System Management Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 24.1.x , 24.2.x , 24.3.x , 24.4.x

First Published: 2023-11-30

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

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

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

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

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

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

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

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

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

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

© 2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xi

Changes to this Document xi

Communications, Services, and Additional Information xi

CHAPTER 1

New and Changed System Management Features 1

System Management Features Added or Modified in IOS XR Release 24.x.x 1

CHAPTER 2

YANG Data Models for System Management Features 3

Using YANG Data Models 3

CHAPTER 3

Configuring Manageability 5

Information about XML Manageability 5

How to Configure Manageability 5

Configuring the XML Agent 5

Configuration Examples for Manageability 6

Enabling VRF on an XML Agent: Examples 6

CHAPTER 4

Configuring Physical and Virtual Terminals 9

Prerequisites for Implementing Physical and Virtual Terminals 9

Information About Implementing Physical and Virtual Terminals 9

Line Templates 9

Line Template Configuration Mode 10

Line Template Guidelines 10

Terminal Identification 11

vty Pools 11

How to Implement Physical and Virtual Terminals on Cisco IOS XR Software 12

Modifying Templates 12
Creating and Modifying vty Pools 13
Monitoring Terminals and Terminal Sessions 15
Configuration Examples for Implementing Physical and Virtual Terminals 16

CHAPTER 5 **Configuring Simple Network Management Protocol 19**
Prerequisites for Implementing SNMP 19
Restrictions for SNMP use on Cisco IOS XR Software 19
Information about Implementing SNMP 20
SNMP Functional Overview 20
SNMP Manager 20
SNMP Agent 20
MIB 20
SNMP Versions 21
Comparison of SNMPv1, v2c, and v3 21
Security Models and Levels for SNMPv1, v2, v3 22
SNMPv3 Benefits 23
SNMPv3 Costs 23
User-Based Security Model 24
View-Based Access Control Model 24
IP Precedence and DSCP Support for SNMP 25
Session MIB support on subscriber sessions 25
SNMP Notifications 25
Session Types 26
How to Implement SNMP on Cisco IOS XR Software 27
Configuring SNMPv3 27
Configure to Drop Error PDUs 29
Configuring SNMPv3: Examples 30
Configuring SNMP Trap Notifications 34
Configure to Drop Error PDUs 35
Configuring Trap Notifications: Example 36
Setting the Contact, Location, and Serial Number of the SNMP Agent 37
Defining the Maximum SNMP Agent Packet Size 39
Changing Notification Operation Values 39

Setting IP Precedence and DSCP Values 41
Setting an IP Precedence Value for SNMP Traffic: Example 42
Setting an IP DSCP Value for SNMP Traffic: Example 42
Displaying SNMP Context Mapping 42
Monitoring Packet Loss 43
Configuring MIB Data to be Persistent 44
Configuring LinkUp and LinkDown Traps for a Subset of Interfaces 45
SNMP Context Mapping Configuration 47

CHAPTER 6 **Configuring Object Tracking 51**
Configuring Object Tracking 51
Prerequisites for Implementing Object Tracking 51
Information about Object Tracking 52
How to Implement Object Tracking 52
Tracking the Line Protocol State of an Interface 52
Tracking IP Route Reachability 54
Building a Track Based on a List of Objects 56
Building a Track Based on a List of Objects - Threshold Percentage 58
Building a Track Based on a List of Objects - Threshold Weight 60
Tracking IPSLA Reachability 62
Configuration Examples for Configuring Object Tracking 63
Additional References 65

CHAPTER 7 **Configuring Cisco Discovery Protocol 67**
Prerequisites for Implementing CDP 67
Information About Implementing CDP 67
How to Implement CDP on Cisco IOS XR Software 69
Enabling CDP 69
Modifying CDP Default Settings 70
Monitoring CDP 71
Examples 72
Configuration Examples for Implementing CDP 75

CHAPTER 8 **Configuring Periodic MIB Data Collection and Transfer 77**

Prerequisites for Periodic MIB Data Collection and Transfer 77
Information About Periodic MIB Data Collection and Transfer 77
SNMP Objects and Instances 77
Bulk Statistics Object Lists 78
Bulk Statistics Schemas 78
Bulk Statistics Transfer Options 78
Benefits of Periodic MIB Data Collection and Transfer 78
How to Configure Periodic MIB Data Collection and Transfer 79
Configuring a Bulk Statistics Object List 79
Configuring a Bulk Statistics Schema 80
Configuring Bulk Statistics Transfer Options 82
Periodic MIB Data Collection and Transfer: Example 85

CHAPTER 9 **Configuring Flexible Command Line Interface** 87
Flexible CLI Configuration Groups 87
Flexible Configuration Restrictions 87
Configuring a Configuration Group 89
Simple Configuration Group: Example 90
Configuration Group Applied to Different Places: Example 91
Verifying the Configuration of Configuration Groups 91
Regular Expressions in Configuration Groups 93
Configuration Examples Using Regular Expressions 100
Configuration Group with Regular Expression: Example 100
Configuration Group Inheritance with Regular Expressions: Example 102
Layer 2 Transport Configuration Group: Example 103
Configuration Group Precedence: Example 103
Changes to Configuration Group are Automatically Inherited: Example 104
Configuration Examples for Flexible CLI Configuration 104
Basic Flexible CLI Configuration: Example 104
Interface MTU Settings for Different Interface Types: Example 106
ACL Referencing: Example 108
Local Configuration Takes Precedence: Example 109
ISIS Hierarchical Configuration: Example 111
OSPF Hierarchy: Example 114

Link Bundling Usage: Example 117

CHAPTER 10 **Configuring Network Time Protocol 119**

Prerequisites for Implementing NTP on Cisco IOS XR Software 119

Best Practices for NTP configuration 119

Information About Implementing NTP 120

PTP-NTP Interworking 122

Enable PTP-NTP Interworking 122

Configuring Poll-Based Associations 123

Configuring Broadcast-Based NTP Associates 126

Configuring NTP Access Groups 128

Configuring NTP Authentication 130

Disabling NTP Services on a Specific Interface 132

Configuring the Source IP Address for NTP Packets 133

Configuring the System as an Authoritative NTP Server 135

FQDN for NTP Server 136

Configure FQDN for NTP server 136

Updating the Hardware Clock 137

Verifying the Status of the External Reference Clock 138

Examples 139

Configuration Examples for Implementing NTP 140

Configuring NTP server inside VRF interface 143

CHAPTER 11 **Configuring Precision Time Protocol 145**

PTP Overview 145

Restrictions for PTP 148

PTP Support Information 149

PTP Hardware Support 149

ITU-T Telecom Profiles for PTP 158

G.8265.1 158

G.8275.1 159

G.8275.2 160

Configure PTP 162

Configure Global G.8275.1 Profile 162

Configure PTP Master Interface 163
Configure PTP Slave Interface 164
Configure PTP Hybrid Mode 164
Configure PTP for SyncE and PTP Traceability 167
Configure PTP for SyncE and PTP Traceability 167
Configure PTP Telecom Profile Interface 168
Configure PTP Telecom Profile Clock 170
Configure PTP Delay Asymmetry 172
IEEE Default Profile 174
Example: Global PTP Configuration 175
Example: PTP Master Configuration 175
Example:PTP Slave Configuration 175
Performance Monitoring for PTP Networks 176
Configure PTP Performance Monitoring 179
Configuration Examples 181
Slave Configuration Example 181
Master Configuration Example 181
PTP Hybrid Mode Configuration Example 182
ITU-T Telecom Profile Examples: 182
G.8265.1 Profile Configuration Examples 182
G.8275.1 Profile Configuration Examples 184
G.8275.2 Profile Configuration Examples 185
Monitor PTP virtual port using PTP timeReceiver ports 187
Alarm conditions 188
Configure threshold to monitor PTP virtual port using PTP timeReceiver ports 189
Configuration example 189
Verify PTP virtual port using PTP timeReceiver ports 190
Restriction to monitor PTP virtual port using PTP timeReceiver ports 192
Configure E-SyncE on Primary and Secondary Interface 192

CHAPTER 12 **Synchronous Ethernet ESMC and SSM** 195
Frequency Synchronization Timing Concepts 195
Sources 195
Selection Points 196

Restrictions 197
SyncE Hardware Support 197
Configuring Frequency Synchronization 200
Enabling Frequency Synchronization on the Router 200
Configuring Frequency Synchronization on an Interface 200
Configuring Frequency Synchronization on a Clock Interface 200
SyncE Preference for PTP Receiver Interface 201
Configure SyncE Preference for PTP Receiver Interface 202
Verifying the Frequency Synchronization Configuration 203
Verifying the ESMC Configuration 205
Verifying Controllers Timing LEDs 206

CHAPTER 13 **Network Synchronization Design Best Practices 207**
Network Synchronization Design Best Practices 207
Network Synchronization Decision Tree 207
General Guidelines for Successful Synchronization Deployments 208
Guidelines for Phase Synchronization Deployments 209
PTP over IP Network Design 210
Selecting the Correct Profile For Network Synchronization 211
Reducing Asymmetry 212
Reducing Packet Delay Variation 212
Remediating Transport Asymmetry 212
Synchronizing Across Networks 212

CHAPTER 14 **Transparent PDH over Packet (TPoP) and Channelized SDH over Packet (CSoP) 215**
Restrictions for Smart SFP 215
Configuring TPoP and CSoP 217
VPWS with Smart SFP 219
Multi Router Automatic Protection Switching 219
Field-Pluggable Device (FPD) Version Upgrade for Smart SFP 221

CHAPTER 15 **Upgrading Field-Programmable Device 225**
Prerequisites for FPD Image Upgrades 225
Overview of FPD Image Upgrade Support 225

FPD upgrade service 226
Determining Upgrade Requirement 226
Manual FPD Upgrade 226
How to Upgrade FPD Images 227
Configuration Examples for FPD Image Upgrade 230
Auto FPD Upgrade 233
Limitations and Usage Guidelines 233
Automatic FPD Upgrade for PSU 235
Upgrade Failure 235

CHAPTER 16 **Configuration and File System Management** 237
Auto-Save Configuration 237
Configure Auto-Save 237
Increasing Commit Limit 237
Guidelines and Restrictions for Increasing the Commit Limit 239
Increasing the Rebase Limits 240
Perform ASCII Backup and Rest ASCII Backup Timer 240
Concurrent Configuration Rebase during Commit 241

Preface

This guide describes the System Management configuration details for Cisco IOS XR software. This chapter contains details on the changes made to this document.

- Changes to this Document, on page xi
- Communications, Services, and Additional Information, on page xi

Changes to this Document

Table 1: Changes to this Document

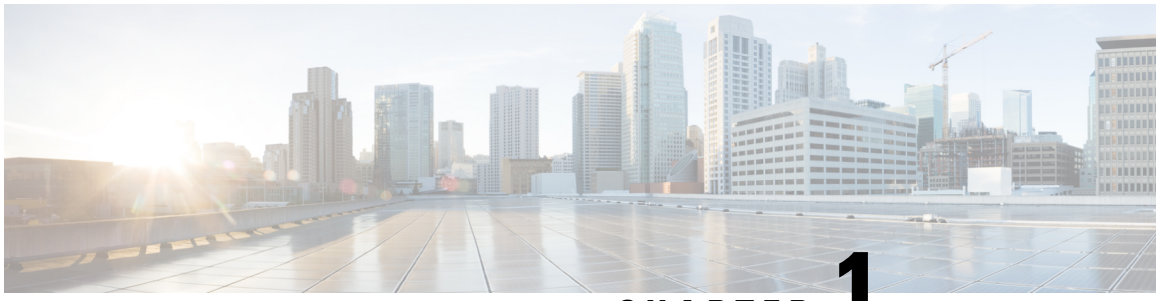
Date	Summary
February 2024	Initial release of this document

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

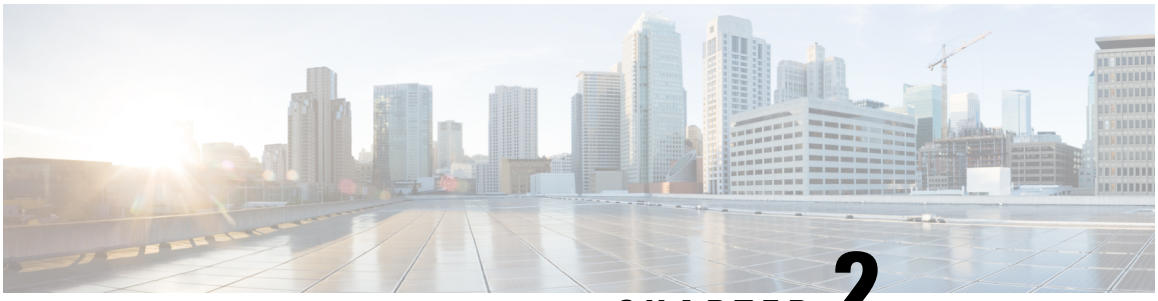
New and Changed System Management Features

This chapter lists all the features that have been added or modified in this guide. The table also contains references to these feature documentation sections.

- System Management Features Added or Modified in IOS XR Release 24.x.x, on page 1

System Management Features Added or Modified in IOS XR Release 24.x.x

Feature	Description	Changed in Release	Where Documented
Performance Monitoring for PTP Networks	This feature is introduced.	Release 24.3.1	Performance Monitoring for PTP Networks, on page 176
PTP-NTP Interworking	This feature is introduced.	Release 24.1.1	PTP-NTP Interworking, on page 122
PTP and SyncE on NC-57-48Q2D-S and NC-57-48Q2D-SE-S	This feature is introduced.	Release 24.2.1	PTP Hardware Support, on page 149
Increasing Commit Limit	This feature is introduced.	Release 24.2.1	Increasing Commit Limit, on page 237
Concurrent Configuration Rebase during Commit	This feature is introduced.	Release 24.3.1	Concurrent Configuration Rebase during Commit, on page 241



CHAPTER 2

YANG Data Models for System Management Features

This chapter provides information about the YANG data models for System Management features.

- Using YANG Data Models, on page 3

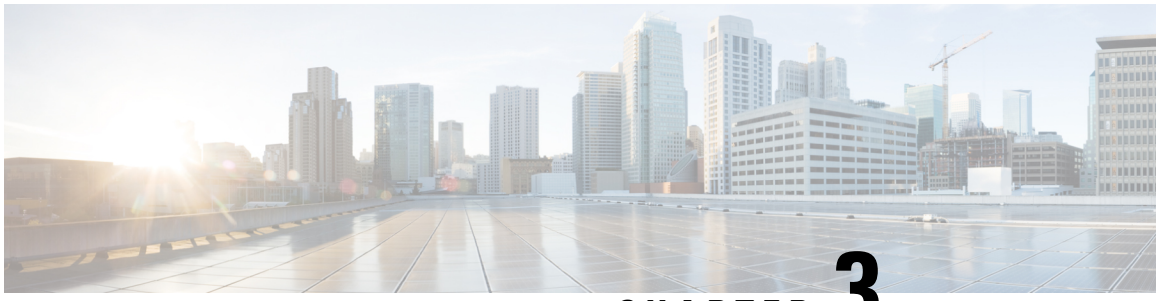
Using YANG Data Models

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

The data models are available in the release image, and are also published in the Github repository. Navigate to the release folder of interest to view the list of supported data models and their definitions. Each data model defines a complete and cohesive model, or augments an existing data model with additional XPaths. To view a comprehensive list of the data models supported in a release, navigate to the **Available-Content.md** file in the repository.

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

To get started with using the data models, see the *Programmability Configuration Guide*.



CHAPTER 3

Configuring Manageability

This module describes the configuration required to enable the Extensible Markup Language (XML) agent services. The XML Parser Infrastructure provides parsing and generation of XML documents with Document Object Model (DOM), Simple Application Programming Interface (API) for XML (SAX), and Document Type Definition (DTD) validation capabilities:

- DOM allows customers to programmatically create, manipulate, and generate XML documents.
- SAX supports user-defined functions for XML tags.
- DTD allows for validation of defined document types.

- Information about XML Manageability, on page 5
- How to Configure Manageability, on page 5
- Configuration Examples for Manageability, on page 6

Information about XML Manageability

The Cisco IOS XR Extensible Markup Language (XML) API provides a programmable interface to the router for use by external management applications. This interface provides a mechanism for router configuration and monitoring utilizing XML formatted request and response streams. The XML interface is built on top of the Management Data API (MDA), which provides a mechanism for Cisco IOS XR components to publish their data models through MDA schema definition files.

Cisco IOS XR software provides the ability to access the router via XML using a dedicated TCP connection, Secure Socket Layer (SSL), or a specific VPN routing and forwarding (VRF) instance.

How to Configure Manageability

Configuring the XML Agent

This explains how to configure the XML agent.

SUMMARY STEPS

1. **xml agent** [**ssl**]

2. **iteration on size** *iteration-size*
3. **session timeout** *timeout*
4. **throttle** {**memory** *size* | **process-rate** *tags*}
5. **vrf** { **vrfname** | **ipv4**} [**access-list** *access-list-name*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**xml agent** [**ssl**] **Example:** `RP/0/RP0/CPU0:router(config)# xml agent ssl`	Enables Extensible Markup Language (XML) requests over a dedicated TCP connection and enters XML agent configuration mode. Use the **ssl** keyword to enable XML requests over Secure Socket Layer (SSL).
Step 2	**iteration on size** *iteration-size* **Example:** `RP/0/RP0/CPU0:router(config-xml-agent)# iteration on size 500`	Configures the iteration size for large XML agent responses in KBytes. The default is 48.
Step 3	**session timeout** *timeout* **Example:** `RP/0/RP0/CPU0:router(config-xml-agent)# session timeout 5`	Configures an idle timeout for the XML agent in minutes. By default, there is no timeout.
Step 4	**throttle** {**memory** *size*	**process-rate** *tags*} **Example:** `RP/0/RP0/CPU0:router(config-xml-agent)# throttle memory 300`	Configures the XML agent processing capabilities. • Specify the memory size in Mbytes. Values can range from 100 to 600. The default is 300. • Specify the process-rate as the number of tags that the XML agent can process per second. Values can range from 1000 to 30000. By default the process rate is not throttled.
Step 5	**vrf** { **vrfname**	**ipv4**} [**access-list** *access-list-name*] **Example:** `RP/0/RP0/CPU0:router(config-xml-agent)# vrf vrf1`	Configures the dedicated agent or SSL agent to receive and send messages via the specified VPN routing and forwarding (VRF) instance.

Configuration Examples for Manageability

Enabling VRF on an XML Agent: Examples

The following example illustrates how to configure the dedicated XML agent to receive and send messages via VRF1, VRF2 and the default VRF:

```
RP/0/RP0/CPU0:router(config)# xml agent
RP/0/RP0/CPU0:router(config-xml-agent)# vrf VRF1
RP/0/RP0/CPU0:router(config-xml-agent)# vrf VRF2
```

The following example illustrates how to remove access to VRF2 from the dedicated agent:

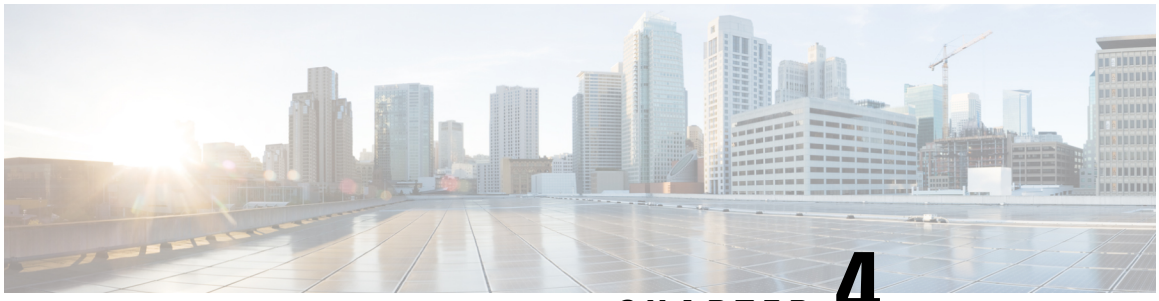
```
RP/0/RP0/CPU0:router(config)# xml agent ssl
RP/0/RP0/CPU0:router(config-xml-ssl)# vrf VRF1
RP/0/RP0/CPU0:router(config-xml-ssl-vrf)# vrf VRF2

RP/0/RP0/CPU0:router(config)# xml agent
RP/0/RP0/CPU0:router(config-xml-agent)# no vrf VRF1
```

The following example shows how to configure the XML SSL agent to receive and send messages through VRF1, VRF2 and the default VRF:

```
RP/0/RP0/CPU0:router(config)# xml agent ssl
RP/0/RP0/CPU0:router(config-xml-agent)# vrf VRF1
RP/0/RP0/CPU0:router(config-xml-agent)# vrf VRF2
```

The following example removes access for VRF2 from the dedicated XML agent:

```
RP/0/RP0/CPU0:router(config)# xml agent ssl
RP/0/RP0/CPU0:router(config-xml-agent)# no vrf VRF2
```



CHAPTER 4

Configuring Physical and Virtual Terminals

Line templates define standard attribute settings for incoming and outgoing transport over physical and virtual terminal lines (vtys). Vty pools are used to apply template settings to ranges of vtys.

This module describes the tasks you need to implement physical and virtual terminals on your Cisco IOS XR network.

