters at the global and interface levels.

Troubleshooting

Table 8: SyncE Debug Commands , on page 70 list the debug commands that are available for troubleshooting the SyncE configuration on the Cisco ASR 903 Series Router:

⚠

Caution We recommend that you do not use **debug** commands without TAC supervision.

Table 8: SyncE Debug Commands

Debug Command	Purpose
debug platform network-clock	Debugs issues related to the network clock including active-standby selection, alarms, and OOR messages.
debug network-clock	Debugs issues related to network clock selection.
debug esmc error **debug esmc event** debug esmc packet [interface *interface-name*] debug esmc packet rx [interface *interface-name*] debug esmc packet tx [interface *interface-name*]	These commands verify whether the ESMC packets are transmitted and received with proper quality-level values.

Table 9: Troubleshooting Scenarios , on page 70 provides the information about troubleshooting your configuration

Table 9: Troubleshooting Scenarios

Problem	Solution
Clock selection	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Ensure that the nonrevertive configurations are in place. • Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists.
Incorrect QL values	• Ensure that there is no framing mismatch with the SSM option. • Reproduce the issue using the debug network-clock errors and debug network-clock event commands.
Alarms	• Reproduce the issue using the debug platform network-clock command enabled in the RSP. Alternatively, enable the debug network-clock event and debug network-clock errors commands.

Problem	Solution
Incorrect clock limit set or queue limit disabled mode	• Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command. • Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations. • Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm RSP commands.
Incorrect QL values when you use the **show network-clock synchronization detail** command.	• Use the **network clock synchronization SSM** (*option 1* |*option 2*) command to confirm that there is no framing mismatch. Use the **show run interface** command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1. • Reproduce the issue using the debug network-clock errors and debug network-clock event RSP commands.

Configuration Examples

Example: Input Synchronous Ethernet Clocking

The following example shows how to configure the router to use the BITS interface and two Gigabit Ethernet interfaces as input synchronous Ethernet timing sources. The configuration enables SSM on the BITS port.

```
!
Interface GigabitEthernet0/0
    synchronous mode
    network-clock wait-to-restore 720
!
Interface GigabitEthernet0/1
    synchronous mode
!
!
network-clock synchronization automatic
network-clock input-source 1 External R0 e1 crc4
network-clock input-source 1 gigabitethernet 0/0
network-clock input-source 2 gigabitethernet 0/1
network-clock synchronization mode QL-enabled
no network-clock revertive
```

SSM Support on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 Interface Module

SSM is carried over OC-3 and OC-12 optical links. Effective Cisco IOS-XE release 3.18 SP, the SSM is transported in the S1 byte when it is carried over an optical line for SONET and SDH. The SSM messages enable SONET and SDH devices to select the highest quality timing reference automatically and avoid the timing loops.

SSM is supported on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 Module. It has four ports and the default rate is OC-3. OC-3 rate is supported on all the four ports and OC-12 rate is supported on first port only.

S1 Byte

The SSM is transported in the S1 byte when it is carried over an optical line for SONET and SDH. S1 byte resides in Multiplex Section Overhead (MSOH) in SDH frame. The last four bits (5 to 8) carries SSM information.

Supported Quality Levels

The quality levels supported for SDH framing mode are:

- QL-PRC
- QL-SSU-A
- QL-SSU-B
- QL-SEC (SDH equipment clock)
- QL-DNU

The quality levels supported for SONET framing mode are:

- GEN1—PRS, STU, ST2, ST3, SMC, ST4, and DUS
- GEN2—PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, and DUS

Configuring SSM on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 IM

```
enable
configure terminal
network-clock synchronization automatic
network-clock eec 1
network-clock synchronization ssm option 2 GEN2
controller SONET 0/0/0
framing sdh
network-clock input-source 10 controller SONET 0/5/1
network-clock synchronization mode ql-enabled
network-clock hold-off 0
network-clock wait-to-restore 70
network-clock revertive
network-clock quality-level tx ql-prC controller SONET 0/0/0
network-clock quality-level rx ql-ssu-a controller SONET 0/5/1
network-clock hold-off 0 global
network-clock wait-to-restore 70
end
```

Configuring Clock Source

```
enable
configure terminal
controller sonet 0/5/0
clock source line
end
```

Verification of SSM Configuration

Use the **show network-clocks synchronization** command to verify the SSM configuration on Cisco ASR 900 Series 4-Port OC3/STM1 or 1-Port OC12/STM4 IM:

```
Router#show network-clocks synchronization
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : TenGigabitEthernet0/3/0
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : Yes

Nominated Interfaces

Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*SONET 0/5/1          NA          NA/En        10    QL-PRC  NA        NA
Router#
```

SSM Support on Cisco 48-Port T3/E3 CEM Interface Module

Synchronization Status Message (SSM) is transported over T3 links using proprietary method. SSM enables T3 to select the highest quality timing reference automatically and avoid the timing loops.

SSM is supported on Cisco 48-Port T3/E3 CEM Interface Module.

Note Effective IOS XE Everest 16.5.1, E3 mode is not supported.

Supported Quality Levels

The quality levels supported on T3 are:

- GEN1—PRS, STU, ST2, ST3, SMC, ST4, and DUS
- GEN2—PRS, STU, ST2, TNC, ST3E, ST3, SMC, ST4, and DUS

Configuring SSM on Cisco 48-Port T3/E3 CEM Interface Module

```
enable
configure terminal
controller media-type controller 0/5/0
mode t3
controller t3 0/0/0
network-clock synchronization automatic
network-clock eec 1
network-clock synchronization ssm option 2 GEN2
network-clock input-source 10 controller t3 0/5/1
network-clock synchronization mode ql-enabled
network-clock hold-off 0
network-clock wait-to-restore 70
network-clock revertive
network-clock quality-level tx ql-prs controller t3 0/0/0
network-clock quality-level rx ql-st2 controller t3 0/5/1
network-clock hold-off 0
network-clock wait-to-restore 70
end
```

Configuring Clock Source

```
enable
configure terminal
controller media-type controller 0/5/0
mode t3
controller t3 0/5/0
clock source line
end
```

Verification of SSM Configuration

Use the **show network-clocks synchronization detail** command to verify the SSM configuration on Cisco 48-Port T3/E3 CEM Interface Module:

```
show network-clock synchronization detail
Symbols: En - Enable, Dis - Disable, Adis - Admin Disable
NA - Not Applicable
* - Synchronization source selected
# - Synchronization source force selected
& - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 1544 (EEC-Option2)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : GEN1
T0 : T3 0/0/21
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 1
Squelch Threshold: QL-ST3
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (begin)-> 2A (ql_mode_enable)-> 1A (src_added)-> 1A (ql_change)->
```

```
 1A (sf_change)-> 1A (ql_change)-> 1A


Nominated Interfaces

Interface SigType Mode/QL Prio QL_IN ESMC Tx ESMC Rx
Internal NA NA/Dis 251 QL-ST3 NA NA
*T3 0/0/21 NA NA/En 2 QL-PRS NA NA

Interface:
---------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-ST3
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms: None
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0
Description: None

Local Interface: T3 0/0/21
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: ENABLED
SSM Rx: ENABLED
Priority: 2
QL Receive: QL-PRS
QL Receive Configured: QL-PRS
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms: None
Slot Disabled: FALSE
SNMP input source index: 8
SNMP parent list index: 0
Description: None
```

CHAPTER 4

Configuring the Global Navigation Satellite System

The chassis uses a satellite receiver, also called the global navigation satellite system (GNSS), as a new timing interface.

In typical telecom networks, synchronization works in a hierarchal manner where the core network is connected to a stratum-1 clock and this 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 satellites in sky using an on-board GPS chips.

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

Information About the GNSS

Overview of the GNSS Module

The GNSS module is present on the front panel of the RSP3 module and can be ordered separately with PID=. However, there is no license required to enable the GNSS module.

The GNSS LED on the RSP3 front panel indicates the status of the module. The following table explains the different LED status.

LED Status	Description
Green	GNSS Normal State. Self survey is complete.

LED Status	Description
Amber	All other states

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 The RSP3 module 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.

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

Operation of the GNSS Module

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 minimum four different satellites and computes approximately 2000 different positions of the satellites to obtain a 3-D location (Latitude, Longitude, and Height) of it current position. This operation takes about 35-to-40 minutes. During this stage also, the module is 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. If you want to change the tracking data, use the **no shutdown** command to set the GNSS interface to its default value.

The GNSS module stays in the OD mode unless 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 only in the OD mode.

Note GLONASS and BeiDou satellites cannot be enabled simultaneously. GALILEO is not supported.

When the router is reloaded, it always comes up in the 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 m from it's pre-reloaded condition.

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

High Availability for GNSS

The chassis has two GNSS modules, one each on the active and standby RSP3 modules. Each GNSS module must have a separate connection to the antenna in case of an RSP3 switchover.

Firmware Upgrade

GNSS firmware is integrated into the Cisco IOS XE Everest 16.5.1 image. When you load this image, the GNSS firmware is copied to the `/usr/binos/bin/` directory.

If the version of the firmware in the software image is greater than the current running verison, firmware is automatically upgraded.

Points to Note During Upgrade

- During firmware upgrade, the GNSS module status is displayed as *not detected* and lock status as *disabled*.
- After firmware upgrade is complete or if firmware upgrade is not required, firmware upgrade progress in the show command is displayed as *NA (Not-Applicable)*.
- Syslog messages are displayed to indicate the firmware upgrade start, cancel, and finish states.
- While firmware upgrade is in progress, GNSS configuration is not allowed.
- To display the status of the firmware ugrade or downgrade, use the **show platform hardware slot** *R0/R1* **network-clock | sec GNSS** or the **show gnss status** commands.

Prerequisites for GNSS

To use GNSS:

- 1PPS, 10 MHz, and ToD must be configured for netsync and PTP. For more information see the Configuring Clocking and Timing chapter .
- The antenna must have a clear view of the sky. For proper timing, minimum of four satellites should be locked. For information, see the *Cisco NCS 4206 Series Hardware Installation Guide* .