- Prerequisites for Implementing Physical and Virtual Terminals, on page 9
- Information About Implementing Physical and Virtual Terminals, on page 9
- How to Implement Physical and Virtual Terminals on Cisco IOS XR Software, on page 12
- Configuration Examples for Implementing Physical and Virtual Terminals, on page 16

Prerequisites for Implementing Physical and Virtual Terminals

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Implementing Physical and Virtual Terminals

To implement physical and virtual terminals, you need to understand the concepts in this section.

Tip You can programmatically manage the physical and virtual terminals using `openconfig-system-terminal.yang` OpenConfig data model. To get started with using data models, see the *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

Line Templates

The following line templates are available in the Cisco IOS XR software.

- Default line template—The default line template that applies to a physical and virtual terminal lines.
- Console line template—The line template that applies to the console line.

- User-defined line templates—User-defined line templates that can be applied to a range of virtual terminal lines.

Line Template Configuration Mode

Changes to line template attributes are made in line template configuration mode. To enter line template configuration mode, issue the **line** command from XR Config mode, specifying the template to be modified. These line templates can be configured with the **line** command:

- console—console template
- default—default template
- template—user-defined template

After you specify a template with the **line** command, the router enters line template configuration mode where you can set the terminal attributes for the specified line. This example shows how to specify the attributes for the console:

```
RP/0/RP0/CPU0:router(config)# line console
RP/0/RP0/CPU0:router(config-line)#
```

From line template configuration mode, use the online help feature (**?**) to view all available options. Some useful options include:

- absolute-timeout—Specifies a timeout value for line disconnection.
- escape-character—Changes the line escape character.
- exec-timeout—Specifies the EXEC timeout.
- length—Sets the number of lines displayed on the screen.
- session-limit—Specifies the allowable number of outgoing connections.
- session-timeout—Specifies an interval for closing the connection if there is no input traffic.
- timestamp—Displays the timestamp before each command.
- width—Specifies the width of the display terminal.

Note The *default* session-limit for line template is applicable to Telnet sessions only. It is not applicable for SSH sessions.

Line Template Guidelines

The following guidelines apply to modifying the console template and to configuring a user-defined template:

- Modify the templates for the physical terminal lines on the router (the console port) from line template configuration mode. Use the **line console** command from XR Config mode to enter line template configuration mode for the console template.

- Modify the template for virtual lines by configuring a user-defined template with the **line** *template-name* command, configuring the terminal attributes for the user-defined template from line template configuration, and applying the template to a range of virtual terminal lines using the **vty pool** command.

Note Before creating or modifying the vty pools, enable the telnet server using the **telnet server** command in XR Config mode. See Cisco IOS XR IP Addresses and Services Configuration Guide and Cisco IOS XR IP Addresses and Services Command Reference for more information.

Terminal Identification

The physical terminal lines for the console port is identified by its location, expressed in the format of *rack*/*slot*/*module* , on the active or standby route processor (RP) where the respective console port resides. For virtual terminals, physical location is not applicable; the Cisco IOS XR software assigns a vty identifier to vtys according to the order in which the vty connection has been established.

vty Pools

Each virtual line is a member of a pool of connections using a common line template configuration. Multiple vty pools may exist, each containing a defined number of vtys as configured in the vty pool. The Cisco IOS XR software supports the following vty pools by default:

- Default vty pool—The default vty pool consists of five vtys (vtys 0 through 4) that each reference the default line template.
- Default fault manager pool—The default fault manager pool consists of six vtys (vtys 100 through 105) that each reference the default line template.

In addition to the default vty pool and default fault manager pool, you can also configure a user-defined vty pool that can reference the default template or a user-defined template.

When configuring vty pools, follow these guidelines:

- The vty range for the default vty pool must start at vty 0 and must contain a minimum of five vtys.
- The vty range from 0 through 99 can reference the default vty pool.
- The vty range from 5 through 99 can reference a user-defined vty pool.
- The vty range from 100 is reserved for the fault manager vty pool.
- The vty range for fault manager vty pools must start at vty 100 and must contain a minimum of six vtys.
- A vty can be a member of only one vty pool. A vty pool configuration will fail if the vty pool includes a vty that is already in another pool.
- If you attempt to remove an active vty from the active vty pool when configuring a vty pool, the configuration for that vty pool will fail.

How to Implement Physical and Virtual Terminals on Cisco IOS XR Software

Modifying Templates

This task explains how to modify the terminal attributes for the console and default line templates. The terminal attributes that you set will modify the template settings for the specified template.

SUMMARY STEPS

1. **configure**
2. **line** {**console** | **default**}
3. Configure the terminal attribute settings for the specified template using the commands in line template configuration mode.
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

Step 2	**line** {**console**	**default**}
		Example:
		`RP/0/RP0/CPU0:router(config)# line console`
		or
		`RP/0/RP0/CPU0:router(config)# line default`
			Enters line template configuration mode for the specified line template.
			• **console** —Enters line template configuration mode for the console template.
			• **default** —Enters line template configuration mode for the default line template.

Step 3	Configure the terminal attribute settings for the specified template using the commands in line template configuration mode.	—
Step 4	Use one of the following commands: • **end** • **commit**	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes:

	Command or Action	Purpose

	Example:
	`RP/0/RP0/CPU0:router(config-line)# end`
	or
	`RP/0/RP0/CPU0:router(config-line)# commit`
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Creating and Modifying vty Pools

This task explains how to create and modify vty pools.

You can omit Step 3 to Step 5 (**line template** and **exit** commands) if you are configuring the default line template to reference a vty pool.

SUMMARY STEPS

1. **configure**
2. **telnet** {**ipv4** | **ipv6**} **server max-servers** *limit*
3. **line template** *template-name*
4. Configure the terminal attribute settings for the specified line template using the commands in line template configuration mode.
5. **exit**
6. **vty-pool** {**default** | *pool-name* | **eem**} *first-vty last-vty* [**line-template** {**default** | *template-name*}]
7. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**telnet** {**ipv4** | **ipv6**} **server max-servers** *limit* **Example:** `RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers 10`	Specifies the number of allowable Telnet servers. Up to 100 Telnet servers are allowed. **Note** By default no Telnet servers are allowed. You must configure this command in order to enable the use of Telnet servers.
Step 3	**line template** *template-name* **Example:** `RP/0/RP0/CPU0:router(config)# line template 1`	Enters line template configuration mode for a user-defined template.
Step 4	Configure the terminal attribute settings for the specified line template using the commands in line template configuration mode.	—
Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(config-line)# exit`	Exits line template configuration mode and returns the router to global configuration mode.

Step 6	**vty-pool** {**default** | *pool-name* | **eem**} *first-vty last-vty* [**line-template** {**default** | *template-name*}]
	Example:
	`RP/0/RP0/CPU0:router(config)#vty-pool default 0 5 line-template default`
	or
	`RP/0/RP0/CPU0:router(config)#vty-pool pool1 5 50 line-template template1`
	or
	`RP/0/RP0/CPU0:router(config)#vty-pool eem 100 105 line-template template1`
	`RP/0/RP0/CPU0:router(config)#vty-pool default 0 5 line-template template1`
		Creates or modifies vty pools.
		• If you do not specify a line template with the **line-template** keyword, a vty pool defaults to the default line template.
		• **default** —Configures the default vty pool.
		  • The default vty pool must start at vty 0 and must contain a minimum of five vtys (vtys 0 through 4).
		  • You can resize the default vty pool by increasing the range of vtys that compose the default vty pool.
		• *pool-name* —Creates a user-defined vty pool.
		  • A user-defined pool must start at least at vty 5, depending on whether the default vty pool has been resized.
		  • If the range of vtys for the default vty pool has been resized, use the first range value free from the default line template. For example, if the range of vtys for the default vty pool has been configured to include 10 vtys (vty 0 through 9), the range value for the user-defined vty pool must start with vty 10.

	Command or Action	Purpose
		• **eem** —Configures the embedded event manager pool. • The default embedded event manager vty pool must start at vty 100 and must contain a minimum of six vtys (vtys 100 through 105). • **line-template** *template-name* —Configures the vty pool to reference a user-defined template.
Step 7	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Monitoring Terminals and Terminal Sessions

This task explains how to monitor terminals and terminal sessions using the **show** EXEC commands available for physical and terminal lines.

Note The commands can be entered in any order.

SUMMARY STEPS

1. (Optional) **show line** [**aux location** *node-id* | **console location** *node-id* | **vty** *number*]
2. (Optional) **show terminal**
3. (Optional) **show users**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	(Optional) **show line** [**aux location** *node-id*	**console location** *node-id*	**vty** *number*] **Example:** `RP/0/RP0/CPU0:router# show line`	Displays the terminal parameters of terminal lines. • Specifying the **show line aux location** *node-id* EXEC command displays the terminal parameters of the auxiliary line.

	Command or Action	Purpose

		• Specifying the **show line console location** *node-id* EXEC command displays the terminal parameters of the console.
		  • For the **location** *node-id* keyword and argument, enter the location of the Route Processor (RP) on which the respective auxiliary or console port resides.
		  • The *node-id* argument is expressed in the format of *rack*/*slot*/*module* .
		• Specifying the **show line vty** *number* EXEC command displays the terminal parameters for the specified vty.

Step 2	(Optional) **show terminal** **Example:** `RP/0/RP0/CPU0:router# show terminal`	Displays the terminal attribute settings for the current terminal line.
Step 3	(Optional) **show users** **Example:** `RP/0/RP0/CPU0:router# show users`	Displays information about the active lines on the router.

Configuration Examples for Implementing Physical and Virtual Terminals

Modifying the Console Template: Example

This configuration example shows how to modify the terminal attribute settings for the console line template:

```
RP/0/RP0/CPU0:router# show running-config line console
line console
  exec-timeout 0 0
  escape-character 0x5a
  session-limit 10
  disconnect-character 0x59
  session-timeout 100
  transport input telnet
  transport output telnet
```

In this configuration example, the following terminal attributes are applied to the console line template:

- The EXEC time out for terminal sessions is set to 0 minutes, 0 seconds. Setting the EXEC timeout to 0 minutes and 0 seconds disables the EXEC timeout function; thus, the EXEC session for the terminal session will never time out.
- The escape character is set to the 0x5a hexadecimal value (the 0x5a hexadecimal value translates into the “Z” character).
- The session limit for outgoing terminal sessions is set to 10 connections.
- The disconnect character is set to 0x59 hexadecimal value (the 0x59 hexadecimal character translates into the “Y” character).
- The session time out for outgoing terminal sessions is set to 100 minutes (1 hour and 40 minutes).
- The allowed transport protocol for incoming terminal sessions is Telnet.
- The allowed transport protocol for outgoing terminal sessions is Telnet.

To verify that the terminal attributes for the console line template have been applied to the console, use the **show line** command:

```
RP/0/RP0/CPU0:router:router# show line console location 0/0/CPU0
Tue Nov 24 03:10:24.656 UTC
Tty             Speed     Overruns           Acc I/O
*con0/0/CPU0      9600       0/0               -/-

Line "con0_RP1_CPU0", Location "0/RP1/CPU0", Type "Console"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600, "No" Parity, 2 stopbits, 8 databits
Template: console
Capabilities: Timestamp Enabled
Allowed transports are telnet.
```

Modifying the Default Template: Example

This configuration example shows how to override the terminal settings for the default line template:

```
line default
  exec-timeout 0 0
  width 512
  length 512
```

In this example, the following terminal attributes override the default line template default terminal attribute settings:

- The EXEC timeout for terminal sessions is set to 0 minutes and 0 seconds. Setting the EXEC timeout to 0 minutes and 0 seconds disables the EXEC timeout function; thus, the EXEC session for the terminal session will never time out (the default EXEC timeout for the default line template is 10 minutes).
- The width of the terminal screen for the terminals referencing the default template is set to 512 characters (the default width for the default line template is 80 characters).
- The length, the number of lines that will display at one time on the terminal referencing the default template, is set to 512 lines (the default length for the default line template is 24 lines).

Configuring a User-Defined Template to Reference the Default vty Pool: Example

This configuration example shows how to configure a user-defined line template (named test in this example) for vtys and to configure the line template test to reference the default vty pool:

```
line template test
  exec-timeout 100 0
  width 100
  length 100
  exit
vty-pool default 0 4 line-template test
```

Configuring a User-Defined Template to Reference a User-Defined vty Pool: Example

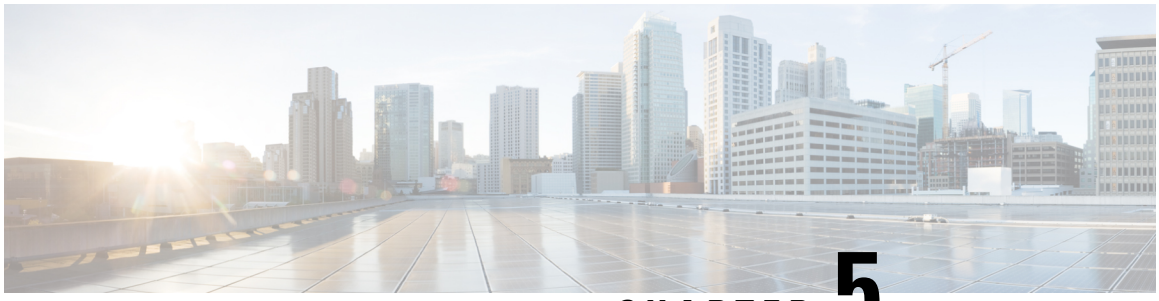
This configuration example shows how to configure a user-defined line template (named test2 in this example) for vtys and to configure the line template test to reference a user-defined vty pool (named pool1 in this example):

```
line template test2
  exec-timeout 0 0
  session-limit 10
  session-timeout 100
  transport input all
  transport output all
  exit
vty-pool pool1 5 50 line-template test2
```

Configuring a User-Defined Template to Reference the Fault Manager vty Pool: Example

This configuration example shows how to configure a user-defined line template (named test3 in this example) for vtys and to configure the line template test to reference the fault manager vty pool:

```
line template test3
  width 110
  length 100
  session-timeout 100
  exit
  vty-pool eem 100 105 line-template test3
```



CHAPTER 5

Configuring Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

This module describes the tasks you need to implement SNMP on your Cisco IOS XR network.

- Prerequisites for Implementing SNMP, on page 19
- Restrictions for SNMP use on Cisco IOS XR Software, on page 19
- Information about Implementing SNMP, on page 20
- Session MIB support on subscriber sessions , on page 25
- How to Implement SNMP on Cisco IOS XR Software, on page 27
- SNMP Context Mapping Configuration, on page 47

Prerequisites for Implementing SNMP

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for SNMP use on Cisco IOS XR Software

SNMP outputs are only 32-bits wide and therefore cannot display any information greater than 2^{32}. 2^{32} is equal to 4.29 Gigabits.

Note A 10 Gigabit interface is greater than 2^{32}, so if you are trying to display speed information regarding the interface, you might see concatenated results.

To display correct speed of an interface greater than 10 Gigabit, ifHighSpeed can be used.

The recommended maximum number of object identifiers (OIDs) that can be accommodated in a single SNMP request is 75. A request with more than 75 OIDs can result in SNMP requests being dropped with SNMP polling timeout.

Information about Implementing SNMP

To implement SNMP, you need to understand the concepts described in this section.

SNMP Functional Overview

The SNMP framework consists of three parts:

- SNMP manager
- SNMP agent
- Management Information Base (MIB)

SNMP Manager

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a *network management system* (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks 2000 line of products).

SNMP Agent

The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the router. To enable the SNMP agent, you must define the relationship between the manager and the agent.

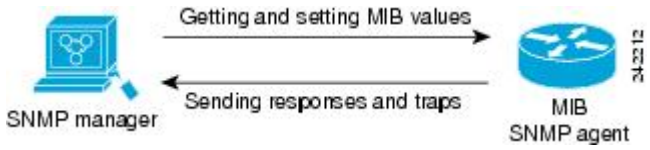
MIB

The *Management Information Base* (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects. Within the MIB there are collections of related objects, defined in MIB modules. MIB modules are written in the SNMP MIB module language, as defined in STD 58, RFC 2578, RFC 2579, and RFC 2580. Note that individual MIB modules are also referred to as MIBs; for example, the Interfaces Group MIB (IF-MIB) is a MIB module within the MIB on your system.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change through Get or Set operations. A manager can get a value from an agent or store a value into that agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to manager requests to get or set data.

This figure illustrates the communications relationship between the SNMP manager and agent. A manager can send the agent requests to get and set MIB values. The agent can respond to these requests. Independent of this interaction, the agent can send unsolicited notifications (traps) to the manager to notify the manager of network conditions.

Figure 1: Communication Between an SNMP Agent and Manager



SNMP Versions

Cisco IOS XR software supports the following versions of SNMP:

- Simple Network Management Protocol Version 1 (SNMPv1)
- Simple Network Management Protocol Version 2c (SNMPv2c)
- Simple Network Management Protocol Version 3 (SNMPv3)

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is defined by an IP address access control list and password.

SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

SNMPv3 is a security model. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when an SNMP packet is handled. See Security Models and Levels for SNMPv1, v2, v3, on page 22 for a list of security levels available in SNMPv3. The SNMPv3 feature supports RFCs 3411 to 3418.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS-XR software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Comparison of SNMPv1, v2c, and v3

SNMP v1, v2c, and v3 all support the following operations:

- get-request—Retrieves a value from a specific variable.
- get-next-request—Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
- get-response—Operation that replies to a get-request, get-next-request, and set-request sent by an NMS.
- set-request—Operation that stores a value in a specific variable.
- trap—Unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

This table identifies other key SNMP features supported by the SNMP v1, v2c, and v3.

Table 2: SNMPv1, v2c, and v3 Feature Support

Feature	SNMP v1	SNMP v2c	SNMP v3
Get-Bulk Operation	No	Yes	Yes

Feature	SNMP v1	SNMP v2c	SNMP v3
Inform Operation	No	Yes (No on the Cisco IOS XR software)	Yes (No on the Cisco IOS XR software)
64 Bit Counter	No	Yes	Yes
Textual Conventions	No	Yes	Yes
Authentication	No	No	Yes
Privacy (Encryption)	No	No	Yes
Authorization and Access Controls (Views)	No	No	Yes

Security Models and Levels for SNMPv1, v2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

The below table identifies what the combinations of security models and levels mean.

Table 3: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the HMAC[1]-MD5[2] algorithm or the HMAC-SHA[3].
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES[4] 56-bit encryption in addition to authentication based on the CBC[5] DES (DES-56) standard.

Model	Level	Authentication	Encryption	What Happens
v3	authPriv	HMAC-MD5 or HMAC-SHA	3DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 168-bit 3DES[6] level of encryption.
v3	authPriv	HMAC-MD5 or HMAC-SHA	AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides 128-bit AES[7] level of encryption.

1 Hash-Based Message Authentication Code
2 Message Digest 5
3 Secure Hash Algorithm
4 Data Encryption Standard
5 Cipher Block Chaining
6 Triple Data Encryption Standard
7 Advanced Encryption Standard

Use of 3DES and AES encryption standards requires that the security package (k9sec) be installed. For information on installing software packages, see *Upgrading and Managing Cisco IOS XR Software*.

SNMPv3 Benefits

SNMPv3 provides secure access to devices by providing authentication, encryption and access control. These added security benefits secure SNMP against the following security threats:

- Masquerade—The threat that an SNMP user may assume the identity of another SNMP user to perform management operations for which that SNMP user does not have authorization.
- Message stream modification—The threat that messages may be maliciously reordered, delayed, or replayed (to an extent that is greater than can occur through the natural operation of a subnetwork service) to cause SNMP to perform unauthorized management operations.
- Disclosure—The threat that exchanges between SNMP engines could be eavesdropped. Protecting against this threat may be required as a matter of local policy.

In addition, SNMPv3 provides access control over protocol operations on SNMP managed objects.

SNMPv3 Costs

SNMPv3 authentication and encryption contribute to a slight increase in the response time when SNMP operations on MIB objects are performed. This cost is far outweighed by the security advantages provided by SNMPv3.

This table shows the order of response time (from least to greatest) for the various security model and security level combinations.

Table 4: Order of Response Times from Least to Greatest

Security Model	Security Level
SNMPv2c	noAuthNoPriv
SNMPv3	noAuthNoPriv

Security Model	Security Level
SNMPv3	authNoPriv
SNMPv3	authPriv

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

USM uses two authentication protocols:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

USM uses Cipher Block Chaining (CBC)-DES (DES-56) as the privacy protocol for message encryption.

View-Based Access Control Model

The View-Based Access Control Model (VACM) enables SNMP users to control access to SNMP managed objects by supplying read, write, or notify access to SNMP objects. It prevents access to objects restricted by views. These access policies can be set when user groups are configured with the **snmp-server group** command.

MIB Views

For security reasons, it is often valuable to be able to restrict the access rights of some groups to only a subset of the management information within the management domain. To provide this capability, access to a management object is controlled through MIB views, which contain the set of managed object types (and, optionally, the specific instances of object types) that can be viewed.

Access Policy

Access policy determines the access rights of a group. The three types of access rights are as follows:

- read-view access—The set of object instances authorized for the group when objects are read.
- write-view access—The set of object instances authorized for the group when objects are written.
- notify-view access—The set of object instances authorized for the group when objects are sent in a notification.

IP Precedence and DSCP Support for SNMP

SNMP IP Precedence and differentiated services code point (DSCP) support delivers QoS specifically for SNMP traffic. You can change the priority setting so that SNMP traffic generated in a router is assigned a specific QoS class. The IP Precedence or IP DSCP code point value is used to determine how packets are handled in weighted random early detection (WRED).

After the IP Precedence or DSCP is set for the SNMP traffic generated in a router, different QoS classes cannot be assigned to different types of SNMP traffic in that router.

The IP Precedence value is the first three bits in the type of service (ToS) byte of an IP header. The IP DSCP code point value is the first six bits of the differentiate services (DiffServ Field) byte. You can configure up to eight different IP Precedence markings or 64 different IP DSCP markings.

Session MIB support on subscriber sessions

SNMP monitoring requires information about subscribers of all types. The CISCO-SUBSCRIBER-SESSION-MIB is defined to model per-subscriber data as well as aggregate subscriber (PPPoE) data. It is required to support notifications (traps) for aggregate session counts crossing configured thresholds. Generic MIB Data Collector Manager (DCM) support for CISCO-SUBSCRIBER-SESSION-MIB, helps faster data collection and also better handling of parallel data.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. On Cisco IOS XR software, unsolicited (asynchronous) notifications can be generated only as *traps*. Traps are messages alerting the SNMP manager to a condition on the network. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Note Inform requests (inform operations) are supported in Cisco IOS XR software.

Traps are less reliable than informs because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, traps are often preferred because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, and an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources.

Figure 2: Trap Received by the SNMP Manager

In this illustration, the agent router sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

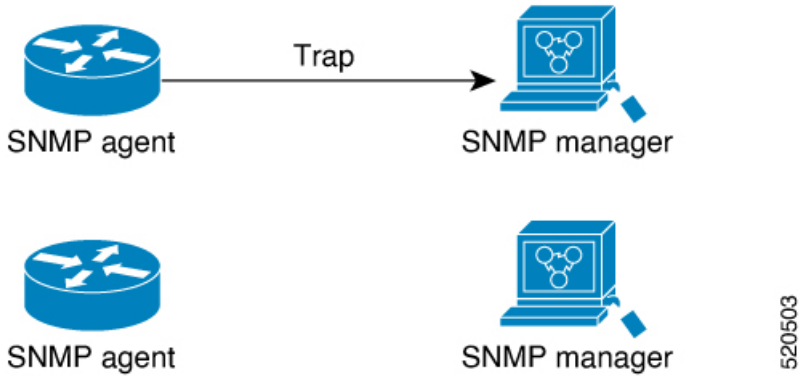
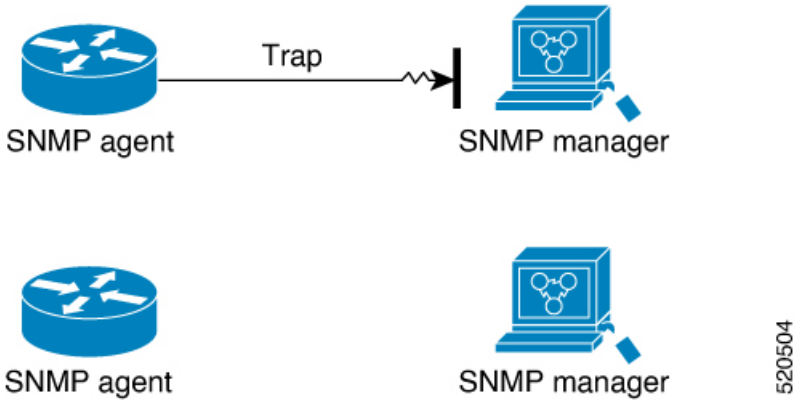


Figure 3: Trap Not Received by the SNMP Manager

In this illustration, the agent sends a trap to the manager, but the trap does not reach the manager. Because the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.



Note Previously, the SNMP agent would drop traps after 5 minutes if the respective hosts were unreachable. In its new behavior, the SNMP agent now sends traps to all unreachable hosts instead of dropping them. There is no change in the trap delay timer behavior.

Session Types

The supported session types are:

- PPPoE
- IP SUB PKT
- IP SUB DHCP

How to Implement SNMP on Cisco IOS XR Software

This section describes how to implement SNMP.

The **snmp-server** commands enable SNMP on Management Ethernet interfaces by default. For information on how to enable SNMP server support on other inband interfaces, see the *Implementing Management Plane Protection on Cisco IOS XR Software* module in *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Configuring SNMPv3

This task explains how to configure SNMPv3 for network management and monitoring.

Note No specific command enables SNMPv3; the first **snmp-server** global configuration command (config), that you issue enables SNMPv3. Therefore, the sequence in which you issue the **snmp-server** commands for this task does not matter.

SUMMARY STEPS

1. **configure**
2. (Optional) **snmp-server engineid local** *engine-id*
3. (Optional) **snmp-server vrf** *vrf-name*
4. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
5. **snmp-server group** *name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *view*] [**write** *view*] [**notify** *view*] [*access-list-name*]
6. **snmp-server user** *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv des56** {**clear** | **encrypted**} *priv-password*]]} [*access-list-name*]
7. Use the **commit** or **end** command.
8. (Optional) **show snmp**
9. (Optional) **show snmp engineid**
10. (Optional) **show snmp group**
11. (Optional) **show snmp users**
12. (Optional) **show snmp view**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	(Optional) **snmp-server engineid local** *engine-id* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:61`	Specifies the identification number of the local SNMP engine.
Step 3	(Optional) **snmp-server vrf** *vrf-name* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server vrf vrfa`	Configures VRF properties of SNMP.
Step 4	**snmp-server view** *view-name oid-tree* {**included** | **excluded**} **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server view view_name 1.3.6.1.2.1.1.5 included`	Creates or modifies a view record.
Step 5	**snmp-server group** *name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *view*] [**write** *view*] [**notify** *view*] [*access-list-name*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server group group_name v3 noauth read view_name1 write view_name2`	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
Step 6	**snmp-server user** *username groupname* {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} {**clear** | **encrypted**} *auth-password* [**priv des56** {**clear** | **encrypted**} *priv-password*]]} [*access-list-name*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server user noauthuser group_name v3`	Configures a new user to an SNMP group.
Step 7	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

	Command or Action	Purpose
Step 8	(Optional) **show snmp** **Example:** `RP/0/RP0/CPU0:router# show snmp`	Displays information about the status of SNMP.
Step 9	(Optional) **show snmp engineid** **Example:** `RP/0/RP0/CPU0:router# show snmp engineid`	Displays information about the local SNMP engine.
Step 10	(Optional) **show snmp group** **Example:** `RP/0/RP0/CPU0:router# show snmp group`	Displays information about each SNMP group on the network.
Step 11	(Optional) **show snmp users** **Example:** `RP/0/RP0/CPU0:router# show snmp users`	Displays information about each SNMP username in the SNMP users table.
Step 12	(Optional) **show snmp view** **Example:** `RP/0/RP0/CPU0:router# show snmp view`	Displays information about the configured views, including the associated MIB view family name, storage type, and status.

Configure to Drop Error PDUs

Perform this configuration to avoid error PDUs being sent out of router when polled with incorrect SNMPv3 user name. If the configuration is not set, it will respond with error PDUs by default. After applying this configuration, when router is polled with unknown SNMPv3 user name, the NMS will get time out instead of getting unknown user name error code.

SUMMARY STEPS

1. **configure**
2. **snmp-server drop unknown-user**
3. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router# configure`	
Step 2	**snmp-server drop unknown-user** **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server drop unknown-user`	Drop the error PDUs when the router is polled with incorrect SNMPv3 user name.
Step 3	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Configuring SNMPv3: Examples

Setting an Engine ID

This example shows how to set the identification of the local SNMP engine:

```
config
snmp-server engineID local 00:00:00:09:00:00:00:a1:61:6c:20:61
```

Note After the engine ID has been configured, the SNMP agent restarts.

Verifying the Identification of the Local SNMP Engines

This example shows how to verify the identification of the local SNMP engine:

```
show snmp engineid

SNMP engineID 00000009000000a1ffffffff
```

Creating a View

There are two ways to create a view:

- You can include the object identifier (OID) of an ASN.1 subtree of a MIB family from a view by using the **included** keyword of the **snmp-server view** command.
- You can exclude the OID subtree of the ASN.1 subtree of a MIB family from a view by using the **excluded** keyword of the **snmp-server view** command.

This example shows how to create a view that includes the sysName (1.3.6.1.2.1.1.5) object:

```
config
  snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1.5 included
```

This example shows how to create a view that includes all the OIDs of a system group:

```
config
  snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included
```

This example shows how to create a view that includes all the OIDs under the system group except the sysName object (1.3.6.1.2.1.1.5), which has been excluded:

```
config
  snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included
  snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1.5 excluded
```

Verifying Configured Views

This example shows how to display information about the configured views:

```
RP/0/RP0/CPU0:router# show snmp view

  v1default 1.3.6.1 - included nonVolatile active
  SNMP_VIEW1 1.3.6.1.2.1.1 - included nonVolatile active
  SNMP_VIEW1 1.3.6.1.2.1.1.5 - excluded nonVolatile active
```

Creating Groups

If you do not explicitly specify a notify, read, or write view, the Cisco IOS XR software uses the v1 default (1.3.6.1). This example shows how to create a group that utilizes the default view:

```
RP/0/RP0/CPU0:router# snmp-server group group-name v3 auth
```

The following configuration example shows how to create a group that has read access to all the OIDs in the system except the sysUpTime object (1.3.6.1.2.1.1.3), which has been excluded from the view applied to the group, but write access only to the sysName object (1.3.6.1.2.1.1.5):

```
!
  snmp-server view view_name1 1.3.6.1.2.1.1 included
  snmp-server view view_name1 1.3.6.1.2.1.1.3 excluded
  snmp-server view view_name2 1.3.6.1.2.1.1.5 included
  snmp-server group group_name1 v3 auth read view_name1 write view_name2
```

```
!
```

Verifying Groups

This example shows how to verify the attributes of configured groups:

```
RP/0/RP0/CPU0:router# show snmp group

  groupname: group_name1                  security model:usm
  readview : view_name1                   writeview: view_name2
  notifyview: v1default
  row status: nonVolatile
```

Creating and Verifying Users

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!
  snmp-server view view_name 1.3.6.1.2.1.1 included
  snmp-server group group_name v3 noauth read view_name write view-name
  !
```

This example shows how to create a noAuthNoPriv user with read and write view access to a system group:

```
config
  snmp-server user noauthuser group_name v3
```

Note The user must belong to a noauth group before a noAuthNoPriv user can be created.

This example shows how to verify the attributes that apply to the SNMP user:

```
RP/0/RP0/CPU0:router# show snmp user

  User name: noauthuser
  Engine ID: localSnmpID
  storage-type: nonvolatile active
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!
  snmp-server view SNMP_VIEW1 1.3.6.1.2.1.1 included
  snmp-server group SNMP_GROUP1 v3 auth notify SNMP_VIEW1 read SNMP_VIEW1 write SNMP_VIEW1
 !
```

This example shows how to create a user with authentication (including encryption), read, and write view access to a system group:

```
config
```

```
snmp-server user userv3authpriv SNMP_GROUP1 v3 auth md5 password123 priv aes 128 password123
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!
  snmp-server view view_name 1.3.6.1.2.1.1 included
  snmp group group_name v3 priv read view_name write view_name
  !
```

This example shows how to create authNoPriv user with read and write view access to a system group:

```
RP/0/RP0/CPU0:router# snmp-server user authuser group_name v3 auth md5 clear auth_passwd
```

Note Because the group is configured at a security level of Auth, the user must be configured as "auth" at a minimum to access this group ("priv" users could also access this group). The authNoPriv user configured in this group, authuser, must supply an authentication password to access the view. In the example, auth_passwd is set as the authentication password string. Note that **clear** keyword is specified before the auth_passwd password string. The **clear** keyword indicates that the password string being supplied is unencrypted.

This example shows how to verify the attributes that apply to SNMP user:

```
RP/0/RP0/CPU0:router# show snmp user

  User name: authuser
  Engine ID: localSnmpID
  storage-type: nonvolatile active
```

Given the following SNMPv3 view and SNMPv3 group configuration:

```
!
  snmp view view_name 1.3.6.1.2.1.1 included
  snmp group group_name v3 priv read view_name write view_name
  !
```

This example shows how to create an authPriv user with read and write view access to a system group:

```
config
  snmp-server user privuser group_name v3 auth md5 clear auth_passwd priv des56 clear
priv_passwd
```

Note Because the group has a security level of Priv, the user must be configured as a "priv" user to access this group. In this example, the user, privuser, must supply both an authentication password and privacy password to access the OIDs in the view.

This example shows how to verify the attributes that apply to the SNMP user:

```
RP/0/RP0/CPU0:router# show snmp user

  User name: privuser
  Engine ID: localSnmpID
  storage-type: nonvolatile active
```

Configuring SNMP Trap Notifications

This task explains how to configure the router to send SNMP trap notifications.

Note You can omit #unique_58 if you have already completed the steps documented under the #unique_58 task.

SUMMARY STEPS

1. **configure**
2. **snmp-server group** *name* {**v1 v2 v3** {**auth** | **noauth** | **priv**}} [**read** *view*] **write** *view*] [**notify** *view*] [*access-list-name*]
3. **snmp-server user** *username groupname* {**v1 v2c v3** {**auth** | **md5** | **sha**} {**clear** | **encrypted**} *auth-password*] [**priv des56** {**clear** | *access-list-name*]
4. [**snmp-server host** *address* [**traps**] [**version** {**1** | **2c** | **3** [**auth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
5. **snmp-server traps** [*notification-type*]
6. Use the **commit** or **end** command.
7. (Optional) **show snmp host**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**snmp-server group** *name* {**v1 v2 v3** {**auth**	**noauth**	**priv**}} [**read** *view*] **write** *view*] [**notify** *view*] [*access-list-name*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server group group_name v3 noauth read view_name1 writer view_name2`	Configures a new SNMP group or a table that maps SNMP users to SNMP views.

	Command or Action	Purpose
Step 3	**snmp-server user** *username groupname* {**v1 v2c v3** {**auth** | **md5** | **sha**} {**clear** | **encrypted**} *auth-password*] [**priv des56** {**clear** | *access-list-name*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server group group_name v3 noauth read view_name1 writer view_name2`	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
Step 4	[**snmp-server host** *address* [**traps**] [**version** {**1** | **2c** | **3** [**auth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server host 12.26.25.61 traps version 3 noauth userV3noauth`	Specifies SNMP trap notifications, the version of SNMP to use, the security level of the notifications, and the recipient (host) of the notifications.
Step 5	**snmp-server traps** [*notification-type*] **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server traps bgp`	Enables the sending of trap notifications and specifies the type of trap notifications to be sent. • If a trap is not specified with the *notification-type* argument, all supported trap notifications are enabled on the router. To display which trap notifications are available on your router, enter the **snmp-server traps ?** command.
Step 6	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.
Step 7	(Optional) **show snmp host** **Example:** `RP/0/RP0/CPU0:router# show snmp host`	Displays information about the configured SNMP notification recipient (host), port number, and security model.

Configure to Drop Error PDUs

Perform this configuration to avoid error PDUs being sent out of router when polled with incorrect SNMPv3 user name. If the configuration is not set, it will respond with error PDUs by default. After applying this

configuration, when router is polled with unknown SNMPv3 user name, the NMS will get time out instead of getting unknown user name error code.

SUMMARY STEPS

1. **configure**
2. **snmp-server drop unknown-user**
3. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**snmp-server drop unknown-user** **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server drop unknown-user`	Drop the error PDUs when the router is polled with incorrect SNMPv3 user name.
Step 3	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Configuring Trap Notifications: Example

The following example configures an SNMP agent to send out different types of traps. The configuration includes a v2c user, a noAuthNoPriv user, anauthNoPriv user, and an AuthPriv user.

Note The default User Datagram Protocol (UDP) port is 161. If you do not a specify a UDP port with the **udp-port** keyword and *port* argument, then the configured SNMP trap notifications are sent to port 161.

```
!
  snmp-server host 10.50.32.170 version 2c public udp-port 2345
  snmp-server host 10.50.32.170 version 3 auth userV3auth udp-port 2345
  snmp-server host 10.50.32.170 version 3 priv userV3priv udp-port 2345
  snmp-server host 10.50.32.170 version 3 noauth userV3noauth udp-port 2345
  snmp-server user userv2c groupv2c v2c
  snmp-server user userV3auth groupV3auth v3 auth md5 encrypted 140F0A13
 snmp-server user userV3priv groupV3priv v3 auth md5 encrypted 021E1C43 priv des56 encrypted
1110001C
  snmp-server user userV3noauth groupV3noauth v3 LROwner
  snmp-server view view_name 1.3 included
  snmp-server community public RW
  snmp-server group groupv2c v2c read view_name
  snmp-server group groupV3auth v3 auth read view_name
  snmp-server group groupV3priv v3 priv read view_name
  snmp-server group groupV3noauth v3 noauth read view_name
  !
```

In the following example, the output of the **show snmp host** commaand shows how to verify the configuration SNMP trap notification recipients host, the recipients of SNMP trap notifications. The output displays the following information:

- IP address of the configured notification host
- UDP port where SNMP notification messages are sent
- Type of trap configured
- Security level of the configured user
- Security model configured

```
Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3auth security model: v3 auth

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3noauth security model: v3 noauth

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userV3priv security model: v3 priv

Notification host: 10.50.32.170 udp-port: 2345 type: trap
user: userv2c security model: v2c
```

Setting the Contact, Location, and Serial Number of the SNMP Agent

This task explains how to set the system contact string, system location string, and system serial number of the SNMP agent.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

SUMMARY STEPS

1. **configure**
2. (Optional) **snmp-server contact** *system-contact-string*
3. (Optional) **snmp-server location** *system-location*
4. (Optional) **snmp-server chassis-id** *serial-number*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

Step 2	(Optional) **snmp-server contact** *system-contact-string*
	Example:
	`RP/0/RP0/CPU0:router(config)# snmp-server contact`
	`Dial System Operator at beeper # 27345`
		Sets the system contact string.

Step 3	(Optional) **snmp-server location** *system-location*
	Example:
	`RP/0/RP0/CPU0:router(config)# snmp-server location`
	`Building 3/Room 214`
		Sets the system location string.

Step 4	(Optional) **snmp-server chassis-id** *serial-number* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server chassis-id 1234456`	Sets the system serial number.
Step 5	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Defining the Maximum SNMP Agent Packet Size

This task shows how to configure the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

SUMMARY STEPS

1. **configure**
2. (Optional) **snmp-server packetsize** *byte-count*
3. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	(Optional) **snmp-server packetsize** *byte-count* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server packetsize 1024`	Sets the maximum packet size.
Step 3	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Changing Notification Operation Values

After SNMP notifications have been enabled, you can specify a value other than the default for the source interface, message queue length, or retransmission interval.

This task explains how to specify a source interface for trap notifications, the message queue length for each host, and the retransmission interval.

Note The sequence in which you issue the **snmp-server** commands for this task does not matter.

SUMMARY STEPS

1. **configure**
2. (Optional) **snmp-server trap-source** *type interface-path-id*
3. (Optional) **snmp-server queue-length** *length*
4. (Optional) **snmp-server trap-timeout** *seconds*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	(Optional) **snmp-server trap-source** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server trap-source POS 0/0/1/0`	Specifies a source interface for trap notifications.
Step 3	(Optional) **snmp-server queue-length** *length* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server queue-length 20`	Establishes the message queue length for each notification.
Step 4	(Optional) **snmp-server trap-timeout** *seconds* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server trap-timeout 20`	Defines how often to resend notifications on the retransmission queue.
Step 5	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session.

	Command or Action	Purpose
		• **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Setting IP Precedence and DSCP Values

This task describes how to configure IP Precedence or IP DSCP for SNMP traffic.

Before you begin

SNMP must be configured.

SUMMARY STEPS

1. **configure**
2. Use one of the following commands:
   - **snmp-server ipv4 precedence** *value*
   - **snmp-server ipv4 dscp** *value*
3. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	Use one of the following commands: • **snmp-server ipv4 precedence** *value* • **snmp-server ipv4 dscp** *value* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server dscp 24`	Configures an IP precedence or IP DSCP value for SNMP traffic.
Step 3	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session.

	Command or Action	Purpose
		• **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Setting an IP Precedence Value for SNMP Traffic: Example

The following example shows how to set the SNMP IP Precedence value to 7:

```
configure
  snmp-server ipv4 precedence 7
  exit

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y
```

Setting an IP DSCP Value for SNMP Traffic: Example

The following example shows how to set the IP DSCP value of SNMP traffic to 45:

```
configure
  snmp-server ipv4 dscp 45
  exit

  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: y
```

Displaying SNMP Context Mapping

The SNMP agent serves queries based on SNMP contexts created by the client features. There is a context mapping table. Each entry in the context mapping table includes a context name, the name of the feature that created the context, and the name of the specific instance of the feature.

SUMMARY STEPS

1. **show snmp context-mapping**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show snmp context-mapping** **Example:**	Displays the SNMP context mapping table.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router# show snmp context-mapping`	

Monitoring Packet Loss

It is possible to monitor packet loss by configuring the generation of SNMP traps when packet loss exceeds a specified threshold. The configuration described in this task enables the creation of entries in the MIB tables of the EVENT-MIB. This can then be monitored for packet loss using SNMP GET operations.

Before you begin

Note Entries created in the EVENT-MIB MIB tables using the configuration described in this task cannot be altered using an SNMP SET.

Entries to the EVENT-MIB MIB tables created using an SNMP SET cannot be altered using the configuration described in this task.

SUMMARY STEPS

1. **snmp-server mibs eventmib packet-loss** *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**snmp-server mibs eventmib packet-loss** *type interface-path-id* **falling** *lower-threshold* **interval** *sampling-interval* **rising** *upper-threshold* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server mibs eventmib packet-loss falling 1 interval 5 rising 2`	Generates SNMP EVENT-MIB traps for the interface when the packet loss exceeds the specified thresholds. Up to 100 interfaces can be monitored. **falling** *lower-threshold* —Specifies the lower threshold. When packet loss between two intervals falls below this threshold and an mteTriggerRising trap was generated previously, a SNMP mteTriggerFalling trap is generated. This trap is not generated until the packet loss exceeds the upper threshold and then falls back below the lower threshold. **interval** *sampling-interval* —Specifies how often packet loss statistics are polled. This is a value between 5 and 1440 minutes, in multiples of 5. **rising** *upper-threshold* —Specifies the upper threshold. When packet loss between two intervals increases above this threshold, an SNMP mteTriggreRising trap is generated.

	Command or Action	Purpose
		This trap is not generated until the packet loss drops below the lower threshold and then rises above the upper threshold.

Configuring MIB Data to be Persistent

Many SNMP MIB definitions define arbitrary 32-bit indices for their object tables. MIB implementations often do a mapping from the MIB indices to some internal data structure that is keyed by some other set of data. In these MIB tables the data contained in the table are often other identifiers of the element being modelled. For example, in the ENTITY-MIB, entries in the entPhysicalTable are indexed by the 31-bit value, entPhysicalIndex, but the entities could also be identified by the entPhysicalName or a combination of the other objects in the table.

Because of the size of some MIB tables, significant processing is required to discover all the mappings from the 32-bit MIB indices to the other data which the network management station identifies the entry. For this reason, it may be necessary for some MIB indices to be persistent across process restarts, switchovers, or device reloads. The ENTITY-MIB entPhysicalTable and CISCO-CLASS-BASED-QOS-MIB are two such MIBs that often require index values to be persistent.

Also, because of query response times and CPU utilization during CISCO-CLASS-BASED-QOS-MIB statistics queries, it is desirable to cache service policy statistics.

SUMMARY STEPS

1. (Optional) **snmp-server entityindex persist**
2. (Optional) **snmp-server mibs cbqosmib persist**
3. (Optional) **snmp-server cbqosmib cache refresh time** *time*
4. (Optional) **snmp-server cbqosmib cache service-policy count** *count*
5. **snmp-server ifindex persist**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	(Optional) **snmp-server entityindex persist** **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server entityindex persist`	Enables the persistent storage of ENTITY-MIB data.
Step 2	(Optional) **snmp-server mibs cbqosmib persist** **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib persist`	Enables persistent storage of the CISCO-CLASS-BASED-QOS-MIB data.

	Command or Action	Purpose
Step 3	(Optional) **snmp-server cbqosmib cache refresh time** *time* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib cache refresh time 45`	Enables QoS MIB caching with a specified cache refresh time.
Step 4	(Optional) **snmp-server cbqosmib cache service-policy count** *count* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib cache service-policy count 50`	Enables QoS MIB caching with a limited number of service policies to cache.
Step 5	**snmp-server ifindex persist** **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server ifindex persist`	Enables ifIndex persistence globally on all Simple Network Management Protocol (SNMP) interfaces.

Configuring LinkUp and LinkDown Traps for a Subset of Interfaces

By specifying a regular expression to represent the interfaces for which you are interested in setting traps, you can enable or disable linkUp and linkDown traps for a large number of interfaces simultaneously.

Before you begin

SNMP must be configured.

SUMMARY STEPS

1. **configure**
2. **snmp-server interface subset** *subset-number* **regular-expression** *expression*
3. **notification linkupdown disable**
4. Use the **commit** or **end** command.
5. (Optional) **show snmp interface notification subset** *subset-number*
6. (Optional) **show snmp interface notification regular-expression** *expression*
7. (Optional) **show snmp interface notification** *type interface-path-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

Step 2	**snmp-server interface subset** *subset-number* **regular-expression** *expression*
	Example:
	`RP/0/RP0/CPU0:router(config)# snmp-server interface subset 10 regular-expression "^Gig[a-zA-Z]+[0-9/]+\."`
	`RP/0/RP0/CPU0:router(config-snmp-if-subset)#`
		Enters snmp-server interface mode for the interfaces identified by the regular expression.
		The subset-number argument identifies the set of interfaces, and also assigns a priority to the subset in the event that an interface is included in more than one subset. Lower numbers have higher priority and their configuration takes precedent over interface subsets with higher numbers.
		The *expression* argument must be entered surrounded by double quotes.
		Refer to the *Understanding Regular Expressions, Special Characters, and Patterns* module in for more information regarding regular expressions.

Step 3	**notification linkupdown disable** **Example:** `RP/0/RP0/CPU0:router(config-snmp-if-subset)# notification linkupdown disable`	Disables linkUp and linkDown traps for all interfaces being configured. To enable previously disabled interfaces, use the **no** form of this command.
Step 4	Use the **commit** or **end** command.	**commit** —Saves the configuration changes, and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration mode, without committing the configuration changes.
Step 5	(Optional) **show snmp interface notification subset** *subset-number* **Example:** `RP/0/RP0/CPU0:router# show snmp interface notification subset 10`	Displays the linkUp and linkDown notification status for all interfaces identified by the subset priority.

	Command or Action	Purpose
Step 6	(Optional) **show snmp interface notification regular-expression** *expression* **Example:** `RP/0/RP0/CPU0:router# show snmp interface notification regular-expression "^Gig[a-zA-Z]+[0-9/]+\."`	Displays the linkUp and linkDown notification status for all interfaces identified by the regular expression.
Step 7	(Optional) **show snmp interface notification** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router# show snmp interface notification tengige 0/4/0/3.10`	Displays the linkUp and linkDown notification status for the specified interface.

SNMP Context Mapping Configuration

SNMP behavior with BGP at scale

In large-scale BGP deployments, polling the entire BGP routing table via SNMP, particularly when querying the cbgpRoute table, can significantly increase CPU utilization. This elevated load may cause temporary performance impacts, such as:

- Slower response times for SNMP queries
- Transient mutex contention issues within the system
- Elevated CPU usage during the polling process
- Potential SNMP timeouts when retrieving large BGP route datasets

During SNMP polling operations, users might notice slower execution of BGP show commands. These behaviors are expected in high-scale environments due to the resource-intensive nature of polling large BGP tables with SNMP.

Configuration of VRF Aware SNMP Context for Polling BGP Data

VRF awareness is usually done using existing, non-VRF aware MIB definitions. This means that MIB definition doesn't mention anything about VRFs. However they could be used within VRF context.

The VRF-awareness is done using SNMP contexts, where a SNMP context maps to a specific VRF.

Before you begin

- Ensure that MIB implementation is VRF-aware.
- Ensure that the implementation of all get requests support VRF context.

The following example configures VRF aware SNMP context to allow polling BGP data using BGP4-MIB.

```
snmp-server vrf <vrf_1> context <context_1>
snmp-server community <vrf_1> RW
```

```
snmp-server context <context_1>
snmp-server community-map <vrf_1> context <context_1>
snmp-server host <IP> traps version 2c <vrf_1>
```

Verification

The following configuration extracts BGP data from a peer VRF using context.

```
snmp-server vrf V1
 context V1_bgp
!
snmp-server community V1 RW
snmp-server context V1_bgp
snmp-server community-map V1 context V1_bgp
router bgp 65000
 nsr
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 192.0.2.254
  remote-as 65001
  address-family ipv4 unicast
   route-policy ALL in
   route-policy ALL out
  !
 !
 vrf V1
  rd 111:111
  address-family ipv4 unicast
  !
  neighbor 192.0.2.255
   remote-as 65003
   address-family ipv4 unicast
   !
  !
 !
!
end
```

Configuration of OSPF processes Using SNMP Context

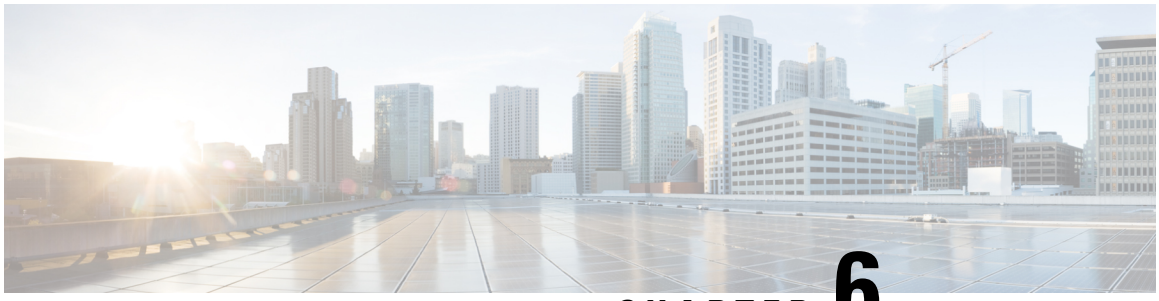
The following example configures data polling from two OSPF processes.

```
snmp-server community com1 RW
snmp-server community com2 RW
snmp-server context ctx1
snmp-server context ctx2
snmp-server community-map com1 context ctx1
snmp-server community-map com2 context ctx2
router ospf one
 snmp context ctx1
 area 0
  interface GigabitEthernet0/2/0/0
  !
 !
!
router ospf two
 snmp context ctx2
 area 0
  interface GigabitEthernet0/2/0/1
  !
 !
!
```

Configuration of OSPF Neighbour in VRF

The following example configures OSFP neighbours in VRF using SNMP context.

```
snmp-server vrf VRF_A
 context ctx1
!
snmp-server community com1 RW
snmp-server context ctx1
snmp-server community-map com1 context ctx1
router ospf core
 vrf VRF_A
  snmp context ctx1
 !
!
end
```



CHAPTER 6

Configuring Object Tracking

This module describes the configuration of object tracking on your Cisco IOS XR network. For complete descriptions of the commands listed in this module, see **Additional References** section. To locate documentation for other commands that might appear in the course of performing a configuration task, see **Technical Documentation** section in the Additional References topic.

- Configuring Object Tracking, on page 51
- Prerequisites for Implementing Object Tracking, on page 51
- Information about Object Tracking, on page 52
- How to Implement Object Tracking, on page 52
- Configuration Examples for Configuring Object Tracking, on page 63
- Additional References, on page 65

Configuring Object Tracking

This module describes the configuration of object tracking on your Cisco IOS XR network. For complete descriptions of the commands listed in this module, see **Additional References** section. To locate documentation for other commands that might appear in the course of performing a configuration task, see **Technical Documentation** section in the Additional References topic.

Prerequisites for Implementing Object Tracking

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note Object Tracking is an optional package. You must check if this package is installed on your system by running the command **show install active summary**.

Information about Object Tracking

Object tracking is a mechanism to track an object and to take an action on another object with no relationship to the tracked objects, based on changes to the properties of the object being tracked.

Each tracked object is identified by a unique name specified on the tracking command-line interface (CLI). Cisco IOS XR processes then use this name to track a specific object.

The tracking process periodically polls the tracked object and reports any changes to its state in terms of its being up or down, either immediately or after a delay, as configured by the user.

Multiple objects can also be tracked by means of a list, using a flexible method for combining objects with Boolean logic. This functionality includes:

- **Boolean AND function—**When a tracked list has been assigned a Boolean AND function, each object defined within a subset must be in an up state, so that the tracked object can also be in the up state.
- **Boolean OR function—**When the tracked list has been assigned a Boolean OR function, it means that at least one object defined within a subset must also be in an up state, so that the tracked object can also be in the up state.

How to Implement Object Tracking

This section describes the various object tracking procedures.

Tracking the Line Protocol State of an Interface

Perform this task in global configuration mode to track the line protocol state of an interface.

A tracked object is considered up when a line protocol of the interface is up.

After configuring the tracked object, you may associate the interface whose state should be tracked and specify the number of seconds to wait before the tracking object polls the interface for its state.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type line-protocol state**
4. **interface** *type interface-path-id*
5. **exit**
6. (Optional) **delay** {**up** *seconds* | **down** *seconds*}
7. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RP0/CPU0:router(config)# track track1`	Enters track configuration mode. • *track-name*—Specifies a name for the object to be tracked. **Note** Special characters are not allowed in a *track-name*.
Step 3	**type line-protocol state** **Example:** `RP/0/RP0/CPU0:router(config-track)# type line-protocol state`	Creates a track based on the line protocol of an interface.
Step 4	**interface** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config-track-line-prot)# interface atm 0/2/0/0.1`	Specifies the interface to track the protocol state. • *type*—Specifies the interface type. For more information, use the question mark (?) online help function. • *interface-path-id*—Identifies a physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. **Note** The loopback and null interfaces are always in the up state and, therefore, cannot be tracked.
Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(config-track-line-prot)# exit`	Exits the track line protocol configuration mode.
Step 6	(Optional) **delay** {**up** *seconds* | **down** *seconds*} **Example:** `RP/0/RP0/CPU0:router(config-track)# delay up 10`	Schedules the delay that can occur between tracking whether the object is up or down.

	Command or Action	Purpose

Step 7	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-track)# end`
	or
	`RP/0/RP0/CPU0:router(config-track)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Tracking IP Route Reachability

When a host or a network goes down on a remote site, routing protocols notify the router and the routing table is updated accordingly. The routing process is configured to notify the tracking process when the route state changes due to a routing update.

A tracked object is considered up when a routing table entry exists for the route and the route is accessible.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type route reachability**
4. Use one of the following commands:
   - **vrf** *vrf-table-name*
   - **route ipv4** *IP-prefix/mask*
5. **exit**
6. (Optional) **delay** {**up** *seconds* | **down** *seconds*}
7. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RP0/CPU0:router(config)# track track1`	Enters track configuration mode. • *track-name*—Specifies a name for the object to be tracked. **Note** Special characters are not allowed in a *track-name*.
Step 3	**type route reachability** **Example:** `RP/0/RP0/CPU0:router(config-track)# type route reachability vrf internet`	Configures the routing process to notify the tracking process when the state of the route changes due to a routing update.

Step 4	Use one of the following commands:
	• **vrf** *vrf-table-name*
	• **route ipv4** *IP-prefix/mask*
	Example:
	`RP/0/RP0/CPU0:router(config-track-route)# vrf vrf-table-4`
	or
	`RP/0/RP0/CPU0:router(config-track-route)# route ipv4 10.56.8.10/16`
		Configures the type of IP route to be tracked, which can consist of either of the following, depending on your router type:
		• *vrf-table-name*—A VRF table name.
		• *IP-prefix/mask*—An IP prefix consisting of the network and subnet mask (for example, 10.56.8.10/16).

Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(config-track-line-prot)# exit`	Exits the track line protocol configuration mode.
Step 6	(Optional) **delay** {**up** *seconds* | **down** *seconds*} **Example:** `RP/0/RP0/CPU0:router(config-track)# delay up 10`	Schedules the delay that can occur between tracking whether the object is up or down.
Step 7	Use the **commit** or **end** command.	**commit** —Saves the configuration changes, and remains within the configuration session. **end** —Prompts user to take one of these actions:

	Command or Action	Purpose
		• **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration mode, without committing the configuration changes.

Building a Track Based on a List of Objects

Perform this task in the global configuration mode to create a tracked list of objects (which, in this case, are lists of interfaces or prefixes) using a Boolean expression to determine the state of the list.

A tracked list contains one or more objects. The Boolean expression enables two types of calculations by using either AND or OR operators. For example, when tracking two interfaces, using the AND operator, up means that *both* interfaces are up, and down means that *either* interface is down.

Note An object must exist before it can be added to a tracked list.

The NOT operator is specified for one or more objects and negates the state of the object.

After configuring the tracked object, you must associate the interface whose state should be tracked and you may optionally specify the number of seconds to wait before the tracking object polls the interface for its state.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type list boolean** { **and** | **or** }
4. **object** *object-name* [**not**]
5. **exit**
6. (Optional) **delay** {**up** *seconds* | **down** *seconds*}
7. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RP0/CPU0:router(config)# track track1`	Enters track configuration mode. • *track-name*—Specifies a name for the object to be tracked. **Note** Special characters are not allowed in a *track-name*.
Step 3	**type list boolean** { **and** | **or** } **Example:** `RP/0/RP0/CPU0:router(config-track)# type list boolean and`	Configures a Boolean list object and enters track list configuration mode. • **boolean**—Specifies that the state of the tracked list is based on a Boolean calculation. • **and**—Specifies that the list is up if all objects are up, or down if one or more objects are down. For example when tracking two interfaces, up means that both interfaces are up, and down means that either interface is down. • **or**—Specifies that the list is up if at least one object is up. For example, when tracking two interfaces, up means that either interface is up, and down means that both interfaces are down.
Step 4	**object** *object-name* [**not**] **Example:** `RP/0/RP0/CPU0:router(config-track-list)# object 3 not`	Specifies the object to be tracked by the list • *obect-name*—Name of the object to track. • **not**—Negates the state of the object.
Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(config-track-line-prot)# exit`	Exits the track line protocol configuration mode.
Step 6	(Optional) **delay** {**up** *seconds* | **down** *seconds*} **Example:** `RP/0/RP0/CPU0:router(config-track)# delay up 10`	Schedules the delay that can occur between tracking whether the object is up or down.

	Command or Action	Purpose

Step 7	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-track)# end`
	or
	`RP/0/RP0/CPU0:router(config-track)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Building a Track Based on a List of Objects - Threshold Percentage

Perform this task in the global configuration mode to create a tracked list of objects (which, in this case, are lists of interfaces or prefixes) using a threshold percentage to determine the state of the list.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type list threshold percentage**
4. **object** *object-name*
5. **threshold percentage up** *percentage* **down** *percentage*
6. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RP0/CPU0:router(config)# track track1`	Enters track configuration mode. • *track-name*—Specifies a name for the object to be tracked. **Note** Special characters are not allowed in a *track-name*.
Step 3	**type list threshold percentage** **Example:** `RP/0/RP0/CPU0:router(config-track)# type list threshold percentage`	Configures a track of type threshold percentage list.

Step 4	**object** *object-name*
	Example:
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 1`
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 2`
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 3`
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 4`
		Configures object 1, object 2, object 3 and object 4 as members of track type track1.

Step 5	**threshold percentage up** *percentage* **down** *percentage* **Example:** `RP/0/RP0/CPU0:router(config-track-list-threshold)# threshold percentage up 50 down 33`	Configures the percentage of objects that need to be UP or DOWN for the list to be considered UP or Down respectively. For example, if object 1, object 2, and object 3 are in the UP state and object 4 is in the DOWN state, the list is considered to be in the UP state.
Step 6	Use one of the following commands: • **end** • **commit** **Example:** `RP/0/RP0/CPU0:router(config-track)# end`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`

	Command or Action	Purpose
	or `RP/0/RP0/CPU0:router(config-track)# commit`	• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. • Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Building a Track Based on a List of Objects - Threshold Weight

Perform this task in the global configuration mode to create a tracked list of objects (which, in this case, are lists of interfaces or prefixes) using a threshold weight to determine the state of the list.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type list threshold weight**
4. **object** *object-name* **weight** *weight*
5. **threshold weight up** *weight* **down** *weight*
6. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:**	Enters track configuration mode. • *track-name*—Specifies a name for the object to be tracked.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(config)# track track1`	**Note** Special characters are not allowed in a *track-name*.
Step 3	**type list threshold weight** **Example:** `RP/0/RP0/CPU0:router(config-track)# type list threshold weight`	Configures a a track of type, threshold weighted list.

Step 4	**object** *object-name* **weight** *weight*
	Example:
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 1 weight 10`
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 2 weight 5`
	`RP/0/RP0/CPU0:router(config-track-list-threshold)# object 3 weight 3`
		Configures object 1, object 2 and object 3 as members of track t1 and with weights 10, 5 and 3 respectively.

Step 5	**threshold weight up** *weight* **down** *weight* **Example:** `RP/0/RP0/CPU0:router(config-track-list-threshold)# threshold weight up 10 down 5`	Configures the range of weights for the objects that need to be UP or DOWN for the list to be considered UP or DOWN respectively. In this example, the list is considered to be in the DOWN state because objects 1 and 2 are in the UP state and the cumulative weight is 15 (not in the 10-5 range).

Step 6	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-track)# end`
	or
	`RP/0/RP0/CPU0:router(config-track)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Tracking IPSLA Reachability

Use this task to enable the tracking of the return code of IP service level agreement (SLA) operations.

SUMMARY STEPS

1. **configure**
2. **track** *track-name*
3. **type rtr** *ipsla-no* **reachability**
4. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**track** *track-name* **Example:** `RP/0/RP0/CPU0:router(config)# track t1`	Enters track configuration mode. **Note** Special characters are not allowed in a *track-name*.
Step 3	**type rtr** *ipsla-no* **reachability** **Example:** `RP/0/RP0/CPU0:router(config-track)# type rtr 100 reachability`	Specifies the IP SLA operation ID to be tracked for reachability. Values for the *ipsla-no* can range from1 to 2048.
Step 4	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Configuring IPSLA Tracking: Example

This example shows the configuration of IPSLA tracking:

```
RP/0/RP0/CPU0:router(config)# track track1
```

```
RP/0/RP0/CPU0:router(config-track)# type rtr 1 reachability
RP/0/RP0/CPU0:router(config-track)# delay up 5
RP/0/RP0/CPU0:router(config-track)# delay down 10
```

Configuration Examples for Configuring Object Tracking

Tracking Whether the Interface Is Up or Down: Running Configuration Example

```
track connection100
  type list boolean and
    object object3 not
    delay up 10
    !
interface service-ipsec 23
  line-protocol track connection100
  !
```

Tracking the Line Protocol State of an Interface: Running Configuration Example

In this example, traffic arrives from interface service-ipsec1 and exits through interface gigabitethernet0/0/0/3:

```
track IPSec1
  type line-protocol state
    interface gigabitethernet0/0/0/3
    !
interface service-ipsec 1
  ipv4 address 70.0.0.1 255.255.255.0
  profile vrf1_profile_ipsec
  line-protocol track IPSec1
  tunnel source 80.0.0.1
  tunnel destination 80.0.0.2
  service-location preferred-active 0/0/1
  !
```

This example displays the output from the **show track** command after performing the previous example:

```
RP/0/RP0/CPU0:router# show run track

  Track IPSec1
  Interface GigabitEthernet0_0_0_3 line-protocol
  !
    Line protocol is UP
    1 change, last change 10:37:32 UTC Thu Sep 20 2007
    Tracked by:
    service-ipsec1
    !
```

Tracking IP Route Reachability: Running Configuration Example

In this example, traffic arriving from interface service-ipsec1 has its destination in network 7.0.0.0/24. This tracking procedure follows the state of the routing protocol prefix to signal when there are changes in the routing table.