Restrictions for GNSS

- The GNSS module is not supported through SNMP; all configurations are performed through commands.
- On HA system, the traps from the standby system are logged to the console as the SNMP infra does not get enabled on standby RSP module.
- GNSS objects or performance counters are updated every 5 seconds locally and acknowledge the MIB object request accordingly.
- GNSS traps generation is delayed for 300 seconds for the first time after system startes to avoid any drop of GNSS traps.

GNSS MIB

The MIB file, CISCO-GNSS-MIB, has the following objects:

- **cGnssModuleLockStatus**: This object specifies the lock status of GNSS module. If the GNSS module is able to acquire and lock a set of satellites and provide a valid 10 M and 1 pps signal to the system, it indicates that the GNSS module is locked and its status is Up.

  Similarly, if it is not able to acquire or lock to the satellites or is unable to provide valid signals to the router where it is inserted, it indicates that the GNSS module is not locked and its status is Down.

GNSS Lock Status	Value
Down	1
Up	2

- **cGnssModulePresenceStatus**:

  This object specifies the presence of the GNSS module on system. Hence, if the GNSS module is present or inserted and if it is not present or removed from the router, the status is updated as Present or Absent.

GNSS Module	Value
Absent	1
Present	2

- **cGnssModuleSlotInfo**: This object specifies slot information where the GNSS module is inserted. It can be Slot-0 or Slot-1 for Cisco RSP3 Module and is Slot-0 for Cisco ASR-920-12SZ-IM and ASR-920U-12SZ-IM and Cisco ASR-920-12SZ-A and Cisco ASR-920-12SZ-D.
- **cGnssModuleSlotState**:

  This object specifies state of the RSP (active or standby) where the GNSS module is inserted.
- **cGnssSatelliteVisibilityStatus**:

  This object specifies the status of the GNSS satellite visibility (good or bad). If the tracking is minimum 3 satellites with more than 30 dBm, then GNSS satellite visibility is good, otherwise bad.

GNSS Module Satellite Visibility	Value
Bad	1
Good	2

- **cGnssModuleSatelliteCount**:

  This object specifies the total number of satellites tracked by GNSS module at that particular time.

- **cGnssModuleSvIdSNR**:

  This object specifies the SNR value and the satellite ID for each visible satellite. Satellite ID and SNR of satellites are formatted in a string as show below:

  ```
  "<SvID1:SNR SvID2:SNR …. SvID32:SNR>"
  ```

- **cGnssAntennaShortAlarmStatus**:

  This object specifies GNSS module antenna short alarm status. It is used as the antenna short alarm status identifier of the GNSS module. Notification generated for the antenna short alarm is Raise or Clear status.

Antenna Short Status	Value
Raise	1
Clear	2

- **cGnssAntennaOpenAlarmStatus**:

  This object specifies GNSS module antenna open alarm status. It is used as the antenna open alarm status identifier of the GNSS module. Notification generated for the antenna open alarm is Raise or Clear status.

Antenna Open Status	Value
Raise	1
Clear	2

Telemetry for GNSS Module

Table 10: Feature History

Feature Name	Release Information	Description
Telemetry for GNSS Module	Cisco IOS XE Amsterdam 17.3.1	This feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language. Prior to this release, the traditional show commands were available to only view the GNSS statistic data. But, you could not use these show command outputs to manage network devices as demanded by centralized orchestration application such as Cisco Digital Network Architecture Center (DNAC). The introduction of this feature provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language to bring more visibility in the timing services operations. This feature is supported on Cisco ASR 900 RSP3 module.

Any deployed network requires constant monitoring and troubleshooting facilities to spot issues and trends, and to resolve them. Thus, the network devices must expose the operational state and important events to provide network assurance. The GNSS module has various statistic data like module lock status, satellite count, survey progress, alarm status, and so on. Prior to Cisco IOS XE Amsterdam 17.3.x, you could only use the traditional show commands to view these statistic data. But, you could not use these show command outputs to manage network devices as demanded by centralized orchestration application such as Cisco Digital Network Architecture Center (DNAC).

Effective Cisco IOS XE Amsterdam 17.3.x, the telemetry feature for GNSS module is introduced that provides externalization of operational data using Network Configuration Protocol (NETCONF) or Yet Another Next Generation (YANG) data modeling language. This feature helps to bring more visibility in the timing services operations.

For more information on the Telemetry feature, see the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.1.x.

Restrictions

You cannot obtain the GNSS data from the standby RSP device for Cisco ASR900 RSP3 Module HA system.

GNSS Traps

- **GNSS Antenna Short Alarm Trap**:

  Once the GNSS module is inserted or powered on to the router and configured, the module detects if there is any antenna short present according to the power drawn from the module. If the power drawn is above the threshold level, it is notified as an antenna short alarm.

  A trap is generated when the GNSS module detects an antenna short alarm. Similarly, the trap is cleared when the antenna short alarm is cleared. This trap and its clearance are generated based on the antenna short alarm status reading from the GNSS module.

- **GNSS Antenna Open Alarm Trap**:

  Once the GNSS module is inserted or powered on to the router and configured, the module detects if there is any antenna open present according to the power drawn from the module. If the power drawn is below the threshold level, it is notified as an antenna open alarm.

  A trap is generated when the GNSS module detects an antenna open alarm. Similarly, the trap is cleared when the antenna open alarm is cleared. This trap and its clearance are generated based on the antenna open alarm status reading from the GNSS module.

- **GNSS Satellite Visibility Trap**:

  Once the GNSS module is inserted or powered on to the router and configured, it gets locked onto a set of satellites and provides valid 10 M and 1 pps signals to the system.

  Based on the following conditions, the satellite visibility condition is decided:

  - Number of satellites tracked is less than three
  - Signal strength of the tracked satellites is less than 30 dBm

  So, if more than 3 satellites are visible with more than 30 dBm, then it indicates the signal strength is good, else its bad. Traps are generated accordingly when the signal strength status changes between good and bad. This trap and its clearance are generated based on the signal strength status reading from the GNSS module.

Trap OID

When a trap is generated, it contains a unique OID for each trap that acts as primary key to identify a trap.

The following tables show the mapping of trap and clearance names to its OIDs:

Trap Name	OID
ciscoGnssModuleLockStatus	1.3.6.1.4.1.9.9.862.0.1
ciscoGnssModuleLockClear	1.3.6.1.4.1.9.9.862.0.2
ciscoGnssModulePresenceStatus	1.3.6.1.4.1.9.9.862.0.3

Trap Name	OID
ciscoGnssModulePresenceClear	1.3.6.1.4.1.9.9.862.0.4
ciscoGnssAntennaShortAlarmStatus	1.3.6.1.4.1.9.9.862.0.5
ciscoGnssAntennaShortAlarmClear	1.3.6.1.4.1.9.9.862.0.6
ciscoGnssAntennaOpenAlarmStatus	1.3.6.1.4.1.9.9.862.0.7
ciscoGnssAntennaOpenAlarmClear	1.3.6.1.4.1.9.9.862.0.8
ciscoGnssSatelliteVisibilityStatus	1.3.6.1.4.1.9.9.862.0.9
ciscoGnssSatelliteVisibilityClear	1.3.6.1.4.1.9.9.862.0.10

Objects/Performance Counters	
cGnssModuleLockStatus	1.3.6.1.4.1.9.9.862.1.1
cGnssModulePresenceStatus	1.3.6.1.4.1.9.9.862.1.2
cGnssModuleSlotInfo	1.3.6.1.4.1.9.9.862.1.3
cGnssModuleSlotState	1.3.6.1.4.1.9.9.862.1.4
cGnssSatelliteVisibilityStatus	1.3.6.1.4.1.9.9.862.1.5
cGnssModuleSatelliteCount	1.3.6.1.4.1.9.9.862.1.6
cGnssModuleSvIdSNR	1.3.6.1.4.1.9.9.862.1.7
cGnssAntennaShortAlarmStatus	1.3.6.1.4.1.9.9.862.1.8
cGnssAntennaOpenAlarmStatus	1.3.6.1.4.1.9.9.862.1.9

How to Configure the GNSS

Note To know more about the commands referenced in this document, see the Cisco IOS Master Command List .

Enabling the GNSS on the Cisco Router

```
enable
configure terminal
gnss slot r0
no shutdown
exit
```

Note After the GNSS module is enabled, GNSS will be the source for 1PPS, ToD, and 10MHz clocking functions.

Configuring the Satellite Constellation for GNSS

```
enable
configure terminal
gnss slot r0
constellation [auto | gps | galelio | beidou | qzss
exit
```

Configuring Pulse Polarity

```
enable
configure terminal
gnss slot r0
1pps polarity negative
exit
```

Note The **no 1pps polarity negative** command returns the GNSS to default mode (positive is the default value).

Configuring Cable Delay

```
enable
configure terminal
gnss slot r0
1pps offset 5
exit
```

Note It is recommended to compensate 5 nanosecond per meter of the cable.

The **no 1pps offset** command sets cable delay offset to zero.

Disabling Anti-Jam Configuration

```
enable
configure terminal
gnss slot

ro
anti-jam disable
exit
```

Verifying the Configuration of the GNSS

Use the **show gnss status** command to display status of GNSS.

```
Router# show gnss status
GNSS status:

  GNSS device: detected
  Lock status: Normal
  Receiver Status: Auto
  Clock Progress: Phase Locking
  Survey progress: 100
  Satellite count: 22
  Holdover Duration: 0
  PDOP: 1.04   TDOP: 1.00
  HDOP: 0.73   VDOP: 0.74
  Minor Alarm: NONE
  Major Alarm: None
```

Use the **show gnss satellite** command to display the status of all satellite vehicles that are tracked by the GNSS module.

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

SV PRN No   Channel No       Acq Flg    Ephemeris Flg     SV Type     Sig Strength
----------------------------------------------------------------------------------
14          0                      1                1           0               47
21          2                      1                1           0               47
22          3                      1                1           0               46
18          4                      1                1           0               47
27          6                      1                1           0               44
31          8                      1                1           0               49
24          10                     1                1           0               42
79          12                     0                1           1               18
78          13                     1                1           1               26

Router# show gnss satellite 21
Selected Satellite Info:

  SV PRN No: 21
  Channel No: 2
  Acquisition Flag: 1
 Ephemeris Flag: 1
  SV Type: 0
  Signal Strength: 47



Router# show gnss time

Current GNSS Time:

  Time: 2015/10/14  12:31:01 UTC Offset: 17

Router# show gnss location
Current GNSS Location:

  LOC: 12:56.184000 N  77:41.768000 E 814.20 m
```

Use the **show gnss device** to displays the hardware information of the active GNSS module.