```
track PREFIX1
  type route reachability
    route ipv4 7.0.0.0/24
    !
  interface service-ipsec 1
  vrf 1
  ipv4 address 70.0.0.2 255.255.255.0
  profile vrf_1_ipsec
  line-protocol track PREFIX1
  tunnel source 80.0.0.2
  tunnel destination 80.0.0.1
  service-location preferred-active 0/2/0
```

Building a Track Based on a List of Objects: Running Configuration Example

In this example, traffic arriving from interface service-ipsec1 exits through interface gigabitethernet0/0/0/3 and interface ATM 0/2/0/0.1. The destination of the traffic is at network 7.0.0.0/24.

If either one of the interfaces or the remote network goes down, the flow of traffic must stop. To do this, we use a Boolean AND expression.

```
track C1
 type route reachability
  route ipv4 3.3.3.3/32
 !
!
track C2
 type route reachability
  route ipv4 1.2.3.4/32
 !
!
track C3
 type route reachability
  route ipv4 10.0.20.2/32
 !
!
track C4
 type route reachability
  route ipv4 10.0.20.0/24
 !
!
track OBJ
 type list boolean and
  object C1
  object C2
 !
!
track OBJ2
 type list boolean or
  object C1
```

```
 object C2
!
```

Additional References

The following sections provide references related to implementing object tracking for IPSec network security.

Related Documents

Related Topic	Document Title
IP SLA configuration information	*Implementing IP Service Level Agreements on* module in *System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers*
IP SLA commands	*IP Service Level Agreement Commands on* module in *System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers*
Object tracking commands	*Object Tracking Commands on* module in

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

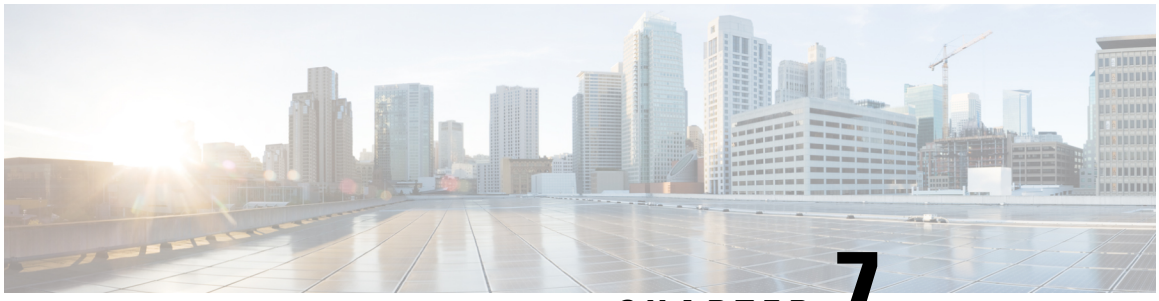
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://cfnng-stg.cisco.com/mibs.

RFCs

RFCs	Title
RFC 2401	*Security Architecture for the Internet Protocol*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 7

Configuring Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a media- and protocol-independent protocol that runs on all Cisco-manufactured equipment including routers, bridges, access and communication servers, and switches. Using CDP, you can view information about all the Cisco devices that are directly attached to the device.

- Prerequisites for Implementing CDP, on page 67
- Information About Implementing CDP, on page 67
- How to Implement CDP on Cisco IOS XR Software, on page 69
- Configuration Examples for Implementing CDP, on page 75

Prerequisites for Implementing CDP

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note CDP is an optional package. You must check if this package is installed on your system by running the command **show install active summary**.

Information About Implementing CDP

CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to display information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all equipment manufactured by Cisco, including routers, bridges, access servers, and switches.

Use of SNMP with the CDP MIB allows network management applications to learn the device type and the SNMP agent address of neighboring devices and to send SNMP queries to those devices. CDP uses the CISCO-CDP-MIB.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including LAN, Frame Relay, and ATM physical media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages, known as *advertisements*, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or hold-time, information, which indicates the length of time a receiving device holds CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others to learn about neighboring devices and determine when their interfaces to the media go up or down.

CDP Version-2 (CDPv2) is the most recent release of the protocol and provides more intelligent device tracking features. These features include a reporting mechanism that allows for more rapid error tracking, thereby reducing costly downtime. Reported error messages can be sent to the console or to a logging server, and can cover instances of unmatching native VLAN IDs (IEEE 802.1Q) on connecting ports, and unmatching port duplex states between connecting devices.

CDPv2 **show** commands can provide detailed output on VLAN Trunking Protocol (VTP) management domain and duplex modes of neighbor devices, CDP-related counters, and VLAN IDs of connecting ports.

Type-length-value fields (TLVs) are blocks of information embedded in CDP advertisements. This table summarizes the TLV definitions for CDP advertisements.

Table 5: Type-Length-Value Definitions for CDPv2

TLV	Definition
Device-ID TLV	Identifies the device name in the form of a character string.
Address TLV	Contains a list of network addresses of both receiving and sending devices.
Port-ID TLV	Identifies the port on which the CDP packet is sent.
Capabilities TLV	Describes the functional capability for the device in the form of a device type; for example, a switch.
Version TLV	Contains information about the software release version on which the device is running.
Platform TLV	Describes the hardware platform name of the device, for example, Cisco 4500.
VTP Management Domain TLV	Advertises the system's configured VTP management domain name-string. Used by network operators to verify VTP domain configuration in adjacent network nodes.
Native VLAN TLV	Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This feature is implemented only for interfaces that support the IEEE 802.1Q protocol.
Full/Half Duplex TLV	Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.

How to Implement CDP on Cisco IOS XR Software

Enabling CDP

To enable CDP, you must first enable CDP globally on the router and then enable CDP on a per-interface basis. This task explains how to enable CDP globally on the router and then enable CDP on an interface.

SUMMARY STEPS

1. **configure**
2. **cdp**
3. **interface** *type interface-path-id*
4. **cdp**
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**cdp** **Example:** `RP/0/RP0/CPU0:router(config)# cdp`	Enables CDP globally.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config)# int TenGigE 0/5/0/11/1`	Enters interface configuration mode.
Step 4	**cdp** **Example:** `RP/0/RP0/CPU0:router(config-if)# cdp`	Enables CDP on an interface.
Step 5	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions:

	Command or Action	Purpose
		• **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Modifying CDP Default Settings

This task explains how to modify the default version, hold-time setting, and timer settings.

Note The commands can be entered in any order.

SUMMARY STEPS

1. **configure**
2. **cdp advertise v1**
3. **cdp holdtime** *seconds*
4. **cdp timer** *seconds*
5. Use the **commit** or **end** command.
6. (Optional) **show cdp**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**cdp advertise v1** **Example:** `RP/0/RP0/CPU0:router(config)# cdp advertise v1`	Configures CDP to use only version 1 (CDPv1) in communicating with neighboring devices. • By default, when CDP is enabled, the router sends CDPv2 packets. CDP also sends and receives CDPv1 packets if the device with which CDP is interacting does not process CDPv2 packets. • In this example, the router is configured to send and receive only CDPv1 packets.

	Command or Action	Purpose
Step 3	**cdp holdtime** *seconds* **Example:** `RP/0/RP0/CPU0:router(config)# cdp holdtime 30`	Specifies the amount of time that the receiving networking device will hold a CDP packet sent from the router before discarding it. • By default, when CDP is enabled, the receiving networking device holds a CDP packet for 180 seconds before discarding it. **Note** The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set with the **cdp timer** command. • In this example, the value of hold-time for the *seconds* argument is set to 30.
Step 4	**cdp timer** *seconds* **Example:** `RP/0/RP0/CPU0:router(config)# cdp timer 20`	Specifies the frequency at which CDP update packets are sent. • By default, when CDP is enabled, CDP update packets are sent at a frequency of once every 60 seconds. **Note** A lower timer setting causes CDP updates to be sent more frequently. • In this example, CDP update packets are configured to be sent at a frequency of once every 20 seconds.
Step 5	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.
Step 6	(Optional) **show cdp** **Example:** `RP/0/RP0/CPU0:router# show cdp`	Displays global CDP information. The output displays the CDP version running on the router, the hold time setting, and the timer setting.

Monitoring CDP

This task shows how to monitor CDP.

Note The commands can be entered in any order.

SUMMARY STEPS

1. **show cdp entry** {***** | *entry-name*} [**protocol** | **version**]
2. **show cdp interface** [*type interface-path-id* | **location** *node-id*]
3. **show cdp neighbors** [*type interface-path-id* | **location** *node-id*] [**detail**]
4. **show cdp traffic** [**location** *node-id*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show cdp entry** {***** | *entry-name*} [**protocol** | **version**] **Example:** `RP/0/RSP0/CPU0:router# show cdp entry *`	Displays information about a specific neighboring device or all neighboring devices discovered using CDP.
Step 2	**show cdp interface** [*type interface-path-id* | **location** *node-id*] **Example:** `RP/0/RSP0/CPU0:router# show cdp interface pos 0/0/0/1`	Displays information about the interfaces on which CDP is enabled.
Step 3	**show cdp neighbors** [*type interface-path-id* | **location** *node-id*] [**detail**] **Example:** `RP/0/RSP0/CPU0:router# show cdp neighbors`	Displays detailed information about neighboring devices discovered using CDP.
Step 4	**show cdp traffic** [**location** *node-id*] **Example:** `RP/0/RSP0/CPU0:router# show cdp traffic`	Displays information about the traffic gathered between devices using CDP.

Examples

The following is sample output for the **show cdp neighbors** command:

```
RP/0/RP0/CPU0:router# show cdp neighbors

  Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device ID        Local Intrfce   Holdtme  Capability  Platform  Port ID
asr9k-rtr1       Te0/5/0/11/1    152      R           ASR9K Ser Te0/1/0/9
asr9k-rtr1       Te0/5/0/11/2    156      R           ASR9K Ser Te0/1/0/10
asr9k-rtr1       Te0/5/0/11/3    160      R           ASR9K Ser Te0/1/0/11
```

The following is sample output for the **show cdp neighbors** command. In this example, the optional *type instance* arguments are used in conjunction with the **detail** optional keyword to display detailed information about a CDP neighbor. The output includes information on both IPv4 and IPv6 addresses.

```
RP/0/RP0/CPU0:router#  show cdp neighbors TenGigE 0/5/0/11/1 detail

  -------------------------
  Device ID: asr9k-rtr1
  SysName : asr9k-rtr1
  Entry address(es):
  IPv4 address: 90.0.0.2
  Platform: cisco ASR9K Series, Capabilities: Router
  Interface: TenGigE 0/5/0/11/1
  Port ID (outgoing port): TenGigE 0/1/0/9
  Holdtime : 155 sec

  Version :
  Cisco IOS XR Software, Version 5.3.1.10I[Default]
  Copyright (c) 2015 by Cisco Systems, Inc.

  advertisement version: 2
  Duplex: full
```

The following is sample output for the **show cdp entry** command. In this example, the optional *entry* argument is used to display entry information related to a specific CDP neighbor.

```
RP/0/RP0/CPU0:router# show cdp entry asr9k-rtr1

-------------------------
Device ID: asr9k-rtr1
SysName : asr9k-rtr1
Entry address(es):
IPv4 address: 110.0.0.2
Platform: cisco ASR9K Series, Capabilities: Router
Interface: TenGigE 0/5/0/11/3
Port ID (outgoing port): TenGigE 0/1/0/11
Holdtime : 173 sec

Version :
Cisco IOS XR Software, Version 5.3.1.10I[Default]
Copyright (c) 2015 by Cisco Systems, Inc.

advertisement version: 2
Duplex: full

-------------------------
Device ID: asr9k-rtr1
SysName : asr9k-rtr1
Entry address(es):
IPv4 address: 100.0.0.2
Platform: cisco ASR9K Series, Capabilities: Router
Interface: TenGigE 0/5/0/11/2
Port ID (outgoing port): TenGigE 0/1/0/10
Holdtime : 169 sec
```

```
Version :
Cisco IOS XR Software, Version 5.3.1.10I[Default]
Copyright (c) 2015 by Cisco Systems, Inc.

advertisement version: 2
Duplex: full

-------------------------
Device ID: asr9k-rtr1
SysName : asr9k-rtr1
Entry address(es):
IPv4 address: 90.0.0.2
Platform: cisco ASR9K Series, Capabilities: Router
Interface: TenGigE 0/5/0/11/1
Port ID (outgoing port): TenGigE 0/1/0/10
Holdtime : 165 sec

Version :
Cisco IOS XR Software, Version 5.3.1.10I[Default]
Copyright (c) 2015 by Cisco Systems, Inc.

advertisement version: 2
Duplex: full
```

The following is sample output for the **show cdp interface** command. In this example, CDP information related to Packet over SONET/SDH (POS) interface 0/4/0/0 is displayed.

```
RP/0/RP0/CPU0:router#  show cdp interface TenGigE 0/5/0/11/1

  TenGigE 0/5/0/11/1 is Up
    Encapsulation ether
    Sending CDP packets every 20 seconds
    Holdtime is 30 seconds
```

The following is sample output for the **show cdp traffic** command:

```
RP/0/RP0/CPU0:router# show cdp traffic

  CDP counters :
          Packets output: 250, Input: 120
          Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
          No memory: 0, Invalid packet: 0, Truncated: 0
          CDP version 1 advertisements output: 0, Input: 0
          CDP version 2 advertisements output: 250, Input: 120
          Unrecognize Hdr version: 0, File open failed: 0
```

The following is sample output for the **show cdp traffic** command. In this example, the optional **location** keyword and *node-id* argument are used to display information about the traffic gathered between devices using CDP from the specified node.

```
RP/0/RP0/CPU0:router# show cdp traffic 0/5/CPU0

  CDP counters :
          Packets output: 318, Input: 141
          Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
          No memory: 0, Invalid packet: 0, Truncated: 0
          CDP version 1 advertisements output: 0, Input: 0
          CDP version 2 advertisements output: 318, Input: 141
```

```
Unrecognize Hdr version: 0, File open failed: 0
```

Configuration Examples for Implementing CDP

Enabling CDP: Example

The following example shows how to configure CDP globally and then enable CDP on Ethernet interface TenGigE 0/5/0/11/1:

```
cdp
interface 0/5/0/11/1
cdp
```

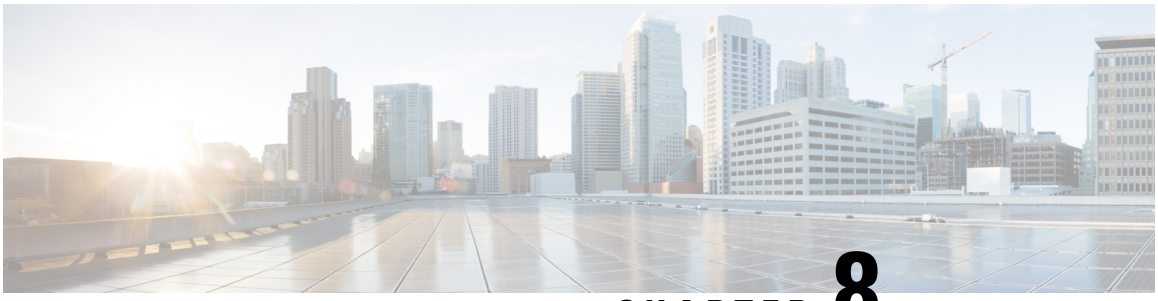
Modifying Global CDP Settings: Example

The following example shows how to modify global CDP settings. In this example, the timer setting is set to 20 seconds, the hold-time setting is set to 30 seconds, and the version of CDP used to communicate with neighboring devices is set to CDPv1:

```
cdp timer 20
cdp holdtime 30
cdp advertise v1
```

The following example shows how to use the **show cdp** command to verify the CDP global settings:

```
RP/0/RP0/CPU0:router# show cdp

  Global CDP information:
  Sending CDP packets every 20 seconds
  Sending a holdtime value of 30 seconds
  Sending CDPv2 advertisements is not enabled
```



CHAPTER 8

Configuring Periodic MIB Data Collection and Transfer

This document describes how to periodically transfer selected MIB data from your router to a specified Network Management System (NMS). The periodic MIB data collection and transfer feature is also known as bulk statistics.

- Prerequisites for Periodic MIB Data Collection and Transfer, on page 77
- Information About Periodic MIB Data Collection and Transfer, on page 77
- How to Configure Periodic MIB Data Collection and Transfer, on page 79
- Periodic MIB Data Collection and Transfer: Example, on page 85

Prerequisites for Periodic MIB Data Collection and Transfer

To use periodic MIB data collection and transfer, you should be familiar with the Simple Network Management Protocol (SNMP) model of management information. You should also know what MIB information you want to monitor on your network devices, and the OIDs or object names for the MIB objects to be monitored.

Information About Periodic MIB Data Collection and Transfer

SNMP Objects and Instances

A type (or class) of SNMP management information is called an object. A specific instance from a type of management information is called an object instance (or SNMP variable). To configure a bulk statistics collection, you must specify the object types to be monitored using a bulk statistics object list and the specific instances of those objects to be collected using a bulk statistics schema.

MIBs, MIB tables, MIB objects, and object indices can all be specified using a series of numbers called an object identifier (OID). OIDs are used in configuring a bulk statistics collection in both the bulk statistics object lists (for general objects) and in the bulk statistics schemas (for specific object instances).

Bulk Statistics Object Lists

To group the MIB objects to be polled, you need to create one or more object lists. A bulk statistics object list is a user-specified set of MIB objects that share the same MIB index. Object lists are identified using a name that you specify. Named bulk statistics object lists allow the same configuration to be reused in different bulk statistics schemas.

All the objects in an object list must share the same MIB index. However, the objects do not need to be in the same MIB and do not need to belong to the same MIB table. For example, it is possible to group ifInOctets and a CISCO-IF-EXTENSION-MIB object in the same schema, because the containing tables for both objects are indexed by the ifIndex.

Bulk Statistics Schemas

Data selection for the Periodic MIB Data Collection and Transfer Mechanism requires the definition of a schema with the following information:

- Name of an object list.
- Instance (specific instance or series of instances defined using a wild card) that needs to be retrieved for objects in the specified object list.
- How often the specified instances need to be sampled (polling interval). The default polling interval is 5 minutes.

A bulk statistics schema is also identified using a name that you specify. This name is used when configuring the transfer options.

Bulk Statistics Transfer Options

After configuring the data to be collected, a single virtual file (VFile or *bulk statistics file*) with all collected data is created. This file can be transferred to a network management station using FTP or TFTP. You can specify how often this file should be transferred. The default transfer interval is once every 30 minutes. You can also configure a secondary destination for the file to be used if, for whatever reason, the file cannot be transferred to the primary network management station.

The value of the transfer interval is also the collection period (collection interval) for the local bulk statistics file. After the collection period ends, the bulk statistics file is frozen, and a new local bulk statistics file is created for storing data. The frozen bulk statistics file is then transferred to the specified destination.

By default, the local bulk statistics file is deleted after successful transfer to an network management station.

Benefits of Periodic MIB Data Collection and Transfer

Periodic MIB data collection and transfer (bulk statistics feature) allows many of the same functions as the bulk file MIB (CISCO-BULK-FILE-MIB.my), but offers some key advantages. The main advantage is that this feature can be configured through the CLI and does not require an external monitoring application.

Periodic MIB data collection and transfer is mainly targeted for medium to high-end platforms that have sufficient local storage (volatile or permanent) to store bulk statistics files. Locally storing bulk statistics files helps minimize loss of data during temporary network outages.

This feature also has more powerful data selection features than the bulk file MIB; it allows grouping of MIB objects from different tables into data groups (object lists). It also incorporates a more flexible instance selection mechanism, where the application is not restricted to fetching an entire MIB table.

How to Configure Periodic MIB Data Collection and Transfer

Configuring a Bulk Statistics Object List

The first step in configuring the Periodic MIB Data Collection and Transfer Mechanism is to configure one or more object lists.

SUMMARY STEPS

1. **configure**
2. **snmp-server mib bulkstat object-list** *list-name*
3. **add** {**oid** | *object-name*}
4. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**snmp-server mib bulkstat object-list** *list-name* **Example:** `snmp-server mib bulkstat object-list ifMib`	Defines an SNMP bulk statistics object list and enters bulk statistics object list configuration mode.

Step 3	**add** {**oid**	*object-name*}
		Example:
		`RP/0/RP0/CPU0:router(config-bulk-objects)# add 1.3.6.1.2.1.2.2.1.11`
		`RP/0/RP0/CPU0:router(config-bulk-objects)# add ifAdminStatus`
		`RP/0/RP0/CPU0:router(config-bulk-objects)# add ifDescr`
			Adds a MIB object to the bulk statistics object list. Repeat as desired until all objects to be monitored in this list are added.
			Note
			All the objects in a bulk statistics object list have to be indexed by the same MIB index. However, the objects in the object list do not need to belong to the same MIB or MIB table.
			When specifying an object name instead of an OID (using the add command), only object names with mappings shown in the **show snmp mib object** command output can be used.

	Command or Action	Purpose
Step 4	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session. • **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Configuring a Bulk Statistics Schema

The second step in configuring periodic MIB data collection and transfer is to configure one or more schemas.

Before you begin

The bulk statistics object list to be used in the schema must be defined.

SUMMARY STEPS

1. **configure**
2. **snmp-server mib bulkstat schema** *schema-name*
3. **object-list** *list-name*
4. Do one of the following:
   - **instance exact** {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
   - **instance wild** {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
   - **instance range start** *oid* **end** *oid*
   - **instance repetition** *oid* **max** *repeat-number*
5. **poll-interval** *minutes*
6. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**snmp-server mib bulkstat schema** *schema-name*
	Example:
	`RP/0/RP0/CPU0:router(config)# snmp-server mib bulkstat schema intE0`
	`RP/0/RP0/CPU0:router(config-bulk-sc)#`
		Names the bulk statistics schema and enters bulk statistics schema mode.

Step 3	**object-list** *list-name* **Example:** `RP/0/RP0/CPU0:router(config-bulk-sc)# object-list ifMib`	Specifies the bulk statistics object list to be included in this schema. Specify only one object list per schema. If multiple object-list commands are executed, the earlier ones are overwritten by newer commands.

Step 4	Do one of the following:
	• **instance exact** {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
	• **instance wild** {**interface** *interface-id* [**sub-if**] | **oid** *oid*}
	• **instance range start** *oid* **end** *oid*
	• **instance repetition** *oid* **max** *repeat-number*
	Example:
	`RP/0/RP0/CPU0:router(config-bulk-sc)# instance wild oid 1`
	or
	`RP/0/RP0/CPU0:router(config-bulk-sc)# instance exact interface TenGigE 0/1.25`
	or
	`RP/0/RP0/CPU0:router(config-bulk-sc)# instance range start 1 end 2`
	or
	`RP/0/RP0/CPU0:router(config-bulk-sc)# instance repetition 1 max 4`
		Specifies the instance information for objects in this schema:
		• The **instance exact** command indicates that the specified instance, when appended to the object list, represents the complete OID.
		• The **instance wild** command indicates that all subindices of the specified OID belong to this schema. The wild keyword allows you to specify a partial, "wild carded" instance.
		• The **instance range** command indicates a range of instances on which to collect data.
		• The **instance repetition** command indicates data collection to repeat for a certain number of instances of a MIB object.
		Note
		Only one **instance** command can be configured per schema. If multiple **instance** commands are executed, the earlier ones are overwritten by new commands.

Step 5	**poll-interval** *minutes* **Example:** `RP/0/RP0/CPU0:router(config-bulk-sc)# poll-interval 10`	Sets how often data should be collected from the object instances specified in this schema, in minutes. The default is once every 5 minutes. The valid range is from 1 to 20000.
Step 6	Use the **commit** or **end** command.	**commit** —Saves the configuration changes and remains within the configuration session. **end** —Prompts user to take one of these actions: • **Yes** — Saves configuration changes and exits the configuration session.

	Command or Action	Purpose
		• **No** —Exits the configuration session without committing the configuration changes. • **Cancel** —Remains in the configuration session, without committing the configuration changes.

Configuring Bulk Statistics Transfer Options

The final step in configuring periodic MIB data collection and transfer is to configure the transfer options. The collected MIB data are kept in a local file-like entity called a VFile (virtual file, referred to as a bulk statistics file in this document). This file can be transferred to a remote network management station at intervals you specify.

Before you begin

The bulk statistics object lists and bulk statistics schemas must be defined before configuring the bulk statistics transfer options.

SUMMARY STEPS

1. **configure**
2. **snmp-server mib bulkstat transfer-id** *transfer-id*
3. **buffer-size** *bytes*
4. **format** {**bulkBinary** | **bulkASCII** | **schemaASCII**}
5. **schema** *schema-name*
6. **transfer-interval** *minutes*
7. **url primary** *url*
8. **url secondary** *url*
9. **retry** *number*
10. **retain** *minutes*
11. **enable**
12. **commit** *minutes*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**snmp-server mib bulkstat transfer-id** *transfer-id* **Example:** `RP/0/RP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1`	Identifies the transfer configuration with a name (*transfer-id* argument) and enters bulk statistics transfer configuration mode.
Step 3	**buffer-size** *bytes* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# buffersize 3072`	(Optional) Specifies the maximum size for the bulk statistics data file, in bytes. The valid range is from 1024 to 2147483647 bytes. The default buffer size is 2048 bytes. **Note** If the maximum buffer size for a bulk statistics file is reached before the transfer interval time expires, all additional data received is deleted. To correct this behavior, you can decrease the polling frequency, or increase the size of the bulk statistics buffer.
Step 4	**format** {**bulkBinary** | **bulkASCII** | **schemaASCII**} **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# format schemaASCII`	(Optional) Specifies the format of the bulk statistics data file (VFile). The default is schemaASCII. **Note** Transfers can only be performed using schemaASCII (cdcSchemaASCII) format. SchemaASCII is a human-readable format that contains parser-friendly hints for parsing data values.

Step 5	**schema** *schema-name*
	Example:
	`RP/0/RP0/CPU0:router(config-bulk-tr)# schema TenGigE 0/5/0/11/1`
	`RP/0/RP0/CPU0:router(config-bulk-tr)# schema TenGigE/0-CAR`
	`RP/0/RP0/CPU0:router(config-bulk-tr)# schema TenGigE 0/5/0/11/1`
		Specifies the bulk statistics schema to be transferred. Repeat this command as desired. Multiple schemas can be associated with a single transfer configuration; all collected data are placed in a single bulk data file (VFile).

Step 6	**transfer-interval** *minutes* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# transfer-interval 20`	(Optional) Specifies how often the bulk statistics file are transferred, in minutes. The default value is once every 30 minutes. The transfer interval is the same as the collection interval.
Step 7	**url primary** *url* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# url primary ftp://user:password@host/folder/bulkstat1`	Specifies the network management system (host) that the bulk statistics data file is transferred to, and the protocol to use for transfer. The destination is specified as a Uniform Resource Locator (URL). FTP or TFTP can be used for the bulk statistics file transfer.
Step 8	**url secondary** *url* **Example:**	(Optional) Specifies a backup transfer destination and protocol for use in the event that transfer to the primary

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(config-bulk-tr)# url secondary tftp://10.1.0.1/tftpboot/user/bulkstat1`	location fails. FTP or TFTP can be used for the bulk statistics file transfer.
Step 9	**retry** *number* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# retry 1`	(Optional) Specifies the number of transmission retries. The default value is 0 (in other words, no retries). If an attempt to send the bulk statistics file fails, the system can be configured to attempt to send the file again using this command. One retry includes an attempt first to the primary destination then, if the transmission fails, to the secondary location. For example, if the retry value is 1, an attempt is made first to the primary URL, then to the secondary URL, then to the primary URL again, then to the secondary URL again. The valid range is from 0 to 100. If all retries fail, the next normal transfer occurs after the configured transfer-interval time.
Step 10	**retain** *minutes* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# retain 60`	(Optional) Specifies how long the bulk statistics file should be kept in system memory, in minutes, after the completion of the collection interval and a transmission attempt is made. The default value is 0. Zero (0) indicates that the file is deleted immediately after the transfer is attempted. The valid range is from 0 to 20000. **Note** If the retry command is used, you should configure a retain interval larger than 0. The interval between retries is the retain interval divided by the retry number. For example, if **retain 10** and **retry 2** are configured, two retries are attempted once every 5 minutes. Therefore, if retain 0 is configured, no retries are attempted.
Step 11	**enable** **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# enable`	Begins the bulk statistics data collection and transfer process for this configuration. • For successful execution of this action, at least one schema with non-zero number of objects must be configured. • Periodic collection and file transfer begins only if this command is configured. Conversely, the **no enable** command stops the collection process. A subsequent **enable** starts the operations again. • Each time the collection process is started using the **enable** command, data is collected into a new bulk statistics file. When the **no enable** command is used, the transfer process for any collected data immediately begins (in other words, the existing bulk statistics file is transferred to the specified management station).

	Command or Action	Purpose
Step 12	**commit** *minutes* **Example:** `RP/0/RP0/CPU0:router(config-bulk-tr)# retain 60`	If the maximum buffer size for a bulk statistics file is reached before the transfer interval time expires, the transfer operation is still initiated, but any bulk statistics data received after the file was full, and before it was transferred, are deleted. To correct this behavior, you can decrease the polling frequency, or increase the size of the bulk statistics buffer. If **retain 0** is configured, no retries are attempted. This is because the interval between retries is the retain value divided by the retry value. For example, if **retain 10** and **retry 2** are configured, retries are attempted once every 5 minutes. Therefore, if you configure the retry command, you should also configure an appropriate value for the retain command.

Periodic MIB Data Collection and Transfer: Example

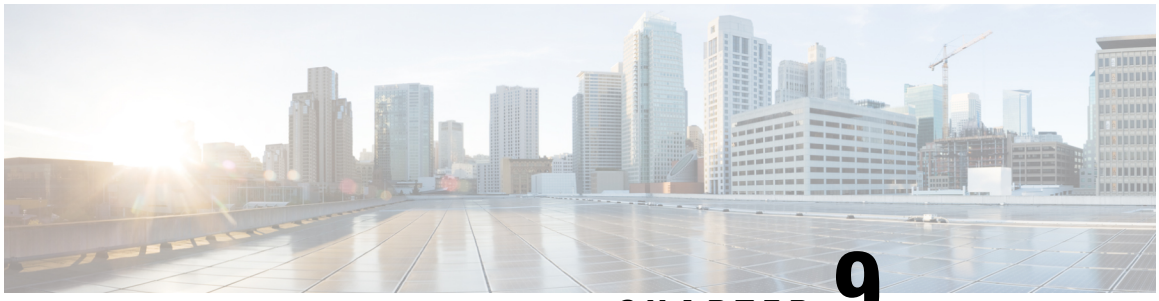
This example shows how to configure periodic MIB data collection and transfer:

```
snmp-server mib bulkstat object-list cempo
add cempMemPoolName
add cempMemPoolType
!
snmp-server mib bulkstat schema cempWild
object-list cempo
instance wild oid 8695772
poll-interval 1
!
snmp-server mib bulkstat schema cempRepeat
object-list cempo
instance repetition 8695772.1 max 4294967295
poll-interval 1
!
snmp-server mib bulkstat transfer-id cempt1
enable
url primary tftp://223.255.254.254/auto/tftp-sjc-users3/username/dumpdcm
schema cempWild
schema cempRepeat
transfer-interval 2
!
```

This example shows sample bulk statistics file content:

```
Schema-def cempt1.cempWild "%u, %s, %s, %d" Epochtime instanceoid
            1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempWild: 1339491515, 8695772.1, processor, 2
cempt1.cempWild: 1339491515, 8695772.2, reserved, 11
cempt1.cempWild: 1339491515, 8695772.3, image, 12
cempt1.cempWild: 1339491575, 8695772.1, processor, 2
cempt1.cempWild: 1339491575, 8695772.2, reserved, 11
cempt1.cempWild: 1339491575, 8695772.3, image, 12
```

```
Schema-def cempt1.cempRepeat "%u, %s, %s, %d" Epochtime instanceoid
            1.3.6.1.4.1.9.9.221.1.1.1.1.3 1.3.6.1.4.1.9.9.221.1.1.1.1.2
cempt1.cempRepeat: 1339491515, 8695772.1, processor, 2
cempt1.cempRepeat: 1339491515, 8695772.2, reserved, 11
cempt1.cempRepeat: 1339491515, 8695772.3, image, 12
cempt1.cempRepeat: 1339491515, 26932192.1, processor, 2
cempt1.cempRepeat: 1339491515, 26932192.2, reserved, 11
cempt1.cempRepeat: 1339491515, 26932192.3, image, 12
cempt1.cempRepeat: 1339491515, 35271015.1, processor, 2
cempt1.cempRepeat: 1339491515, 35271015.2, reserved, 11
cempt1.cempRepeat: 1339491515, 35271015.3, image, 12
cempt1.cempRepeat: 1339491515, 36631989.1, processor, 2
cempt1.cempRepeat: 1339491515, 36631989.2, reserved, 11
cempt1.cempRepeat: 1339491515, 36631989.3, image, 12
cempt1.cempRepeat: 1339491515, 52690955.1, processor, 2
cempt1.cempRepeat: 1339491515, 52690955.2, reserved, 11
cempt1.cempRepeat: 1339491515, 52690955.3, image, 12
```



CHAPTER 9

Configuring Flexible Command Line Interface

This module describes how to configure and use flexible command line interface (CLI) configuration groups.

- Flexible CLI Configuration Groups, on page 87
- Flexible Configuration Restrictions, on page 87
- Configuring a Configuration Group, on page 89
- Verifying the Configuration of Configuration Groups, on page 91
- Regular Expressions in Configuration Groups, on page 93
- Configuration Examples for Flexible CLI Configuration, on page 104

Flexible CLI Configuration Groups

Flexible command line interface (CLI) configuration groups provide the ability to minimize repetitive configurations by defining a series of configuration statements in a configuration group, and then applying this group to multiple hierarchical levels in the router configuration tree.

Flexible CLI configuration groups utilize regular expressions that are checked for a match at multiple submodes of the configuration tree based on where the group is applied within the hierarchy. If a match is found at a configuration submode, the corresponding configuration defined in the group is inherited within the matched submode.

Flexible CLI configuration groups also provide an auto-inheritance feature. Auto-inheritance means that any change done to a CLI configuration group is automatically applied to the configuration in any matched submodes that have an apply-group at that hierarchical level. This allows you to make a configuration change or addition once, and have it applied automatically in multiple locations, depending on where you have applied the flexible CLI configuration group.

Flexible Configuration Restrictions

Note these restrictions while using flexible configuration groups:

- Flexible CLI configuration groups are not supported in administration configurations and corresponding apply-groups are not supported in administration configurations.
- Use of preconfigured interfaces in configuration groups is not supported.
- Downgrading from an image that supports configuration groups to an image that does not support them is not supported.

- Access lists, quality of service and route policy configurations do not support the use of configuration groups. Configurations such as these are not valid:

```
group g-not-supported
 ipv4 access-list ...
 !
 ipv6 access-list ...
 !
 ethernet-service access-list ...
 !
 class-map ...
 !
 policy-map ...
 !
 route-policy ...
 !
end-group
```

  You can, however, reference such configurations, as shown in this example:

```
group g-reference-ok
 router bgp 6500
  neighbor 7::7
   remote-as 65000
   bfd fast-detect
   update-source Loopback300
   graceful-restart disable
   address-family ipv6 unicast
       route-policy test1 in
    route-policy test2 out
    soft-reconfiguration inbound always
   !
  !
 !
 interface Bundle-Ether1005
   bandwidth 10000000
   mtu 9188
      service-policy output input_1
   load-interval 30
 !
end-group
```

- Some regular expressions are not supported within groups. For example, '?', '|' and '$,' are not supported within groups. Also some characters such as /d and /w are not supported.
  - The choice operator "|" to express multiple match expressions within a regular expression is not supported. For example, these expressions are not supported:

    `Gig.*|Gig.*\..*`—To match on either Gigabit Ethernet main interfaces or Gigabit Ethernet sub-interfaces.

    `Gig.*0/0/0/[1-5]|Gig.*0/0/0/[10-20]`—To match on either Gig.*0/0/0/[1-5] or Gig.*0/0/0/[10-20].

    `'TenGigE.*|HundredGigE.*`—To match on either TenGigE.* or HundredGigE.* .

- Commands that require a node identifier for the **location** keyword are not supported. For example, this configuration is not supported:

```
lpts pifib hardware police location 0/RP0/CPU0
```

- Overlapping regular expressions within a configuration group for the same configuration are not supported. For example:

```
group G-INTERFACE
interface 'gig.*a.*'
  mtu 1500
!
interface 'gig.*e.* '
  mtu 2000
!
end-group

interface gigabitethernet0/0/0/* ---- where * is 0 to 79 or 0 to 39
  apply-group G-INTERFACE
```

  This configuration is not permitted because it cannot be determined whether the `interface GigabitEthernet0/0/0/*` configuration inherits `mtu 1500` or `mtu 2000`. Both expressions in the configuration group match GigabitEthernet0/0/0/*.

- Up to eight configuration groups are permitted on one apply-group command.

Configuring a Configuration Group

A configuration group includes a series of configuration statements that can be used in multiple hierarchical levels in the router configuration tree. By using regular expressions in a configuration group, you can create generic commands that can be applied in multiple instances.

Use this task to create and use a configuration group.

Note Flexible CLI configurations are not available through the XML interface.

SUMMARY STEPS

1. **configure**
2. **group** *group-name*
3. Enter configuration commands, starting from global configuration mode. Use regular expressions for interface names and other variable instances.
4. **end-group**
5. **apply-group**

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 **group** *group-name*

Example:

```
RP/0/RP0/CPU0:router(config)# group g-interf
```

Specifies a name for a configuration group and enters group configuration mode to define the group.The *group-name* argument can have up to 32 characters and cannot contain any special characters.

Step 3 Enter configuration commands, starting from global configuration mode. Use regular expressions for interface names and other variable instances.

Example:

```
RP/0/RP0/CPU0:router(config)# group g-interf
RP/0/RP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-if)# mtu 1500
```

Specifies the configuration statements that you want included in this configuration group.

For more information regarding the use of regular expressions, see Configuration Group Inheritance with Regular Expressions: Example, on page 102. This example is applicable to all Gigabit Ethernet interfaces.

Step 4 **end-group**

Example:

```
RP/0/RP0/CPU0:router(config-GRP-if)# end-group
```

Completes the configuration of a configuration group and exits to global configuration mode.

Step 5 **apply-group**

Example:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:router(config-if)# apply-group g-interf
```

Adds the configuration of the configuration group into the router configuration applicable at the location that the group is applied. Groups can be applied in multiple locations, and their effect depends on the location and context.

The MTU value from the group g-interf is applied to the interface GigabitEthernet0/2/0/0. If this group is applied in global configuration mode, the MTU value is inherited by all Gigabit Ethernet interfaces that do not have an MTU value configured.

Simple Configuration Group: Example

This example shows how to use configuration groups to add a global configuration to the system:

```
RP/0/RP0/CPU0:router(config)# group g-logging
RP/0/RP0/CPU0:router(config-GRP)# logging trap notifications
```

```
RP/0/RP0/CPU0:router(config-GRP)# logging console debugging
RP/0/RP0/CPU0:router(config-GRP)# logging monitor debugging
RP/0/RP0/CPU0:router(config-GRP)# logging buffered 10000000
RP/0/RP0/CPU0:router(config-GRP)# end-group

RP/0/RP0/CPU0:router(config)# apply-group g-logging
```

When this configuration is committed, all commands contained in the g-logging configuration group are committed.

Configuration Group Applied to Different Places: Example

Configuration groups can be applied to different places, and their effect depends on the context within which they are applied. Consider this configuration group:

```
RP/0/RP0/CPU0:router(config)# group g-interfaces
RP/0/RP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-if)# mtu 1500
RP/0/RP0/CPU0:router(config-GRP-if)# exit
RP/0/RP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-if)# mtu 1000
RP/0/RP0/CPU0:router(config-GRP-if)# exit
RP/0/RP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-if)# mtu 2000
RP/0/RP0/CPU0:router(config-GRP-if)# end-group
```

This group can be applied to Gigabit Ethernet interface and in each instance the applicable MTU is applied. For instance, in this example, the Gigabit Ethernet interface is configured to have an MTU of 1000:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:router(config-if)# apply-group g-interfaces
RP/0/RP0/CPU0:router(config-if)# ipv4 address 2.2.2.2 255.255.255.0
```

In this example, the Gigabit Ethernet interface is configured to have an MTU of 1500:

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet0/2/0/0
RP/0/RP0/CPU0:router(config-if)# apply-group g-interfaces
RP/0/RP0/CPU0:router(config-if)# ipv4 address 3.3.3.3 255.255.255.0
```

The same configuration group is used in both cases, but only the applicable configuration statements are used.

Verifying the Configuration of Configuration Groups

Use this task to verify the router configuration using configuration groups:

SUMMARY STEPS

1. **show running-config group** [*group-name*]

2. **show running-config**
3. **show running-config inheritance**
4. **show running-config interface x/y/z inheritance** *detail*

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**show running-config group** [*group-name*]
	Example:
	`RP/0/RP0/CPU0:router# show running-config group`
	`group g-int-ge`
	` interface 'GigabitEthernet.*'`
	`  mtu 1000`
	`  negotiation auto`
	` !`
	`end-group`
		Displays the contents of a specific or all configured configuration groups.

Step 2	**show running-config**
	Example:
	`RP/0/RP0/CPU0:router# show running-config`
	`group G-INTERFACE-MTU`
	` interface 'GigabitEthernet.*'`
	`  mtu 1500`
	` !`
	`end-group`
	`interface interface GigabitEthernet0/4/1/0`
	` apply-group G-INTERFACE-MTU`
	`!`
	`interface interface GigabitEthernet0/4/1/1`
	` apply-group G-INTERFACE-MTU`
	` mtu 2000`
	`!`
		Displays the running configuration. Any applied groups are displayed. There is no indication as to whether these configuration groups affect the actual configuration or not. In this example, although the group G-INTERFACE-MTU is applied to interface GigabitEthernet0/4/1/1, the configured MTU value is 2000 and not 1500. This happens if the command **mtu 2000** is configured directly on the interface. An actual configuration overrides a configuration group configuration if they are the same.

Step 3	**show running-config inheritance**
	Example:
	`RP/0/RP0/CPU0:router# show running-config inheritance`
	`.`
	`.`
	`group G-INTERFACE-MTU`
	` interface 'GigabitEthernet.*'`
	`  mtu 1500`
	` !`
	`end-group`
	`.`
		Displays the inherited configuration where ever a configuration group has been applied.

	Command or Action	Purpose
	. interface interface GigabitEthernet0/4/1/0 ## Inherited from group G-INTERFACE-MTU mtu 1500 ! interface interface GigabitEthernet0/4/1/1 mtu 2000 ! . .	
Step 4	**show running-config interface x/y/z inheritance** *detail* **Example:** RP/0/RP0/CPU0:router# **show running-config interface** interface GigabitEthernet0/4/1/0 **inheritance** **detail** interface interface GigabitEthernet0/4/1/0 ## Inherited from group G-INTERFACE-MTU mtu 1500	Displays the inherited configuration for a specific configuration command.

Regular Expressions in Configuration Groups

Regular expressions are used in configuration groups to make them widely applicable. Portable Operating System Interface for UNIX (POSIX) 1003.2 regular expressions are supported in the names of configuration statements. Single quotes must be used to delimit a regular expression.

Note Not all POSIX regular expressions are supported.

Regular Expressions for Interface Identifiers

Configuration groups do not accept exact interface identifiers. You must use a regular expression to identify a group of interfaces that are applicable to the configuration group. The regular expression '.*' is not allowed. You must begin the regular expression for an interface identifier with an unambiguous word, followed by the regular expression. For example, to configure Gigabit Ethernet interfaces, use the regular expression 'GigabitEthernet.*'.

To display a list of available interface types for your router configuration, enter **interface ?** at the configuration group prompt:

```
RP/0/RP0/CPU0:router(config-GRP)# interface ?

  ATM              'RegExp': ATM Network Interface(s)
  BVI              'RegExp': Bridge-Group Virtual Interface
  Bundle-Ether     'RegExp': Aggregated Ethernet interface(s)
  GigabitEthernet  'RegExp': GigabitEthernet/IEEE 802.3 interface(s)
  IMA              'RegExp': ATM Network Interface(s)
  Loopback         'RegExp': Loopback interface(s)
  MgmtEth          'RegExp': Ethernet/IEEE 802.3 interface(s)
```

```
  Multilink        'RegExp': Multilink network interface(s)
  Null             'RegExp': Null interface
  PW-Ether         'RegExp': PWHE Ethernet Interface
  PW-IW            'RegExp': PWHE VC11 IP Interworking Interface
  Serial           'RegExp': Serial network interface(s)
  tunnel-ip        'RegExp': GRE/IPinIP Tunnel Interface(s)
  tunnel-mte       'RegExp': MPLS Traffic Engineering P2MP Tunnel interface(s)
  tunnel-te        'RegExp': MPLS Traffic Engineering Tunnel interface(s)
  tunnel-tp        'RegExp': MPLS Transport Protocol Tunnel interface
```

Note Although you are required to enter only enough characters for the interface type to be unique, it is recommended that you enter the entire phrase. All interface types used in regular expressions are case-sensitive.

To specify a subinterface, prefix the expression with the characters \. (backslash period). For example, use `interface 'GigabitEthernet.*\..*'` to configure all Gigabit Ethernet subinterfaces.

You can specify Layer 2 transport interfaces or point-to-point interfaces as shown in these examples:

```
group g-l2t
  interface 'Gi.*\..*' l2transport
.
.
end-group
group g-ptp
  interface 'Gi.*\..*' point-to-point
.
.
end-group
```

Regular Expressions for an OSPF Configuration

Exact router process names and OSPF areas cannot be used. You must use a regular expression to specify a process name or group of OSPF areas. To specify that the OSFP area can be either a scalar value or an IP address, use the regular expression '.*', as in this example:

```
group g-ospf
router ospf '.*'
area '.*'
mtu-ignore enable
!
!
end-group
```

To specify that the OSPF area must be an IP address, use the expression '\.' as in this example:

```
group g-ospf-ipaddress
router ospf '.*\..*\..*\..*'
area '.*'
passive enable
!
!
 end-group
```

To specify that the OSPF area must be a scalar value, use the expression '1.*', as in this example:

```
group g-ospf-match-number
router ospf '.*'
area '1.*'
passive enable
!
!
end-group
```

Regular Expressions for a BGP AS

Exact BGP AS values cannot be used in configuration groups. Use a regular expression to specify either AS plain format, or AS dot format as in the format X.Y. To match AS plain format instances, use a simple regular expression. To match AS dot format instances, use two regular expressions separated by a dot, as shown in this example:

```
group g-bgp
router bgp '*'.'*'
address-family ipv4 unicast
!
!
end-group
```

Regular Expressions for ANCP

Exact Access Node Control Protocol (ANCP) sender-name identifiers cannot be used in configuration groups. Because the sender name argument can be either an IP address or a MAC address, you must specify in the regular expression which one is being used. Specify an IP address as `'.*\..*\..*\..*'`; specify a MAC address as `'.*\..*\..*'`.

Resolving to a Uniform Type

Regular expressions must resolve to a uniform type. This is an example of an illegal regular expression:

```
group g-invalid
 interface `.*'
  bundle port-priority 10
 !
interface `.*Ethernet.*'
  bundle port-priority 10
 !
end-group
```

In this example, the **bundle** command is supported for interface type GigabitEthernet but not for interface type 'FastEthernet'. The regular expressions '.*' and '.*Ethernet.*' match both GigabitEthernet and FastEthernet types. Because the **bundle** command is not applicable to both these interface types, they do not resolve to a uniform type and therefore the system does not allow this configuration.

Note If the system cannot determine from the regular expression what the configuration should be, the expression is not considered valid.

Note The regular expression '.*' is not allowed when referring to an interface identifier. You must begin the regular expression for an interface identifier with an unambiguous word, followed by the regular expression. Refer to *Regular Expressions for Interface Identifiers* in this section for more information.

Overlapping Regular Expressions

Regular expressions are used in names of configuration statements within a configuration group. This permits inheritance by the configuration when applied to matching names. Single quotes are used to delimit the regular expression. Overlapping regular expression within a configuration group for the same configuration is permitted.

The example, given below, illustrates the process of creating and applying multiple configuration groups:

```
RP/0//CPU0:router(config)#group FB_flexi_snmp
RP/0//CPU0:router(config-GRP)# snmp-server vrf '.*'
RP/0//CPU0:router(config-GRP-snmp-vrf)# host 1.1.1.1 traps version 2c group_1
RP/0//CPU0:router(config-GRP-snmp-vrf)# host 1.1.1.1 informs version 2c group_1
RP/0//CPU0:router(config-GRP-snmp-vrf)# context group_1

RP/0//CPU0:router(config-GRP-snmp-vrf)#
RP/0//CPU0:router(config-GRP-snmp-vrf)#commit

RP/0//CPU0:router(config-GRP-snmp-vrf)#root
RP/0//CPU0:router(config)#
RP/0//CPU0:router(config)#snmp-server vrf vrf1
RP/0//CPU0:router(config-snmp-vrf)#snmp-server vrf vrf10
RP/0//CPU0:router(config-snmp-vrf)#!
RP/0//CPU0:router(config-snmp-vrf)#snmp-server vrf vrf100
RP/0//CPU0:router(config-snmp-vrf)#
RP/0//CPU0:router(config-snmp-vrf)#commit

RP/0//CPU0:router(config-snmp-vrf)#root
RP/0//CPU0:router(config)#
RP/0//CPU0:router(config)#apply-group FB_flexi_snmp
RP/0//CPU0:router(config)#do sh running-config group
group FB_flexi_snmp
 snmp-server vrf '.*'
  host 1.1.1.1 traps version 2c group_1
  host 1.1.1.1 informs version 2c group_1
  context group_1
 !
end-group
apply-group FB_flexi_snmp
snmp-server vrf vrf1
!
snmp-server vrf vrf10
!
snmp-server vrf vrf100
!
RP/0//CPU0:ios#show running-config inheritance detail


group FB_flexi_snmp
 snmp-server vrf '.*'
  host 1.1.1.1 traps version 2c group_1
  host 1.1.1.1 informs version 2c group_1
  context group_1
 !
```

```
end-group
snmp-server vrf vrf1
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 traps version 2c group_1
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 informs version 2c group_1
 ## Inherited from group FB_flexi_snmp
 context group_1
!
snmp-server vrf vrf10
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 traps version 2c group_1
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 informs version 2c group_1
 ## Inherited from group FB_flexi_snmp
 context group_1
!
snmp-server vrf vrf100
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 traps version 2c group_1
 ## Inherited from group FB_flexi_snmp
 host 1.1.1.1 informs version 2c group_1
 ## Inherited from group FB_flexi_snmp
 context group_1
```

The example given below demonstrates the regular expression. In this example `snmp-server vrf '.*'` and `snmp-server vrf '[\w]+` are two different regular expressions.

```
group FB_flexi_snmp
snmp-server vrf '.*'
host 1.1.1.1 traps version 2c group_1
host 1.1.1.1 informs version 2c group_1
context group_1
!
snmp-server vrf '[\w]+'
host 2.2.2.2 traps version 2c group_2
host 2.2.2.2 informs version 2c group_2
context group_2
!
end-group
```

This individual regular expression gets combined to all the three expressions - `snmp-server vrf vrf1`, `snmp-server vrf vrf10` and `snmp-server vrf vrf100` as given below.

```
apply-group FB_flexi_snmp
snmp-server vrf vrf1
!
snmp-server vrf vrf10
!
snmp-server vrf vrf100
!
```

In a configuration group, there can be instances of regular expressions overlap. In such cases, the regular expression with the highest priority is activated and inherited, when applied. It has that regular expression, which comes first in the lexicographic order that has the highest priority.

The following example shows how to use overlapping regular expressions and how the expression with higher priority is applied:

```
 group FB_flexi_snmp

 snmp-server vrf '.*’

  host 1.1.1.1 traps version 2c group_1

  host 1.1.1.1 informs version 2c group_1

  context group_1

 !

 snmp-server vrf '[\w]+’

  host 2.2.2.2 traps version 2c group_2
  host 2.2.2.2 informs version 2c group_2
  context group_2
 !
end-group
```

The expression shown below has the highest priority:

```
  group FB_flexi_snmp

  snmp-server vrf '.*’

  host 1.1.1.1 traps version 2c group_1

  host 1.1.1.1 informs version 2c group_1

  context group_1
```

The examples given above, show two different regular expression `snmp-server vrf '.*’` and `snmp-server vrf '[\w]+'`.

The expression below, shows how these two expressions get merged together:

```
 apply-group FB_flexi_snmp

 snmp-server vrf vrf1
 !
 snmp-server vrf vrf10
 !
 snmp-server vrf vrf100
 !
```

Any change in a regular expression with lower priority will not affect the inheritance.

Any changes made to an existing regular expression, which is of less (non-top) priority, it will not have any effect on the inheritance.

```
 snmp-server vrf '[\w]+'

 host 2.2.2.2 traps version 2c group_2
 host 2.2.2.2 informs version 2c group_2
 context group_2
```

The expression with the higher priority gets inherited, as shown below:

```
group FB_flexi_snmp

snmp-server vrf '.*'

 host 1.1.1.1 traps version 2c group_1

 host 1.1.1.1 informs version 2c group_1

 context group_1
```

Apply Groups Priority Inheritance

Priority governs inheritance.

Note From the Cisco IOS XR, Release 6.3.1 onwards, you are able to enter the Flexible CLI config group definition, **apply-group** and **exclude-group** command in any order as long as the entire commit has all the group definitions needed.

Apply groups priority inheritance helps flexible configuration groups to handle common configuration statements between groups. When multiple configuration groups have common configuration statements, the inheritance priority is such that the configuration statements present in inner groups have precedence over those configuration statements present in outer groups. In case of tiebreakers, the priority is assigned in accordance to the lexicographical order of regular expressions. User defined order of commands are not accepted.

For example, a configuration statement in configuration group ONE has precedence over another group. A configuration statement in configuration group SEVEN is used only if it does not exist in any other group. Within a configuration group, inheritance priority is the longest match.

```
   apply-group SIX SEVEN
    router ospf 0
   apply-group FOUR FIVE
    area 0
   apply-group THREE
    interface GigabitEthernet0/0/0/0
   apply-group ONE TWO

  !
 !
!
```

The above example shows two scenarios. The inner most group (**apply-group ONE TWO**) has the highest priority. Case 1

The first scenario shows which group gets the priority. The example states which group is applied between different configuration groups (different groups with nothing in common). While applying group one (ONE TWO), all the seven groups matches the interface `interface GigabitEthernet0/0/0/0`- is applied.

Case 2

Here, when all have the same (common) configuration, group one will be active. That is `apply-group ONE TWO` is active. If group ONE is deleted, then group TWO will be active.

Configuration Examples Using Regular Expressions

Configuration Group with Regular Expression: Example

This example shows the definition of a configuration group for configuring Gigabit Ethernet interfaces with ISIS routing parameters, using regular expressions for the exact interface:

```
RP/0/RP0/CPU0:router(config)# group g-isis-gige
RP/0/RP0/CPU0:router(config-GRP)# router isis '.*'
RP/0/RP0/CPU0:router(config-GRP-isis)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-isis-if)# lsp-interval 20
RP/0/RP0/CPU0:router(config-GRP-isis-if)# hello-interval 40
RP/0/RP0/CPU0:router(config-GRP-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-GRP-isis-if-af)# metric 10
RP/0/RP0/CPU0:router(config-GRP-isis-if-af)# end-group
RP/0/RP0/CPU0:router(config)#
```

To illustrate the use of this configuration group, assume that you want to configure these Gigabit Ethernet interfaces with the ISIS routing parameters:

```
router isis green
 interface GigabitEthernet0/0/0/0
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/1
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/2
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
 interface GigabitEthernet0/0/0/3
  lsp-interval 20
  hello-interval 40
  address-family ipv4 unicast
   metric 10
  !
 !
!
```

There are three possible ways to use the configuration group to configure these interfaces. The first is by applying the group within the interface configuration, as shown here:

```
router isis green
 interface GigabitEthernet0/0/0/0
     apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/1
     apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/2
     apply-group g-isis-gige
  !
 !
 interface GigabitEthernet0/0/0/3
     apply-group g-isis-gige
  !
 !
```

In this situation, only the interfaces to which you apply the configuration group inherit the configuration.

The second way to configure these interfaces using the configuration group is to apply the configuration group within the **router isis** configuration, as shown here:

```
router isis green
    apply-group g-isis-gige
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
!
```

In this way, any other Gigabit Ethernet interfaces that you configure in the ISIS green configuration also inherit these configurations.

The third way to configure these interfaces using the configuration group is to apply the group at the global level as shown here:

```
   apply-group g-isis-gige
router isis green
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/3
 !
!
```

In this example, the configuration of the group is applied to all Gigabit Ethernet interfaces configured for ISIS.

Configuration Group Inheritance with Regular Expressions: Example

Local Configuration Has Precedence Over Configuration Group

An explicit configuration takes precedence over a configuration applied from a configuration group. For example, assume that this configuration is running on the router:

```
router ospf 100
 packet-size 1000
!
```

You configure this configuration group, apply it, and commit it to the configuration.

```
RP/0/RP0/CPU0:router(config)# group g-ospf
RP/0/RP0/CPU0:router(config-GRP)# router ospf '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf)# nsf cisco
RP/0/RP0/CPU0:router(config-GRP-ospf)# packet-size 3000
RP/0/RP0/CPU0:router(config-GRP-ospf)# end-group

RP/0/RP0/CPU0:router(config)# apply-group g-ospf
```

The result is effectively this configuration:

```
router ospf 100
 packet-size 1000
 nsf cisco
```

Note that `packet-size 3000` is not inherited from the configuration group because the explicit local configuration has precedence.

Compatible Configuration Is Inherited

The configuration in the configuration group must match the configuration on the router to be inherited. If the configuration does not match, it is not inherited. For example, assume that this configuration is running on the router:

```
router ospf 100
 auto-cost disable
!
```

You configure this configuration and commit it to the configuration.

```
RP/0/RP0/CPU0:router(config)# group g-ospf
RP/0/RP0/CPU0:router(config-GRP)# router ospf '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf)# area '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf-ar)# packet-size 2000
RP/0/RP0/CPU0:router(config-GRP-ospf)# end-group

RP/0/RP0/CPU0:router(config)# apply-group g-ospf
```

```
RP/0/RP0/CPU0:router(config)# router ospf 200
RP/0/RP0/CPU0:router(config-ospf)# area 1
```

The result is effectively this configuration:

```
router ospf 100
  auto-cost disable

router ospf 200
  area 1
  packet-size 2000
```

The packet size is inherited by the ospf 200 configuration, but not by the ospf 100 configuration because the area is not configured.

Layer 2 Transport Configuration Group: Example

This example shows how to configure and apply a configuration group with Layer 2 transport subinterfaces:

```
RP/0/RP0/CPU0:router(config)# group g-l2trans-if
RP/0/RP0/CPU0:router(config-GRP)# interface 'TenGigE.*\..*' l2transport
RP/0/RP0/CPU0:router(config-GRP)# mtu 1514
RP/0/RP0/CPU0:router(config-GRP)# end-group

RP/0/RP0/CPU0:router(config)# interface TenGigE0/0/0/0.1 l2transport
RP/0/RP0/CPU0:router(config-if)# apply-group g-l2trans-if
```

When this configuration is committed, the Ten Gigabit Ethernet interface 0/0/0/0.1 inherits the 1514 MTU value. This is the output displayed from the **show running-config inheritence** command for the Ten Gigabit Ethernet interface:

```
interface TenGigE0/0/0/0.1 l2transport
 ## Inherited from group g-l2trans-if
 mtu 1514
!
```

Configuration Group Precedence: Example

When similar configuration statements are contained in multiple configuration groups, groups applied in inner configuration modes take precedence over groups applied in outer modes. This example shows two configuration groups that configure different cost values for OSPF.

```
RP/0/RP0/CPU0:router(config)# group g-ospf2
RP/0/RP0/CPU0:router(config-GRP)# router ospf '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf)# area '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf-ar)# cost 2
RP/0/RP0/CPU0:router(config-GRP-ospf-ar)# end-group

RP/0/RP0/CPU0:router(config)# group g-ospf100
RP/0/RP0/CPU0:router(config-GRP)# router ospf '.*'
```

```
RP/0/RP0/CPU0:router(config-GRP-ospf)# area '.*'
RP/0/RP0/CPU0:router(config-GRP-ospf-ar)# cost 100
RP/0/RP0/CPU0:router(config-GRP-ospf-ar)# end-group
```

If these configuration groups are applied as follows, the cost 2 specified in g-ospf2 is inherited by OSPF area 0 because the group is applied in a more inner configuration mode. In this case, the configuration in group g-ospf100 is ignored.

```
RP/0/RP0/CPU0:router(config)# router ospf 0
RP/0/RP0/CPU0:router(config-ospf)# apply-group g-ospf100
RP/0/RP0/CPU0:router(config-ospf)# area 0
RP/0/RP0/CPU0:router(config-ospf-ar)# apply-group g-ospf2
```

Changes to Configuration Group are Automatically Inherited: Example

When you make changes to a configuration group that is committed and applied to your router configuration, the changes are automatically inherited by the router configuration. For example, assume that this configuration is committed:

```
group g-interface-mtu
 interface 'GigabitEthernet.*'
  mtu 1500
 !
end-group

interface POS0/4/1/0
 apply-group g-interface-mtu
!
```

Now you change the configuration group as in this example:

```
RP/0/RP0/CPU0:router(config)# group g-interface-mtu
RP/0/RP0/CPU0:router(config-GRP)# interface 'GigabitEthernet.*'
RP/0/RP0/CPU0:router(config-GRP-if)# mtu 2000
RP/0/RP0/CPU0:router(config-GRP-if)# end-group
```

When this configuration group is committed, the MTU configuration for interface GigabitEthernet0/4/1/0 is automatically updated to 2000.