```
Router# show gnss device
GNSS device:

  Serial number: FOC2130ND5X
  Firmware version: 1.4
  Firmware update progress: NA
  Authentication: Passed
```

Swapping the GNSS Module

Hot swap is supported on the RSP3 module of the GNSS.

1. Remove the standby RSP module.
2. Replace the GNSS module on the standby RSP slot.
3. Reinsert the RSP into the chassis and wait for the RSP to boot with standby ready.
4. Check for GNSS Lock Status of the standby RSP. Use command **show platform hardware slot** <*R0/R1*> [**network-clocks** | **sec GNSS**] to verify.
5. Trigger SSO after the GNSS on standby RSP is locked.
6. Repeat steps 1–3 for the other RSP.

Configuring Telemetry for GNSS module

The following example shows the configuration example of telemetry for GNSS module:

```
configure terminal
telemetry ietf subscription 1
encoding encode-tdl
filter tdl-uri /services;serviceName=ios_emul_oper/gnss_data
source-vrf Mgmt-intf
stream native
update-policy periodic 1000
receiver ip address 7.0.1.112 45000 protocol native
```

Configuration Example For Configuring GNSS

```
gnss slot R0
no shutdown
anti-jam disable
constellation glonass
1pps polarity negative
1pps offset 1000 negative
operating-mode high-accuracy
```

Verification of Telemetry for GNSS Module Configuration

Use the **show gnss status** command to display the GNSS module status configured in the device.

```
#show gnss status
GNSS status:
  GNSS device: detected
  Lock status: Normal
  Receiver Status: OD
  Clock Progress: Phase Locking
  Survey progress: 100
  Satellite count: 12
  Holdover Duration: 0
  PDOP: 0.00   TDOP: 1.00
  HDOP: 0.00   VDOP: 0.00
  Minor Alarm: NONE
  Major Alarm: None
  High Accuracy Mode: OFF, Bandwidth : 1.7Hz
```

Use the **show gnss satellite all** command to display the information of all visible satellite at a particular time.

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

SV PRN No Channel No Acq Flg  Ephemeris Flg SV Type Sig Strength Elevation Azimuth
------------------------------------------------------------------------------------------
193        0           1           1           5         37         15        138
22         1           1           1           0         47         41        192
9          2           1           1           0         48         32        335
16         3           1           1           0         46         31         31
8          4           1           1           0         47         43        145
3          5           1           1           0         49         54        217
194        6           1           1           5         40         22         52
7          7           1           1           0         44         20        298
195        8           1           1           5         40         21         80
23         9           1           1           0         45         58        359
11         10          1           1           0         43         14        182
27         11          1           1           0         46         40         95
73         12          1           1           1         24         29        273
```

The following example shows the sample output of telemetry configuration:

```
"op": "GREEN_RECORD_UPDATE",
                    "len": 498,
                    "entry_data": {
                        "gnss_data": {
                            "slot": 1,
                            "slot_state": "TDL_RSP_STANDBY",
                            "presence_status": "TDL_GNSS_MODULE_STATUS_PRESENT",
                            "lock_status": "TDL_GNSS_MODULE_LOCK_STATUS_UP",
                            "survey_progress_status": 100,
                            "satellite_tracking_status": "TDL_GNSS_SV_SNR_STATUS_GOOD",
                            "gnss_antenna_open_alarm_status": "TDL_GNSS_ALARM_ENABLE",
                            "gnss_antenna_short_alarm_status": "TDL_GNSS_ALARM_DISABLE",
                            "satellite_cnt": 9,
                            "s_cnt": 9,
                            "satellite_info": [
                                {
                                    "sv_prn": 5,
                                    "channel": 2,
                                    "acq_flag": "TDL_ACQUIRED",
                                    "eph_flag": 1,
                                    "signal_level": 46,
                                    "sv_type": "TDL_GNSS_SV_TYPE_GPS",
                                    "elevation": 62,
                                    "azimuth": 35
                                },
                                {
                                    "sv_prn": 29,
"channel": 0,
"acq_flag": "TDL_ACQUIRED",
"eph_flag": 1,
"signal_level": 44,
"sv_type": "TDL_GNSS_SV_TYPE_GPS",
"elevation": 18,
"azimuth": 328
```

Additional References

Standards

Standard	Title
—	There are no associated standards for this feature,

MIBs

MIB	MIBs Link
• There are no MIBs for this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
—	There are no associated RFCs for this feature.

CHAPTER 5

G.8275.1 Telecom Profile

First Published: March 29, 2016

Precision Time Protocol (PTP) is a protocol for distributing precise time and frequency over packet networks. PTP is defined in the IEEE Standard 1588. It defines an exchange of timed messages

PTP allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

This recommendation allows for proper network operation for phase and time synchronization distribution when network equipment embedding a telecom boundary clock (T-BC) and a telecom time subordinate clock (T-TSC) is timed from another T-BC or a telecom grandmaster clock (T-GM). This recommendation addresses only the distribution of phase and time synchronization with the full timing support architecture as defined in ITU-T G.8275.

Why G.8275.1?

The G.8275.1 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.

The G.8275.1 profile is also used in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol.

Because a boundary clock is used at every node in the chain between PTP Grandmaster and PTP Subordinate, there is reduction in time error accumulation through the network.

More About G.8275.1

The G.8275.1 must meet the following requirements:

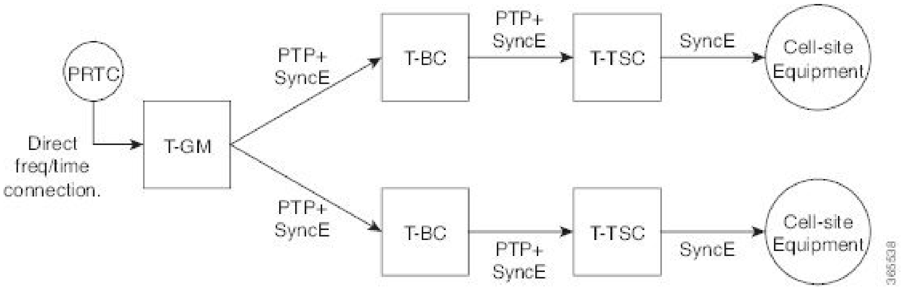
- Non-participant devices, that is, devices that only forward PTP packets, and PTP transparent clocks are not allowed.
- The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock

(PRTC). T-GM in locked mode must have phase and frequency sources that are traceable to PRTC. T-GM in locked mode must always have QL-PRC/PRS frequency. T-GM can be in holdover when losing phase. In such case, its default clock class is defined based on the available frequency source quality.

- The telecom time subordinate 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.
- 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 to a T-BC to synchronize to, it may act as a grandmaster.

The following figure describes a sample G.8275.1 topology.

Figure 4: A Sample G.8275.1 Topology



PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol.

A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

The allowed domain numbers of PTP domains within a G.8275.1 network are between 24 and 43 (both inclusive).

PTP Messages and Transport

The following PTP transport parameters are defined:

- For transmitting PTP packets, either the forwardable multicast MAC address (01-1B-19-00-00-00) or the non-forwardable multicast MAC address (01-80-C2-00-00-0E) must be used as the destination MAC address. The MAC address in use is selected on a per-port basis through the configuration. However, the non-forwardable multicast MAC address (01-80-C2-00-00-0E) will be used if no destination MAC is configured.

The source MAC address is the interface MAC address.

- For receiving PTP packets, both multicast MAC addresses (01-80-C2-00-00-0E and 01-1B-19-00-00-00) are supported.
- The packet rate for Announce messages is 8 packets-per-second. For Sync, Delay-Req, and Delay-Resp messages, the rate is 16 packets-per-second.
- Signaling and management messages are not used.

PTP Modes

Two-Way Operation

To transport phase and time synchronization and to measure propagation delay, PTP operation must be two-way in this profile. Therefore, only two-way operation is allowed in this profile.

One-Step and Two-Step Clock Mode

Both one-step and two-step clock modes are supported in the G.8275.1 profile.

A client port must be capable of receiving and processing messages from both one-step clocks and two-step clocks, without any particular configuration. However, the server clock supports only one-step mode.

PTP Clocks

Two types of ordinary clocks and boundary clocks are used in this profile:

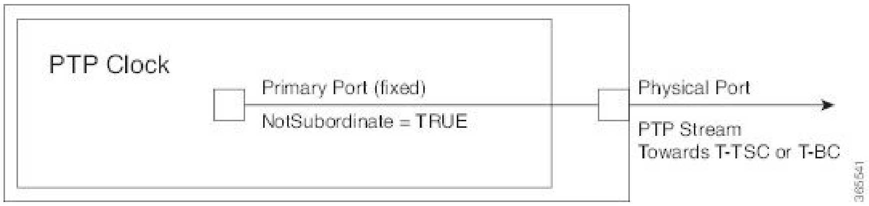
Ordinary Clock (OC)

- OC that can only be a grandmaster clock (T-GM). In this case, one PTP port will be used as a server port.

The T-GM uses the frequency, 1PPS, and ToD input from an upstream grandmaster clock.

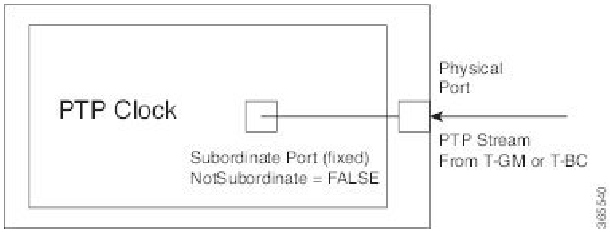
Note The T-GM server port is a fixed server port.

Figure 5: Ordinary Clock As T-GM



- OC that can only be a subordinate/client clock (T-TSC). In this case, only one PTP port is used for T-TSC, which in turn will have only one PTP server associated with it.

Figure 6: Ordinary Clock As Subordinate/Client Clock (T-TSC)

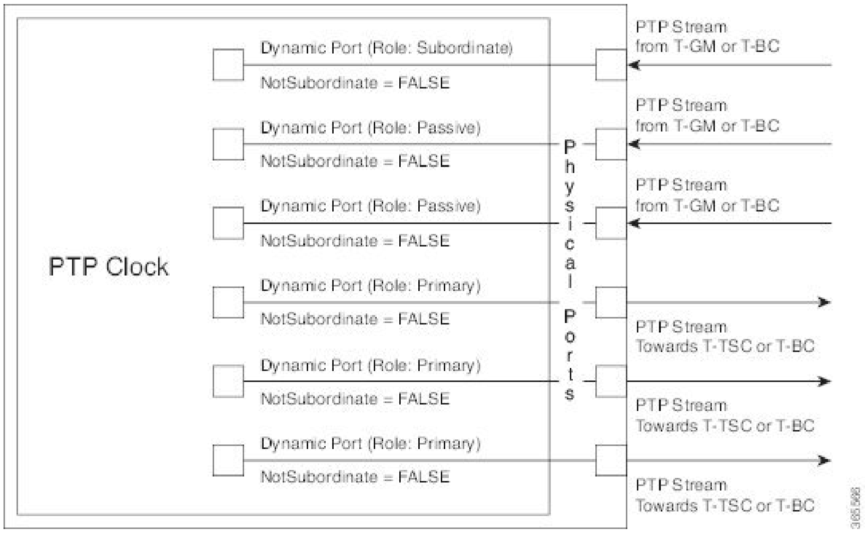


Boundary Clock (T-BC)

1. T-BC that can only be a grandmaster clock (T-GM).
2. T-BC that can become a server clock and can also be a client clock to another PTP clock.

If the BMCA selects a port on the T-BC to be a client port, all other ports are moved into the server role or a passive state.

Figure 7: Boundary Clock


PTP Clock
Dynamic Port (Role: Subordinate)
NotSubordinate = FALSE
Dynamic Port (Role: Passive)
NotSubordinate = FALSE
Dynamic Port (Role: Passive)
NotSubordinate = FALSE
Dynamic Port (Role: Primary)
NotSubordinate = FALSE
Dynamic Port (Role: Primary)
NotSubordinate = FALSE
Dynamic Port (Role: Primary)
NotSubordinate = FALSE
Physical Ports
PTP Stream from T-GM or T-BC
PTP Stream from T-GM or T-BC
PTP Stream from T-GM or T-BC
PTP Stream Towards T-TSC or T-BC
PTP Stream Towards T-TSC or T-BC
PTP Stream Towards T-TSC or T-BC
365568

PTP Ports

A port can be configured to perform either fixed Server or Client role or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a server, passive, or client role based on the BMCA.

A server port provides the clock to its downstream peers.

A client port receives clock from an upstream peer.

A dynamic port can work either as a server or a client based on the BMCA decision.

In Cisco’s implementation of the G.8275.1:

- OC clocks can support only fixed Server or Client port.
- One PTP port can communicate with only one PTP peer.
- BC can have a maximum of 64 ports. Fixed client ports are not supported on the BC.

PTP Asymmetry Readjustment

Each PTP node can introduce delay asymmetry that affects the adequate time and phase accuracy over the networks. Asymmetry in a network occurs when one-way-delay of forward path (also referred as forward path delay or ingress delay) and reverse path (referred as reverse path delay or egress delay) is different. The magnitude of asymmetry can be either positive or negative depending on the difference of the forward and reverse path delays.

Effective Cisco IOS XE Gibraltar 16.10.1, PTP asymmetry readjustment can be performed on each PTP node to compensate for the delay in the network.

Virtual Port Support on T-BC

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.

Alternate BMCA

The BMCA implementation in G.8275.1 is different from that in the default PTP profile. The G.8275.1 implementation is called the Alternate BMCA. Each device uses the alternate BMCA to select a clock to synchronize to, and to decide the port states of its local ports.

Benefits

With upcoming technologies like LTE-TDD, LTE-A CoMP, LTE-MBSFN and Location-based services, eNodeBs (base station devices) are required to be accurately synchronized in phase and time. Having GNSS systems at each node is not only expensive, but also introduces vulnerabilities. The G.8275.1 profile meets the synchronization requirements of these new technologies.

Prerequisites for Using the G.8275.1 Profile

- PTP over Multicast Ethernet must be used.
- Every node in the network must be PTP aware.
- It is mandatory to have a stable physical layer frequency whilst using PTP to define the phase.
- Multiple active grandmasters are recommended for redundancy.

Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.

Configuring the G.8275.1 Profile

Note To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List.

Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM section in the Clocking and Timing chapter of this book.

Creating a Server-Only Ordinary Clock

```
ptp clock ordinary domain 24
local-priority 1
priority2 128
clock-port server-port-1
master profile g8275.1
local-priority 1
transport ethernet multicast interface Gig 0/0/1
clock-port server-port-2
master profile g8275.1
```

Note It is mandatory that when electrical ToD is used, the **utc-offset** command is configured before configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the server and client clocks:

```
ptp clock ordinary domain 0
 utc-offset 37
tod R0 cisco
input 1pps R0
clock-port server-port master
  transport ipv4 unicast interface Loopback0 negotiation
```

Associated Commands

- ptp clock
- local-priority
- priority2

Creating an Ordinary Client

```
ptp clock ordinary domain 24
```

```
hybrid
clock-port slave-port
slave profile g8275.1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 1000
```

Creating Dynamic Ports

Note Dynamic ports can be created when you do not specify whether a port is Server or Client. In such cases, the BMCA dynamically choses the role of the port.

```
ptp clock boundary domain 24 hybrid
time-properties persist 600
utc-offset 45 leap-second “01-01-2017 00:00:00” offset 1
clock-port bc-port-1 profile g8275.1local-priority 1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 500
clock-port bc-port-2 profile g8275.1 local-priority 2
transport ethernet multicast interface Gig 0/0/1
delay-asymmetry -800
```

Configuring Virtual Ports

```
ptp clock boundary domain 24 hybrid
utc-offset 45 leap-second “01-01-2017 00:00:00” offset 1
virtual-port virtual-port-1 profile g8275.1 local-priority 1
input 1pps R0
input tod R0 ntp
```

Note It is mandatory that when electrical ToD is used, the **utc-offset** command is configured *before* configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the primary and subordinate clocks.

Restrictions for Configuring Virtual Ports

- Virtual port configuration is not allowed under Ordinary Clocks.
- Virtual port configuration is not supported under non-hybrid T-BC cases.

Associated Commands

- input

Verifying the Local Priority of the PTP Clock

```
Router# show ptp clock dataset default
CLOCK [Boundary Clock, domain 24]
```

```
  Two Step Flag: No
  Clock Identity: 0x2A:0:0:0:58:67:F3:4
  Number Of Ports: 1
  Priority1: 128
  Priority2: 90
  Local Priority: 200
  Domain Number: 24
  Slave Only: No
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

Verifying the Port Parameters

```
Router# show ptp port dataset port
PORT [SERVER]
  Clock Identity: 0x49:BD:D1:0:0:0:0:0
  Port Number: 0
  Port State: Unknown
  Min Delay Req Interval (log base 2): 42
  Peer Mean Path Delay: 648518346341351424
  Announce interval (log base 2): 0
  Announce Receipt Timeout: 2
  Sync Interval (log base 2): 0
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): 0
  PTP version: 2
  Local Priority: 1
  Not-slave: True
```

Verifying the Foreign Master Information

```
Router# show platform software ptp foreign-master domain 24
PTPd Foreign Master Information:

Current Master: SLA

Port: SLA
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Clock Quality:
    Class: 6
    Accuracy: Within 100ns
    Offset (Log Variance): 0x4E5D
  Steps Removed: 1
  Not-Slave: FALSE
```

Verifying Current PTP Time

```
Router# show platform software ptpd tod
PTPd ToD information:

Time: 01/05/70 06:40:59
```

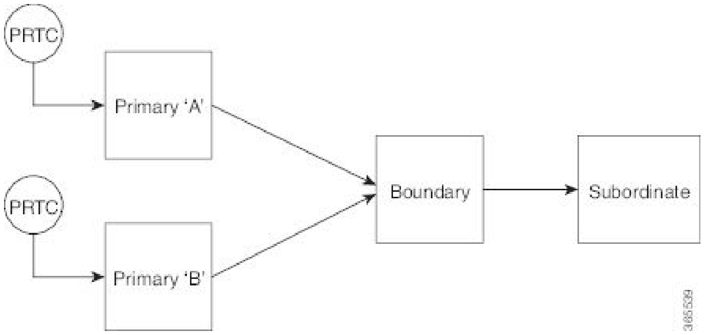
Verifying the Virtual Port Status

```
Router# show ptp port virtual domain 24
VIRTUAL PORT [vp]
  Status: down
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Port Number: 1
  Clock Quality:
    Class: 6
    Accuracy: 0x21
    Offset (log variance): 0x4E5D
  Steps Removed: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Not-slave: False
```

G.8275.1 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.1 network with two server clocks, a boundary clock and a client. Let's assume that server A is the main server and B is the backup server.

Figure 8: Topology for a Configuration Example



The configuration on server clock A is:

```
ptp clock ordinary domain 24
  clock-port server-port profile g8275.1
    transport ethernet multicast interface GigabitEthernet 0/0/0
```

The configuration on server clock B is:

```
ptp clock ordinary domain 25
  clock-port server-port profile g8275.1
```

transport ethernet multicast interface GigabitEthernet 0/1/0

The configuration on the boundary clock is:

```
ptp clock boundary domain 24 hybrid
  local-priority 3
  clock-port client-port-a profile g8275.1 local-priority 1
    transport ethernet multicast interface Gig 0/0/1
  clock-port client-port-b profile g8275.1 local-priority 2
    transport ethernet multicast interface Gig 0/1/1
  clock-port server-port profile g8275.1
    transport Ethernet multicast interface Gig 0/2/1
```

The configuration on the client clock is:

```
ptp clock ordinary domain 24 hybrid
  clock-port client-port slave profile g8275.1
    transport Ethernet multicast interface Gig 0/0/0
```

Feature Information for G.8275.1

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note Table 11: Feature Information for G.8275.1 , on page 100 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 11: Feature Information for G.8275.1

Feature Name	Releases	Feature Information
G.8275.1–Support for 1588 profile	XE 3.18	This PTP telecom profile introduces phase and time synchronization with full timing support from the network. The following commands were introduced • **local-priority** The following commands were modified: • **clock-port** • **show ptp clock dataset default** • **show ptp port dataset port** The following command is deprecated for the G.8275.1 profile clocks: • **show ptp port running** The alternate command is **show platform software ptp foreign-master [domain-number].** **Note** This command is applicable only for the G.8275.1 profile clocks.

CHAPTER 6

G.8275.2 Telecom Profile

Precision Time Protocol (PTP) is a protocol for distributing precise time and frequency over packet networks. PTP is defined in the IEEE Standard 1588. It defines an exchange of timed messages.

PTP allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

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 and IPv6 in unicast mode. However, IPv6 is not supported in Cisco IOS XE Everest 16.5.1.

Note In this document, G.8275.2 refers to ITU-T G.8275.2 (02/2016).

Why G.8275.2?

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.

PTP Clocks

Two types of ordinary clocks and three types of boundary clocks are used in this profile:

Ordinary Clocks (OCs)

- **Telecom Grandmaster (T-GM)**: A telecom grandmaster provides timing for other devices in the network, and is usually connected to a server reference time source, such as a GNSS receiver. It does not synchronize its local clock to other network elements.

  Considerations for a T-GM:

  - Only one PTP port can be configured as a server port.
  - One T-GM server port can have multiple clients associated with it.
  - The T-GM OC server port is a fixed port; that is, it always acts as a server clock and its role does not change by negotiating with its peer.

- **Partial-Support Telecom Time Subordinate/Client Clocks (T-TSC-P)**: A client clock synchronizes its local clock to another PTP clock (GM, T-GM or T-BC), and does not provide synchronization through PTP to any other device.

  Considerations for a T-TSC-P:

  - An ordinary clock with single client port can be configured.
  - Only one peer clock address can be configured as clock source.

Boundary Clocks (BCs)

Boundary clocks can assume any of the following roles:

- A BC that can only be a grandmaster (T-GM)

  A server-only boundary clock can have multiple server port configured. The different server ports can be in different VLANs to serve the clients that need to be served over them.

- A BC that can become a grandmaster and can also be a client to another PTP clock (T-BC-P).

  Client-only port configuration is not allowed under boundary clocks. However, one of the dynamic ports (port state negotiated based on BMCA), can assume the role of client.

- A BC that can only be a subordinate/client (T-TSC-P with more than one port).

Fixed server port, dynamic ports and virtual port can be configured under a boundary clock. However, only one clock source (peer address) can be configured with a dynamic port.

Miscellaneous Notes

- Any clock that has multiple PTP ports within a PTP domain is termed a boundary clock (BC). Ordinary clocks (OC) always have only one PTP port.

  In G.8275.2 (02/2016), PTP transparent clocks are not permitted.

PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol.

A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

The allowed domain numbers of PTP domains within a G.8275.2 network are in the range of 44 and 63 (both inclusive). The default domain number is 44.

PTP Messages and Transport

The following PTP transport parameters are defined:

- In Cisco IOS XE Everest 16.5.1, PTP over IPv4 in unicast mode must be used..
- Either one-step or two-step clock mode must be used.
- For PTP primaary clock, both one-way and two-way operation modes are supported. This means PTP primaary can grant request to a subordinate's one-way or two-way requests.
- In case of PTP subordinate clock, two-way PTP operation is required to allow phase/time-of-day delivery. The delay-request-response mechanism is used to propagate delay measurement; the peer-delay mechanism is not used.
- The G.8275.2 profile supports unicast message negotiation.
- Interfaces carrying PTP traffic can be under different VRFs.
- Sync, Delay_Req, Announce, Follow_Up, Delay_Resp, and Signaling messages are used in this profile. See the table below for rates of transmission for these messages.

Table 12: PTP Messages and their Rate of Transmission

Message	Default Rate (packets per second)	Minimum Rate (packets per second)	Maximum Rate (packets per second)
Sync	32	1	128
Follow_up (only if sync messages are used)	32	1	128
Delay_Req	16	1	128
Delay_Resp	16	1	128
Announce	1	1	8
Signaling	Not Specified	1	Not specified

Limitations

- Pdelay_Req, Pdelay_Resp, Pdelay_Resp_Follow_Up and management messages are not used in this profile.

PTP Ports

A port can be configured to perform either fixed primaary or subordinate role or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a primaary, passive, or subordinate role based on the BMCA.

In G.8275.2, PTP ports are not tied to any specific physical interfaces, but are tied to a loopback (virtual) interface. Traffic from a PTP port is routed through any physical interface based on the routing decision.

For a Boundary Clock, multiple PTP ports are supported. The maximum number of PTP ports supported on a BC node is 64.

For a dynamic port, only one clock source can be configured.

Starting with Cisco IOS XE Release 16.12, PTP 8275.2 supports multiple loopbacks (not in VRFs) for fixed Master ports.

Virtual Port Support on T-BC

In G.8275.2 implementation, virtual PTP ports are used to provide electrical frequency and phase inputs to T-BC. With virtual ports, T-BCs are fed with frequency inputs, such as, synchronous Ethernet, 10M, BITS, and phase/time inputs, such as, 1PPS and ToD. Virtual ports participate in the BMCA of the T-BCs.

If frequency source is of Category-1 (according to G.8275.2) and if 1PPS and ToD inputs are UP, virtual port status is up. Otherwise, virtual port status is down.

A virtual port participates in BMCA only when it is in administratively up state.

A virtual port always has clock class 6, clock accuracy 0x21 (within 100ns), and clock offset Scaled Log Variance of 0x4E5D.

Note The virtual port has the attributes set to the above values only when it is in the UP state.

Whenever virtual port is selected as the best server clock by the BMCA, PTP clock is driven by the electrical inputs. If virtual port is administratively up but not selected by BMCA, 1PPS and ToD inputs do not affect PTP clock.

Alternate BMCA

The BMCA implementation in G.8275.2 is different from that in the default PTP profile. The G.8275.2 implementation specifies an alternate best server clock algorithm, which is used by each device to select a clock to synchronize to, and to decide the port states of its local ports.

The following consideration apply to the G.8275.2 implementation of the BMCA:

- **MasterOnly**: A per port attribute, MasterOnly defines the state of the port. If this attribute is true, the port is never placed in the client state.
- **Priority 1**: Priority 1 is always static in this profile and is set to 128. Priority 1 is not used in BMCA.
- **Priority 2**: Priority 2 is a configurable value and its range if from 0 to 255.
- **Local Priority**: Local priority is configured locally on clock ports to set the priority on nominated clocks. The default value is 128 and valid range is from 1 to 255.

Benefits

With upcoming technologies like LTE-TDD, LTE-A CoMP, LTE-MBSFN and Location-based services, eNodeBs (base station devices) are required to be accurately synchronized in phase and time. Having GNSS systems at each node is not only expensive, but also introduces vulnerabilities. The G.8275.2 profile meets the synchronization requirements of these new technologies.

Restrictions for Using the G.8275.2 Profile

- In G.8275.2, PTP can be used in both hybrid mode and non-hybrid mode. In hybrid mode, PTP is used to provide phase and time-of-day throughout the network synchronization along with PHY layer frequency support (SyncE). In non-hybrid mode, PTP is used without PHY layer frequency support (SyncE).
- A G.8275.2 PTP clock can have redundant clock sources configured (through multiple PTP ports). However, at any given time, a G.8275.2 PTP clock synchronizes to only one clock source, which is selected by BMCA.
- In Cisco IOS XE Everest 16.5.1, the G.8275.2 does not support assisted partial-support telecom time subordinate clock (T-TSC-A).
- The G.8275.2 does not provide any recommendations for performance analysis and network limits for the clocks.
- For the ports configured with G.8275.2 profile, removal of **`transport ipv4 unicast interface Loopback 0 negotiation`** configuration by using the **no** form of the command is not supported.

Configuring the G.8275.2 Profile

Note To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List.

Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM section in the Clocking and Timing chapter of this book.

Creating a Server-Only

T-GM Ordinary Clock

```
ptp clock ordinary domain 44
clock-port server1 master profile g8275.2
transport ipv4 unicast interface Loopback0 negotiation
```

Note It is mandatory that when electrical ToD is used, the **utc-offset** command is configured *before* configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the server and client clocks:

```
ptp clock ordinary domain 44
 utc-offset 37
tod R0 cisco
input 1pps R0
clock-port server-port master
  transport ipv4 unicast interface Loopback0 negotiation
```

T-GM Boundary Clock

A boundary clock can be configured as a T-GM by configuring the external inputs of 10m, 1pps and ToD. However, external inputs to a boundary clock can be given only through a virtual port.

```
ptp clock boundary domain 44 hybrid
virtual-port vp1 profile g8275.2
  input 1pps R0
  input tod R0 ntp
 clock-port dp2
  transport ipv4 unicast interface Loopback0 negotiation
  clock source 60.60.60.60
```

```
ptp clock boundary domain 45
clock-port d1 profile g8275.2 local-priority 12
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.1
clock-port dp2 profile g8275.2 local-priority 13
transport ipv4 unicast interface Lo0 negotiation
clock source 12.12.12.12
clock-port dp3 profile g8275.2 local-priority 14
transport ipv4 unicast interface Lo0 negotiation
clock source 56.56.56.56
clock-port dp1 profile g8275.2 local-priority 12
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.2
```

Creating an Ordinary Subordinate (T-TSC-P)

Creating a Boundary Clock

```
ptp clock boundary domain 44
  clock-port server-port-1 master profile G.8275.2
    transport ipv4 unicast interface lo 0 negotiation
  clock-port port1 profile G.8275.2
    transport ipv4 unicast interface lo 0 negotiation
    clock source 10.0.0.1
  clock-port port2 profile G.8275.2
    transport ipv4 unicast interface lo 0 negotiation
    clock source 10.1.1.2
```

Creating Dynamic Ports

The following considerations apply to dynamic ports:

- Dynamic ports are created by not specifying whether a port is server or client. In such cases, the BMCA dynamically choses the role of the port.
- Dynamic ports do not have a keyword.
- All the dyanamic ports configured under a clock must use the same loopback interface.
- For a dynamic port to communicate with a peer, it must have **clock source x.x.x.x** configured with it.

```
ptp clock boundary domain 44 hybrid
clock-port bc-port-1 profile g8275.2local-priority 1
transport ipv4 unicast interface Lo0 negotiation

clock source 10.0.0.1
clock-port bc-port-2 profile g8275.2 local-priority 2
transport ipv4 unicast interface Lo0 negotiation

clock source 10.0.0.2
```

Configuring Virtual Ports

```
ptp clock boundary domain 44 hybrid
utc-offset 37 leap-second “01-01-2017 00:00:00” offset 1
virtual-port virtual-port-1 profile g8275.2 local-priority 1
input 1pps R0
input tod R0 ntp
```

Note It is mandatory that when electrical ToD is used, the **utc-offset** command is configured *before* configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

Restrictions for Configuring Virtual Ports

- Virtual port configuration is not allowed under Ordinary Clocks.
- Virtual port configuration is not supported under non-hybrid T-BC cases.

Verifying the Default and Parent Datasets

```
Router# show ptp clock dataset default

CLOCK [Boundary Clock, domain 44]

Two Step Flag: No

Clock Identity: 0x5C:83:8F:FF:FE:1F:27:BF
```

```
Number Of Ports: 5

Priority1: 128

Priority2: 128

Local Priority: 128

Domain Number: 44

Slave Only: No

Signal Fail: No

Clock Quality:

Class: 165

Accuracy: Unknown

Offset (log variance): 65535


Router# show ptp clock dataset parent domain 44
CLOCK [Ordinary Clock, domain 44]

  Parent Clock Identity: 0x80:E0:1D:FF:FE:E3:F8:BF
  Parent Port Number: 1
  Parent Stats: No
  Observed Parent Offset (log variance): 65535
  Observed Parent Clock Phase Change Rate: 2147483647

  Grandmaster Clock:
    Identity: 0x70:10:5C:FF:FE:50:3A:3F
    Priority1: 128
    Priority2: 128
    Clock Quality:
      Class: 6
      Accuracy: Within 100ns
      Offset (log variance): 20061
```

Verifying the PTP Clock State

```
Router# show ptp clock  running domain 44

                      PTP Boundary Clock [Domain 44] [Hybrid]
         State             Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         PHASE_ALIGNED      1              2577144        7349181        Hot standby

                               PORT SUMMARY
Name  Tx Mode      Role           Transport    State        Sessions     PTP master Port
Addr
dp1   unicast      negotiated     Lo0          Slave        1                  UNKNOWN

                             SESSION INFORMATION
dp1 [Lo0] [Sessions 1]
 Peer addr          Pkts in   Pkts out   In Errs    Out Errs
 10.0.0.1            7349181    2577144   0          0
```

Verifying the PTP Clock Synchronization State

```
Router# show network-clocks synchronization detail
Symbols:     En - Enable, Dis - Disable, Adis - Admin Disable
             NA - Not Applicable
             *  - Synchronization source selected
             #  - Synchronization source force selected
             &  - Synchronization source manually switched

Automatic selection process : Enable
Equipment Clock : 2048 (EEC-Option1)
Clock State : Frequency Locked
Clock Mode : QL-Enable
ESMC : Enabled
SSM Option : 1
T0 : GigabitEthernet0/0/11
Hold-off (global) : 300 ms
Wait-to-restore (global) : 0 sec
Tsm Delay : 180 ms
Revertive : No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 2
Squelch Threshold: QL-SEC
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (sf_change)-> 1A (sf_change)-> 1A (sf_change)-> 1A (sf_change)->
 1A (sf_change)-> 1A (sf_change)-> 1A (sf_change)-> 1A (ql_change)-> 1A (sf_change)-> 1A
(ql_change)-> 1A


Nominated Interfaces

Interface            SigType     Mode/QL      Prio  QL_IN  ESMC Tx  ESMC Rx
Internal             NA          NA/Dis       251   QL-SEC    NA        NA
*Gi0/0/11             NA          Sync/En      1     QL-PRC    -         -
Te0/0/24             NA          Sync/En      2     QL-PRC    -         -

Interface:
---------------------------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-SEC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms: None
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0
Description: None

Local Interface: Gi0/0/11
Signal Type: NA
Mode: Synchronous(Ql-enabled)
```

```
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 1
QL Receive: QL-PRC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: QL-DNU
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms :  None
Slot Disabled: FALSE
SNMP input source index: 2
SNMP parent list index: 0
Description: None

Local Interface: Te0/0/24
Signal Type: NA
Mode: Synchronous(Ql-enabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 2
QL Receive: QL-PRC
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: QL-PRC
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 0
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Active Alarms :  None
Slot Disabled: FALSE
SNMP input source index: 3
SNMP parent list index: 0
Description: None
```

Verifying the Port Parameters

```
Router# show ptp port dataset port domain 44

PORT [SERVER-1]
Clock Identity: 0x70:10:5C:FF:FE:50:3A:3F
Port Number: 1
Port State: Master
Min Delay Req Interval (log base 2): -4
Peer Mean Path Delay: 0
Announce interval (log base 2): 1
Announce Receipt Timeout: 3
Sync Interval (log base 2): -5
Delay Mechanism: End to End
Peer Delay Request Interval (log base 2): -4
PTP version: 2
Local Priority: 128
Master-only: True
Signal-fail: False
```

Verifying the Foreign Master Information

```
Router# show platform software ptp foreign-master domain 44
PTPd Foreign Master Information:

Current Master: SLA

Port: SLA
GM Clock Identity: 0x70:10:5C:FF:FE:50:3A:3F
Clock Stream Id: 0
Priority1: 128
Priority2: 128
Local Priority: 10
Clock Quality:
Class: 6
Accuracy: Within 100ns
Offset (Log Variance): 0x4E5D
Source Port Identity:
Clock Identity: 0x70:10:5C:FF:FE:50:3A:3F
Port Number: 1
Steps Removed: 1
masterOnly: FALSE
Qualified: TRUE
```

Verifying Current PTP Time

```
Router# show platform software ptpd tod
PTPd ToD information:

Time: 01/05/70 06:40:59
```

Verifying the Virtual Port Status

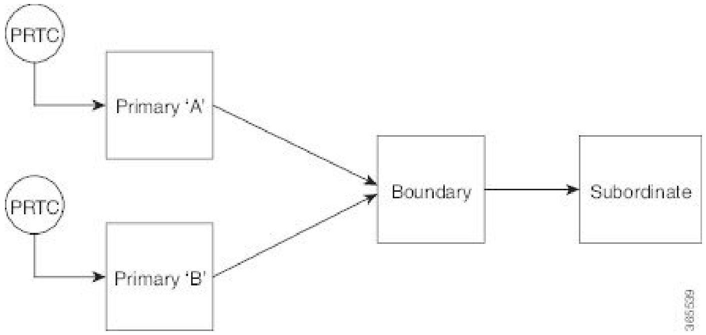
```
Router# show ptp port virtual domain 44

VIRTUAL PORT [vp1]
  Status: up
  Clock Identity: 0x64:F6:9D:FF:FE:F2:25:3F
  Port Number: 2
  Clock Quality:
    Class: 6
    Accuracy: 0x21
    Offset (log variance): 0x4E5D
  Steps Removed: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Not-slave: False
  Signal-fail: True
```

G.8275.2 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.2 network with two primaary clocks, a boundary clock and a subordinaate clock. Let's assume that server A is the ordinary clock and B is the backup server clock with virtual port.

Figure 9: Topology for a Configuration Example



The configuration on TGM A (as ordinary clock):

```
ptp clock ordinary domain 44
tod R0 ntp
input 1pps R0
utc-offset 37
clock-port server-port master profile g8275.2
transport ipv4 unicast interface Lo0 negotiation
```

The configuration on TGM B with Virtual Port:

```
ptp clock boundary domain 44 hybrid
utc-offset 37
clock-port dynamic1 profile g8275.2
transport ipv4 unicast interface Lo0 negotiation
clock source 3.3.3.3
virtual-port virtual1 profile g8275.2
input 1pps R0
input tod R0 ntp
```

The configuration on the boundary clock:

```
ptp clock boundary domain 44 hybrid
clock-port dynamic1 profile g8275.2 local-priority 1
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.1
clock-port dynamic2 profile g8275.2 local-priority 2
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.2
clock-port dynamic3 profile g8275.2
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.4
```

The configuration on the client clock:

```
ptp clock ordinary domain 44 hybrid
clock-port client-port slave
```

```
transport ipv4 unicast interface Lo0 negotiation
clock source 10.0.0.3
```

CHAPTER 7

PTP Multiprofile

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a network. Clock synchronization is achieved by these three elements: Frequency, Phase and Time. Every node in a network must be synchronized with every other node for these three elements..

PTP allows for separate profiles to be defined for it to be adaptable in different scenarios. A profile is a specific selection of PTP configuration options, which are selected to meet the requirements of a particular application.

Based on the synchronization requirements of telecommunication networks, ITU-T defines standard profiles based on PTPv2. Some profiles defined by ITU-T for telecom industry are:

- ITU-T G.8265.1: Precision time protocol telecom profile for frequency synchronization.
- ITU-T G.8275.1: Precision time protocol telecom profile for phase/time synchronization with full timing support from the network.
- ITU-T G.8275.2: Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network.

This chapter explains how a PTP Boundary Clock which works with multiple PTP profiles, can be configured on the Cisco router.

In a typical PTP network deployment all the participating network elements run on the same PTP profile (1588 / ITU-T G.8275.1 / ITU-T G.8275.2). However, due to differences in capabilities or functional requirements, some network elements might require a PTP translation from one profile to another. The PTP multiprofile feature caters to this requirement.

PTP Multiprofile support is achieved in a PTP boundary clock by translating one PTP profile at a PTP subordinate port to another PTP profile at a PTP primary port.

To translate PTP properties from one profile to other, a special type of "inter-op" clock-port is introduced. This special clock-port is configured with the required profile and domain information.

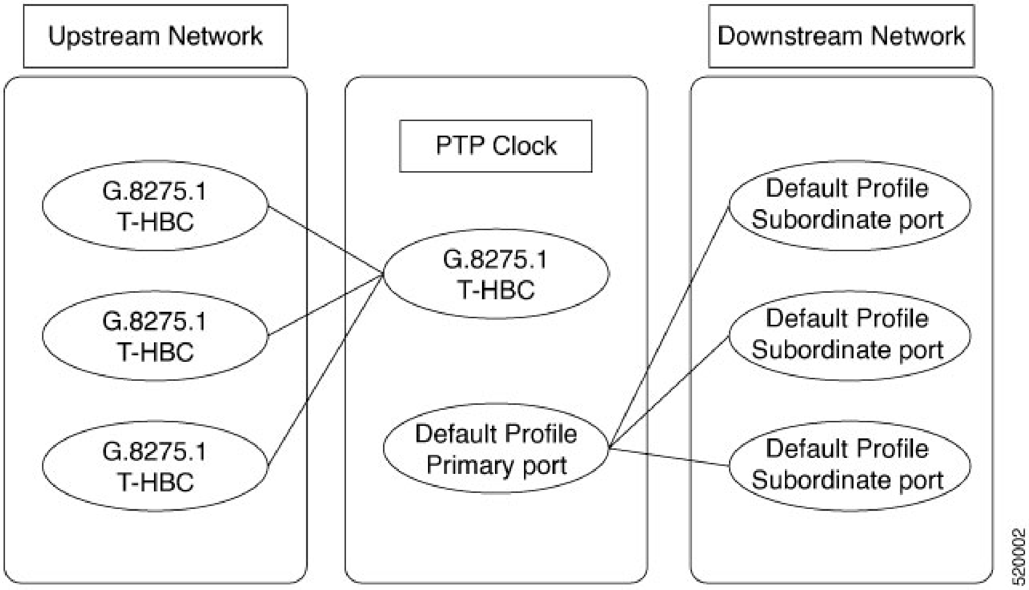
With PTP Multiprofile support, the Boundary Clock can run its subordinate port in one profile or domain and provide the PTP clock to a downstream node in a different profile or domain by using the new "inter-op" port.

PTP Multiprofile is configured on the Cisco router with the following command:

clock-port port-name <*inter-op-port*> domain <*0-127*> inter-op-profile {*1588* |*g8275.1* |*g8275.2*}

transport *{ipv4/ethernet} {multicast |unicast}* interface *interface-type interface-number*.

The following diagram which depicts how PTP Multiprofile works on a Cisco router:


Upstream Network
Downstream Network
PTP Clock
G.8275.1 T-HBC
G.8275.1 T-HBC
G.8275.1 T-HBC
G.8275.1 T-HBC
Default Profile Primary port
Default Profile Subordinate port
Default Profile Subordinate port
Default Profile Subordinate port
520002

- PTP Multiprofile Restrictions, on page 116
- Combination Matrix for PTP over MPLS with Multiprofile Configuration, on page 117
- Configure PTP Multiprofile, on page 118

PTP Multiprofile Restrictions

- A maximum of **three** interop profiles with different domain numbers can be supported on the Cisco router.
- The server clock profile must be mutually exclusive with the interop profile. For example, if the server clock profile is default profile, then the interop profile must **not** be the default profile.
- The Interop port works as the server port. It cannot be used as a client port.
- **ITU-T G.8265.1** is not supported as the Interop profile.
- All interop ports with the 1588-default profile or the G.8275.2 profile must use the same loopback interface as the server server port.
- A server clock and port must be created before creating an Interop port.
- The server clock must be hybrid if the interop port is running the G.8275.1 profile.
- While configuring the PTP multiprofile, the best practice is to reduce the number of hops between the PTP grandmaster clock and the PTP slave router. We recommend a maximum of eight hops to mitigate network delays. You can check the number of hops between the PTP grandmaster and the PTP slave by executing the following command in the PTP slave router:

```
Router#show ptp clock dataset current
CLOCK [Boundary Clock, domain 44]
Steps Removed: 7
Offset From Master: -1981ns
Mean Path Delay: -443ns
```

Combination Matrix for PTP over MPLS with Multiprofile Configuration

This section lists the various supported combinations for PTP Multiprofiles:

Table 13: Supported Combinations for the Cisco ASR-903 RSP3 and Cisco ASR-907 RSP3

Primary Port Type	Interop Port Type	G8275.1 Profile Configured (Primary or Interop)	PTP Over MPLS Support
1G	1G	Yes	No
10G	1G	Yes	No
1G	10G	Yes	No
10G	10G	Yes	Yes
1G	1G	No	Yes
10G	1G	No	Yes
1G	10G	No	Yes
10G	10G	No	Yes

Table 14: Supported Combinations for the Cisco RSP2 Routers

Primary Port Type	Interop Port Type	G8275.1 Profile Configured (Primary or Interop)	PTP Over MPLS Support
1G	1G	Yes	No
10G	1G	Yes	No
1G	10G	Yes	No
10G	10G	Yes	No
1G	1G	No	Yes
10G	1G	No	Yes
1G	10G	No	Yes
10G	10G	No	Yes

Configure PTP Multiprofile

The following sections describe how to configure PTP Multiprofile on the Cisco router; for more information see the *Cisco IOS Interface and Hardware Component Command Reference*.

Default Profile to G8275.1 Profile

```
ptp clock boundary domain 0 hybrid
 clock-port subordinate-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 16.16.16.2
clock-port primary-port master
  transport ipv4 unicast interface Lo1 negotiation
clock-port inter_75_1  inter-op-port domain 24 inter-op-profile g8275.1
  transport ethernet multicast interface Te0/3/1
```

Default Profile to G8275.2 Profile

```
ptp clock boundary domain 0 hybrid
 clock-port subordinate-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 16.16.16.2
clock-port primary-port master
  transport ipv4 unicast interface Lo1 negotiation
clock-port inter_75_2 inter-op-port domain 45 inter-op-profile g8275.2
  transport ipv4 unicast interface Lo1 negotiation
```

G8275.1 Profile to Default Profile

```
ptp clock boundary domain 24 hybrid
 clock-port subordinate-port profile g8275.1 local-priority 1
  transport ethernet multicast interface GigabitEthernet0/1/1
 clock-port primary-port profile g8275.1 local-priority 2
  transport ethernet multicast interface GigabitEthernet0/1/2
clock-port inter_default inter-op-port domain 0 inter-op-profile 1588
  transport ipv4 unicast interface Lo1 negotiation
```

G8275.2 Profile to Default Profile

```
ptp clock boundary domain 45 hybrid
clock-port subordinate_calnex profile g8275.2 local-priority 1
  transport ipv4 unicast interface Lo0 negotiation
  clock source 16.16.16.2
clock-port primary-port profile g8275.2 local-priority 2
  transport ipv4 unicast interface Lo0 negotiation
clock-port inter_default inter-op-port domain 0 inter-op-profile 1588
  transport ipv4 unicast interface Lo0 negotiation
```

G8275.1 Profile to G8275.2 Profile

```
ptp clock boundary domain 24 hybrid
 clock-port subordinate-port profile g8275.1 local-priority 1
  transport ethernet multicast interface GigabitEthernet0/1/1
 clock-port primary-port profile g8275.1 local-priority 2
  transport ethernet multicast interface GigabitEthernet0/1/2
clock-port inter_75_2  inter-op-port domain 45 inter-op-profile g8275.2
  transport ipv4 unicast interface Lo1 negotiation
```

G8275.2 Profile to G8275.1 Profile

```
ptp clock boundary domain 45 hybrid
clock-port subordinate_calnex profile g8275.2 local-priority 1
  transport ipv4 unicast interface Lo0 negotiation
  clock source 16.16.16.2
clock-port primary-port profile g8275.2 local-priority 2
  transport ipv4 unicast interface Lo0 negotiation
clock-port inter_75_1 inter-op-port domain 24 inter-op-profile g8275.1
  transport ethernet multicast interface Te0/3/1
```

Troubleshooting PTP Multiprofile

Effective from Cisco release 17.1.x, you can troubleshoot PTP multiprofile on the Cisco router by using the following command:

show ptp port dataset inter-op-mp-port

```
Clock Identity: 0x74:26:AC:FF:FE:FA:4D:3F <valid clock identity of primary master>
Port Number: 0
Port State: <Master/Unknown >
Profile: <g8275.2/g8275.1/default >
Priority1: 128
Priority2: 128
Local Priority: 128
Domain Number: 24
Slave Only: Yes
Clock Quality:
Class: 255
Accuracy: 250
Offset (log variance): 65535
```

CHAPTER 8

Network Time Protocol

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

NTP services are disabled on all interfaces by default.

Networking devices running NTP can be configured to operate in a variety of association modes when synchronizing time with reference time sources.

Line Aux 0 option is disabled by default.

When you configure both IP address and FQDN of the same NTP server in Cisco IOS XE, only the FQDN configuration is displayed in the **show running-config** command output after FQDN resolves to the same IP address.

This module describes how to configure Network Time Protocol on Cisco devices.

Restrictions for Network Time Protocol

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

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

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

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

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

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

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

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

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

Information About Network Time Protocol

Network Time Protocol

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

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

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

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

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

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

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

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

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

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

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

NTP services are disabled on all interfaces by default. See How to Configure Network Time Protocol to enable NTP services.

NTP Support for IPv6 Networks

Table 15: Feature History

Feature Name	Release Information	Feature Description
NTP Support for IPv6 Networks	Cisco IOS XE Release 17.11.1	Network Time Protocol (NTP) synchronizes device clocks across networks to maintain system accuracy. In this release, NTP supports IPv6 multicast networks. The NTP server sends clock updates as multicast messages to the clients across IPv6 networks. As NTP packets are sent only to the intended clients, it reduces timing traffic in the network.

NTP version 4 supports IPv6 networks. It provides the following capabilities:

- Synchronizes time over IPv6 networks.
- Provides a security framework based on public key cryptography and standard X509 certificates.
- Uses specific multicast groups and automatically calculates its time-distribution hierarchy through an entire network. NTP automatically configures the hierarchy of the servers in order to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

NTP Association Modes

There are different modes in which a NTP-enabled router gathers information about its peer with which it is associated. Using one of the modes listed below, NTP collects peer details:

- Poll-Based NTP Associations
- Broadcast-Based NTP Associations
- Multicast-Based NTP Associations

Poll-Based NTP Associations

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

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

- Client mode
- Symmetric active mode

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

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

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

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

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

Broadcast-Based NTP Associations

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

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

The NTP server and client can communicate using IPv4 broadcast messages.

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

Multicast-Based NTP Associations

Multicast mode is used when you intend having a time source that sends out time to multiple clients—One source and many clients. You must configure multicast capabilities and all related commands on the server and the client. NTP version 4 uses IPv6 multicast messages to send and receive clock updates.

The multicast server periodically sends clock synchronization messages to the multicast address that you have configured. Clients listen to these messages and synchronize to the server. In the multicast mode, the synchronization is only one-way—A multicast client to a multicast server. A multicast server can provide time synchronization for clients in the same subnet or in different subnets.

A multicast client is enabled by using the **ntp multicast client** command and specifying the multicast group address.

NTP Access Group

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

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

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

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

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

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

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

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

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

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

NTP Services on a Specific Interface

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

Source IP Address for NTP Packets

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

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

System as an Authoritative NTP Server

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

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

How to Configure Network Time Protocol

Configuring NTP

There are different modes in which a NTP-enabled router gathers information about its peer with which it is associated. You can configure the router to synchronize its clock with the intended server by using several modes.

Configuring Poll-Based NTP Associations

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ntp peer** *ip-address* |*ipv4*| |*ipv6*| [**normal-sync**] [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp peer 192.168.10.1 normal-sync version 2 prefer`	Forms a peer association with another system.
Step 4	**ntp server** *ip-address* |*ipv4*| |*ipv6*| [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp server 192.168.10.1 version 2 prefer`	Forms a server association with another system.

Step 5	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring Broadcast-Based NTP Associations

Procedure

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

Step 7	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Multicast-Based NTP Associations

To facilitate the configuration of multicast-based NTP associations, you must configure the required interface to send and receive NTP multicast packets.

Configuring an Interface to Send NTP Multicast Packets

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type* *number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ntp multicast** {*ip-address* | *ipv6-address*} [**key** *key-id*] [**ttl** *value*] [**version** *number*] **Example:** `Router(config-if)# ntp multicast FF02::1:FF0E:8C6C`	Configures a system to send NTPv4 multicast packets on a specified interface. We support only IPv6 multicast addresses.

Configuring an Interface to Receive NTP Multicast Packets

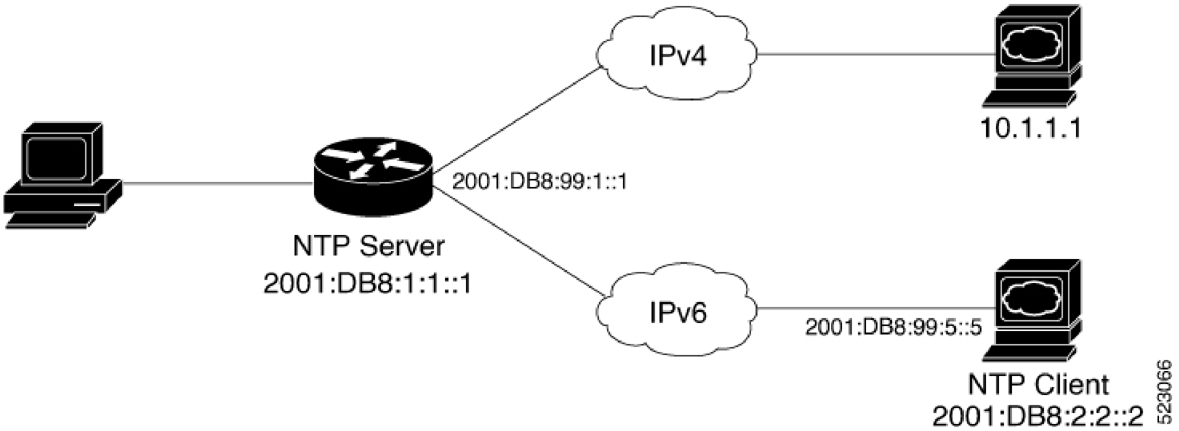
Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type* *number* **Example:** `Router(config)# interface FastEthernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.

	Command or Action	Purpose
Step 4	**ntp multicast client** {*ip-address* | *ipv6-address*} [**novolley**] **Example:** `Router(config-if)# ntp multicast client FF02::2:FF0E:8C6C`	Configures the system to receive NTP multicast packets on a specified interface. We support only IPv6 multicast addresses.

Configuring NTP for IPv6 Networks

The configuration is based on the following topology:



The following sections cover the NTP server and client configurations.

Configuring NTP on the Server

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ntp master** **Example:** `Router(config)#ntp master`	Enables NTP on the server.

	Command or Action	Purpose
Step 4	**ntp peer** *NTP client IPv6 address* **Example:** `Router(config)#ntp peer <2001:DB8::2>`	Specify the NTP client's IPv6 address on the server to send the synchronization request to the client.

Verification-NTP Server

This output shows that the NTP server clock synchronizes time with its own clock. The address 127.127.1.1 is the loopback IP address that is assigned by the **ntp master** command. The NTP server may take several minutes before it synchronizes its clock with itself.

```
NTPserver# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0011 Hz, precision is 2**10
ntp uptime is 60200 (1/100 of seconds), resolution is 4000
reference time is E78DDD9B.F7CEDBC0 (14:06:43.968 IST Wed Feb 8 2023)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 2.31 msec, peer dispersion is 1.20 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000004627 s/s
system poll interval is 16, last update was 10 sec ago.
```

This shows the peer device of the NTP server.

```
R2#show ntp associations
address         ref clock       st   when   poll reach  delay  offset   disp
~2001:DB8:2:2::2 .TIME.         16    -      64    0     0.000   0.000  15937.
*~127.127.1.1     .LOCL.        7     11     16   377    0.000   0.000  1.204
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Configuring NTP on the Client

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ntp client** **Example:** `Router(config)#ntp client`	Enables NTP on the client.
Step 4	**ntp peer** *NTP server IPv6 address* **Example:** `Router(config)#ntp server 2001:DB8::1`	Specify the server IPv6 address. The client listens to the synchronization request sent by the server, and synchronizes its clock with the server.

Verification-NTP Client

This output shows that the NTP client clock is synchronized with the NTP server. It also displays its stratum value and the IP address of the clock that it references.

```
NTPserver# show ntp status
Clock is synchronized, stratum 9, reference is 2001:DB8:1:1::1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 69300 (1/100 of seconds), resolution is 4000
reference time is E78DDDFB.99581208 (14:08:19.599 IST Wed Feb 8 2023)
clock offset is -6.5000 msec, root delay is 3.00 msec
root dispersion is 14.70 msec, peer dispersion is 2.56 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000199 s/s
system poll interval is 128, last update was 13 sec ago.
```

This output shows the peer device of the NTP client.

```
R2#show ntp associations
          address            ref clock      st   when   poll reach  delay  offset   disp
*~2001:DB8::12001:DB8::1     8     17    128   377  3.000  -6.500  2.565
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Configuring an External Reference Clock

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**line aux** *line-number* **Example:** `Device(config)# line aux 0`	Enters line configuration mode for the auxiliary port 0.

Step 4	**end**
	Example:
	`Device(config-line)# end`
		Exits line configuration mode and returns to privileged EXEC mode.

Step 5	**show ntp associations** **Example:** `Device# show ntp associations`	Displays the status of NTP associations, including the status of the GPS reference clock.

	Command or Action	Purpose
Step 6	**show ntp status** **Example:** `Device# show ntp status`	Displays the status of NTP.
Step 7	**debug ntp refclock** **Example:** `Device# debug ntp refclock`	Allows advanced monitoring of reference clock activities for the purposes of debugging.

Configuring NTP Authentication

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ntp authenticate** **Example:** `Device(config)# ntp authenticate`	Enables the NTP Authentication feature.
Step 4	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 5	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 6	**ntp authentication-key** *number* **md5** *key* **Example:**	Defines authentication keys. • Each key has a key number, a type, and a value.
Step 7	**ntp trusted-key** *key-number* [- *end-key*] **Example:**	Defines trusted authentication keys.

	Command or Action	Purpose
	`Device(config)# ntp trusted-key 1 - 3`	• If a key is trusted, this device will be ready to synchronize to a system that uses this key in its NTP packets.
Step 8	**ntp server** *ip-address* **key** *key-id* **Example:** `Device(config)# ntp server 172.16.22.44 key 2`	Allows the software clock to be synchronized by an NTP time server. **Note** When multiple NTP servers are configured and logging is enabled, clock synchronization lost messages are randomly seen on the device. To resolve this issue, configure the NTP server using **peer** keyword. `Device(config)# ntp server ip-address [version number] [key key-id] [prefer]`

Step 9	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Verifying Network Time Protocol

Procedure

Step 1 **show clock** [**detail**]

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

Example:

```
Device# show clock detail

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

Step 2 **show ntp associations detail**

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

Example:

```
Device# show ntp associations detail

192.168.10.1 configured, insane, invalid, unsynced, stratum 16
ref ID .INIT., time 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1900)
our mode active, peer mode unspec, our poll intvl 64, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 15940.56
```

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

Step 3 **show ntp status**

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

Example:

```
Device# show ntp status

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

Configuration Examples for Network Time Protocol

Example: Configuring Network Time Protocol

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

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

ntp server 192.168.13.57
ntp server 192.168.11.58
interface GigabitEthernet 0/0
 ntp broadcast
vines time use-system
```

In the following example, a device with a hardware clock has no outside time source, so it uses the hardware clock as an authoritative time source and distributes the time via NTP broadcast packets:

```
clock timezone MET 2
clock calendar-valid
ntp master
interface vlan 3
 ntp broadcast
```

The following example shows Line Aux 0 option is disabled by default.

```
config-register 0x0
reload
rommon 1 > set
rommon 2 >  AUX_PORT=1
rommon 3 > SYNC
rommon 4 > reset
rommon 1 > set
rommon 2 > confreg 0x2102
rommon 3 > reset
```

Additional References for Network Time Protocol

Related Documents

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

Standards and RFCs

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

Technical Assistance

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

Feature Information for Network Time Protocol

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

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

Table 16: Feature Information for Network Time Protocol

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