Configuration Examples for Flexible CLI Configuration

Basic Flexible CLI Configuration: Example

This example shows that the Media Access Control (MAC) accounting configuration from the gd21 configuration group is applied to all Gigabit Ethernet interfaces in slot 2, ports 1 to 9.

1. Configure the configuration group that configures MAC accounting:

```
RP/0/RP0/CPU0:router# show running group gd21

group gd21
interface 'GigabitEthernet0/0/0/2[1-9]'
description general interface inheritance check
load-interval 30
mac-accounting ingress
mac-accounting egress
!
end-group
```

2. Check that the corresponding apply-group is configured in global configuration or somewhere in the hierarchy:

```
RP/0/RP0/CPU0:router# show running | in apply-group gd21

Building configuration...
apply-group gd21
```

3. Check the concise local view of the configuration of some of the interfaces:

```
RP/0/RP0/CPU0:router# show running interface

interface GigabiEthernet0/0/0/21
!
interface GigabitEthernet0/0/0/22
!
```

4. Verify that the match and inheritance occur on these interfaces:

```
RP/0/RP0/CPU0:router# show running-config inheritance interface

interface GigabitEthernet0/0/0/21
## Inherited from group gd21
description general interface inheritance check
## Inherited from group gd21
load-interval 30
## Inherited from group gd21
mac-accounting ingress
## Inherited from group gd21
mac-accounting egress
!
Interface GigabitEthernet0/0/0/22
## Inherited from group gd21
description general interface inheritance check
## Inherited from group gd21
load-interval 30
## Inherited from group gd21
mac-accounting ingress
## Inherited from group gd21
mac-accounting egress
!
!
```

5. Verify that the inherited configuration actually takes effect:

```
RP/0/RP0/CPU0:router# show mac-accounting GigabitEthernet0/0/0/21
```

```
GigabitEthernet0/0/0/21
  Input (96 free)
    6c9c.ed35.90fd:  1271 packets, 98426 bytes
        Total: 1271 packets, 98426 bytes
  Output (96 free)
    6c9c.ed35.90fd:   774 packets, 63265 bytes
        Total: 774 packets, 63264 bytes
```

Interface MTU Settings for Different Interface Types: Example

This example shows that an MTU value is configured on different interface types.

1. Configure an interface MTU configuration group and apply this group:

```
RP/0/RP0/CPU0:router# show running group l2tr

group l2tr
interface 'GigabitEthernet0/0/0/3.*'
mtu 1500
!
interface 'GigabitEthernet0/0/0/9\..*'
mtu 1400
!
interface 'GigabitEthernet0/0/0/9\..*' l2transport
mtu 1400
!
end-group

RP/0/RP0/CPU0:router# show running | inc apply-group

Building configuration...

apply-group l2tr
```

2. Check the concise view and the inheritance view of the various interfaces:

```
RP/0/RP0/CPU0:router# show running interface gigabitEthernet0/0/0/30

interface GigabitEthernet0/0/0/30
!
RP/0/RP0/CPU0:router# show running interface gigabitEthernet0/0/0/30  inheritance detail

interface GigabitEthernet0/0/0/30
## Inherited from group l2tr
mtu 1500
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet0/0/0/9.800

interface GigabitEthernet0/0/0/9.800
  encapsulation dot1q 800
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet0/0/0/9.800 inheritance
detail

interface GigabitEthernet0/0/0/9.800
```

```
## Inherited from group l2tr
mtu 1400
encapsulation dot1q800
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet0/0/0/9.250

interface GigabitEthernet0/0/0/9.250 l2transport
  encapsulation dot1q 250
!

RP/0/RP0/CPU0:router# show running interface  gigabitEthernet0/0/0/9.800 inheritance
detail

interface GigabitEthernet0/0/0/9.250 l2transport
encapsulation dot1q250
## Inherited from group l2tr
mtu 1400
!
```

3. Verify that the correct values from the group do take effect:

```
RP/0/RP0/CPU0:router# show interface gigabitEthernet 0/0/0/30

GigabitEthernet0/0/0/30 is down, line protocol is down
  Interface state transitions: 0
  Hardware is GigabitEthernet, address is 0026.9824.ee56 (bia 0026.9824.ee56)
  Internet address is Unknown
  MTU 1500 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, link type is force-up
  output flow control is off, input flow control is off
  loopback not set,
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out

RP/0/RP0/CPU0:router# show interface gigabitEthernet 0/0/0/9.801

GigabitEthernet0/0/0/9.801 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 0026.9824.ee41
  Internet address is Unknown
  MTU 1400 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation 802.1Q Virtual LAN, VLAN Id 801,  loopback not set,
  Last input never, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 total input drops
```

```
     0 drops for unrecognized upper-level protocol
     Received 0 broadcast packets, 0 multicast packets
     0 packets output, 0 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets


RP/0/RP0/CPU0:router# show interface gigabitEthernet 0/0/0/9.250

GigabitEthernet0/0/0/9.250 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 0026.9824.ee41
  Layer 2 Transport Mode
  MTU 1400 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability Unknown, txload Unknown, rxload Unknown
  Encapsulation 802.1Q Virtual LAN,
    Outer Match: Dot1Q VLAN 250
    Ethertype Any, MAC Match src any, dest any
  loopback not set,
  Last input never, output never
  Last clearing of "show interface" counters never
     0 packets input, 0 bytes
     0 input drops, 0 queue drops, 0 input errors
     0 packets output, 0 bytes

     0 output drops, 0 queue drops, 0 output errors
```

ACL Referencing: Example

This example shows how to reference access-lists on a number of interfaces using configuration groups.

1. Configure the configuration group and apply-group:

```
RP/0/RP0/CPU0:router# show running group acref

group acref
 interface 'GigabitEthernet0/0/0/3.*'
  ipv4 access-group adem ingress
  ipv4 access-group adem egress
 !
end-group

RP/0/RP0/CPU0:router# show running | inc apply-group

Building configuration...

apply-group isis l2tr isis2 mpp bundle1 acref
```

2. Check the concise and inheritance view of the matching configurations:

```
RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/30

interface GigabitEthernet0/0/0/30
!

RP/0/RP0/CPU0:router# show running interface GigabitEthernet 0/0/0/30 inheritance detail
```

```
interface GigabitEthernet0/0/0/30
 ## Inherited from group l2tr
 mtu 1500
 ## Inherited from group acref
 ipv4 access-group adem ingress
 ## Inherited from group acref
 ipv4 access-group adem egress
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/31

interface GigabitEthernet0/0/0/31
!

RP/0/RP0/CPU0:router# show running interface GigabitEthernet 0/0/0/31 inheritance detail

interface GigabitEthernet0/0/0/31
 ## Inherited from group l2tr
 mtu 1500
 ## Inherited from group acref
 ipv4 access-group adem ingress
 ## Inherited from group acref
 ipv4 access-group adem egress
```

3. Check that the ACL group configuration actually got configured by using a traffic generator and watching that denied traffic is dropped.

Local Configuration Takes Precedence: Example

This example illustrates that local configurations take precedence when there is a discrepancy between a local configuration and the configuration inherited from a configuration group.

1. Configure a local configuration in a configuration submode with an access list:

```
RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/39

interface GigabitEthernet0/0/0/39
 ipv4 access-group smany ingress
 ipv4 access-group smany egress
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/38

interface GigabitEthernet0/0/0/38
!

RP/0/RP0/CPU0:router# show running ipv4 access-list smany

ipv4 access-list smany
 10 permit ipv4 any any
!

RP/0/RP0/CPU0:router# show running ipv4 access-list adem

ipv4 access-list adem
 10 permit ipv4 21.0.0.0 0.255.255.255 host 55.55.55.55
 20 deny ipv4 any any
!
```

2. Configure and apply the access list group configuration:

```
RP/0/RP0/CPU0:router# show running group acref

group acref
 interface 'GigabitEthernet0/0/0/3.*'
  ipv4 access-group adem ingress
  ipv4 access-group adem egress
 !
end-group

RP/0/RP0/CPU0:router# show running | inc apply-group

Building configuration...
apply-group isis l2tr isis2 mpp bundle1 acref
```

3. Check the concise and inheritance views for the matching interface where the access list reference is configured locally:

```
RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/39

interface GigabitEthernet0/0/0/39
 ipv4 access-group smany ingress
 ipv4 access-group smany egress
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/39 inheritance detail

interface GigabitEthernet0/0/0/39
 ## Inherited from group l2tr
 mtu 1500
 ipv4 access-group smany ingress
 ipv4 access-group smany egress     << no config inherited, local config prioritized
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/38

interface GigabitEthernet0/0/0/38
!

RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/0/0/38 inheritance detail

interface GigabitEthernet0/0/0/38
 ## Inherited from group l2tr
 mtu 1500
 ## Inherited from group acref
 ipv4 access-group adem ingress
 ## Inherited from group acref
 ipv4 access-group adem egress
!
```

4. Use a traffic generator to verify that the traffic pattern for interface GigabitEthernet0/0/0/39 gets acted on by the access list in the local configuration (smany) and not according to the inherited referenced access list (adem).

ISIS Hierarchical Configuration: Example

This example illustrates inheritance and priority handling with two ISIS groups using an ISIS configuration.

1. Configure the local ISIS configuration:

```
RP/0/RP0/CPU0:router# show running router isis

router isis vink
 net 49.0011.2222.2222.2222.00
 address-family ipv4 unicast
  mpls traffic-eng level-1-2
  mpls traffic-eng router-id Loopback0
  redistribute connected
 !
 interface Bundle-Ether1
  address-family ipv4 unicast
  !
 !
 interface Bundle-Ether2
 !
 interface Loopback0
 !
 interface TenGigE0/2/0/0.3521
  address-family ipv4 unicast
  !
 !
 interface TenGigE0/2/0/0.3522
  address-family ipv4 unicast
  !
 !
 interface TenGigE0/2/0/0.3523
  address-family ipv4 unicast
  !
 !
 interface TenGigE0/2/0/0.3524
  address-family ipv4 unicast
  !
 !
 interface TenGigE0/2/0/0.3525
  address-family ipv4 unicast
  !
 !
 interface TenGigE0/2/0/0.3526
 !
 interface TenGigE0/2/0/0.3527
 !
 interface TenGigE0/2/0/0.3528
 !
 interface TenGigE0/2/0/1
  address-family ipv4 unicast
  !
 !
!
```

2. Configure two ISIS groups and apply these to the configuration:

```
RP/0/RP0/CPU0:router# show running group isis
```

```
group isis
 router isis '.*'
  address-family ipv4 unicast
   mpls traffic-eng level-1-2
   mpls traffic-eng router-id Loopback0
   redistribute connected
   redistribute ospf 1 level-1-2
  !
  interface 'TenGig.*'
   lsp-interval 40
   hello-interval 15
   address-family ipv4 unicast
    metric 50
   !
  !
  interface 'Bundle-Ether.*'
   address-family ipv4 unicast
    metric 55
   !
  !
 !
end-group

RP/0/RP0/CPU0:router# show running group isis2

group isis2
 router isis '.*'
 !
 router isis '^(vink)'
  address-family ipv4 unicast
  !
  interface '(^Ten)Gig.*'
  !
  interface '^(Ten)Gig.*'
   address-family ipv4 unicast
    metric 66
   !
  !
 !
end-group

RP/0/RP0/CPU0:router# show running | inc apply-group

Building configuration...

apply-group isis  l2tr  isis2  mpp  bundle1  acref
```

3. Check the inheritance view of the ISIS configuration:

```
RP/0/RP0/CPU0:router# show running router isis inheritance detail

router isis vink
 net 49.0011.2222.2222.2222.00
 address-family ipv4 unicast
  mpls traffic-eng level-1-2
  mpls traffic-eng router-id Loopback0
  redistribute connected
  ## Inherited from group isis
  redistribute ospf 1 level-1-2
 !
 interface Bundle-Ether1
  address-family ipv4 unicast
```

```
  ## Inherited from group isis
  metric 55
 !
!
interface Bundle-Ether2
 ## Inherited from group isis
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 55
 !
!
interface Loopback0
!
interface TenGigE0/2/0/0.3521
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3522
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3523
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3524
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3525
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3526
```

```
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 ## Inherited from group isis
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3527
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 ## Inherited from group isis
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/0.3528
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 ## Inherited from group isis
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
interface TenGigE0/2/0/1
 ## Inherited from group isis
 lsp-interval 40
 ## Inherited from group isis
 hello-interval 15
 address-family ipv4 unicast
  ## Inherited from group isis
  metric 50
 !
!
!
```

4. Verify the actual functionality:

```
RP/0/RP0/CPU0:router# show isis interface TenGigE0/2/0/0.3528 | inc Metric

Metric (L1/L2):         50/50
```

OSPF Hierarchy: Example

This example illustrates hierarchical inheritance and priority. The configuration that is lower in hierarchy gets the highest priority.

1. Configure a local OSPF configuration:

```
RP/0/RP0/CPU0:router# show running router ospf
```

```
router ospf 1
 apply-group go-c
 nsr
 router-id 121.121.121.121
 nsf cisco
 redistribute connected
 address-family ipv4 unicast
 area 0
  apply-group go-b
  interface GigabitEthernet0/0/0/0
   apply-group go-a
  !
  interface GigabitEthernet0/0/0/1
  !
  interface GigabitEthernet0/0/0/3
  !
  interface GigabitEthernet0/0/0/4
  !
  interface GigabitEthernet0/0/0/21
   bfd minimum-interval 100
   bfd fast-detect
   bfd multiplier 3
  !
  interface TenGigE0/2/0/0.3891
  !
  interface TenGigE0/2/0/0.3892
  !
  interface TenGigE0/2/0/0.3893
  !
  interface TenGigE0/2/0/0.3894
  !
 !
!
router ospf 100
!
router ospf 1000
!
router ospf 1001
!
```

2. Configure a configuration group and apply it in a configuration submode:

```
RP/0/RP0/CPU0:router# show running group go-a

group go-a
 router ospf '.*'
  area '.*'
   interface 'Gig.*'
    cost 200
   !
  !
 !
end-group

RP/0/RP0/CPU0:router# show running group go-b

group go-b
 router ospf '.*'
  area '.*'
   interface 'Gig.*'
    cost 250
   !
```

```
  !
 !
end-group

RP/0/RP0/CPU0:router# show running group go-c

group go-c
 router ospf '.*'
  area '.*'
   interface 'Gig.*'
    cost 300
   !
  !
 !

end-group
```

3. Check the inheritance view and verify that the apply-group in the lowest configuration submode gets the highest priority:

```
RP/0/RP0/CPU0:router# show running router ospf 1 inheritance detail

router ospf 1
 nsr
 router-id 121.121.121.121
 nsf cisco
 redistribute connected
 address-family ipv4 unicast
 area 0
  interface GigabitEthernet0/0/0/0
   ## Inherited from group go-a
   cost 200                    << apply-group in lowest submode  gets highest priority

  !
  interface GigabitEthernet0/0/0/1
   ## Inherited from group go-b
   cost 250
  !
  interface GigabitEthernet0/0/0/3
   ## Inherited from group go-b
   cost 250
  !
  interface GigabitEthernet0/0/0/4
   ## Inherited from group go-b
   cost 250
  !
  interface GigabitEthernet0/0/0/21
   bfd minimum-interval 100
   bfd fast-detect
   bfd multiplier 3
   ## Inherited from group go-b
   cost 250
  !
  interface TenGigE0/2/0/0.3891
  !
  interface TenGigE0/2/0/0.3892
  !
  interface TenGigE0/2/0/0.3893
  !
  interface TenGigE0/2/0/0.3894
  !
 !
!
```

4. Check the functionality of the cost inheritance through the groups:

```
RP/0/RP0/CPU0:router# show ospf 1 interface GigabitEthernet 0/0/0/0

GigabitEthernet0/0/0/0 is up, line protocol is up
  Internet Address 1.0.1.1/30, Area 0
  Process ID 1, Router ID 121.121.121.121, Network Type BROADCAST, Cost: 200
  Transmit Delay is 1 sec, State DR, Priority 1, MTU 1500, MaxPktSz 1500
  Designated Router (ID) 121.121.121.121, Interface address 1.0.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Non-Stop Forwarding (NSF) enabled
    Hello due in 00:00:02
  Index 5/5, flood queue length 0
  Next 0(0)/0(0)
  Last flood scan length is 1, maximum is 40
  Last flood scan time is 0 msec, maximum is 7 msec
  LS Ack List: current length 0, high water mark 0
  Neighbor Count is 1, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 0
```

Link Bundling Usage: Example

This example shows how to configure interface membership in a bundle link:

1. Configure the configuration groups:

```
RP/0/RP0/CPU0:router# show running group bundle1

group bundle1
 interface 'GigabitEthernet0/1/0/1[1-6]'
  bundle id 1 mode active
 !
end-group

RP/0/RP0/CPU0:router# show running | inc apply-group

Building configuration...

apply-group isis l2tr  isis2  mpp  bundle1
```

2. Check the local configuration:

```
RP/0/RP0/CPU0:router# show running interface gigabitEthernet 0/1/0/11

interface GigabitEthernet0/1/0/11
!

RP/0/RP0/CPU0:router# show running interface Bundle-Ether1

interface Bundle-Ether1
 ipv4 address 108.108.1.1 255.255.255.0
 bundle maximum-active links 10
 bundle minimum-active links 5
```

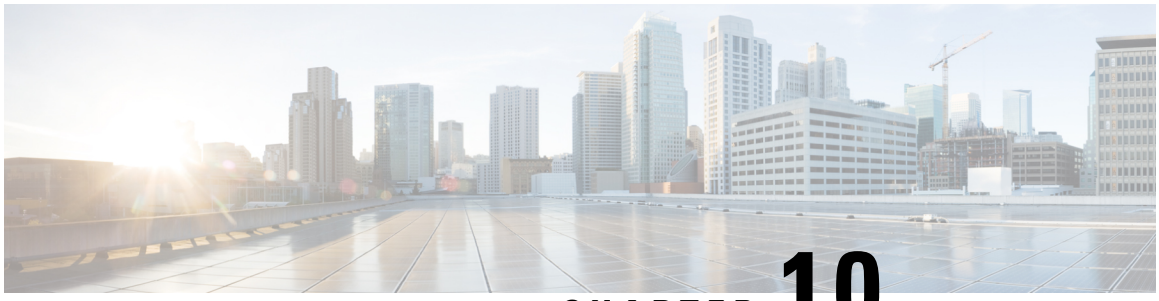
```
!
```

3. Check the inheritance configuration view:

```
RP/0/RP0/CPU0:router# show running interface GigabitEthernet 0/1/0/11  inheritance detail

interface GigabitEthernet0/1/0/11
 ## Inherited from group bundle1
 bundle id 1 mode active
!
```

4. Check that the inheritance configuration took effect:

```
RP/0/RP0/CPU0:router# show interface Bundle-Ether1

Bundle-Ether1 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Aggregated Ethernet interface(s), address is 0024.f71f.4bc3
  Internet address is 108.108.1.1/24
  MTU 1514 bytes, BW 6000000 Kbit (Max: 6000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 6000Mb/s
  loopback not set,
  ARP type ARPA, ARP timeout 04:00:00
    No. of members in this bundle: 6
      GigabitEthernet0/1/0/11      Full-duplex  1000Mb/s     Active
      GigabitEthernet0/1/0/12      Full-duplex  1000Mb/s     Active
      GigabitEthernet0/1/0/13      Full-duplex  1000Mb/s     Active
      GigabitEthernet0/1/0/14      Full-duplex  1000Mb/s     Active
      GigabitEthernet0/1/0/15      Full-duplex  1000Mb/s     Active
      GigabitEthernet0/1/0/16      Full-duplex  1000Mb/s     Active
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 8000 bits/sec, 1 packets/sec
  5 minute output rate 3000 bits/sec, 1 packets/sec
     2058 packets input, 1999803 bytes, 426 total input drops
     0 drops for unrecognized upper-level protocol
     Received 1 broadcast packets, 2057 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1204 packets output, 717972 bytes, 0 total output drops
     Output 2 broadcast packets, 1202 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```



CHAPTER 10

Configuring Network Time Protocol

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

- Prerequisites for Implementing NTP on Cisco IOS XR Software, on page 119
- Best Practices for NTP configuration , on page 119
- Information About Implementing NTP, on page 120
- Configuration Examples for Implementing NTP, on page 140
- Configuring NTP server inside VRF interface, on page 143

Prerequisites for Implementing NTP on Cisco IOS XR Software

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Best Practices for NTP configuration

Follow these best practices when configuring NTP :

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

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

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

Information About Implementing NTP

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

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

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

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

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

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

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

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

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

- By polling host servers
- By listening to NTP broadcasts
- By listening to NTP multicasts
- By using a peer-to-peer relationship.

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

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

An NTP multicast server periodically sends a message to a designated IPv4 or IPv6 local multicast group address. An NTP multicast client listens on this address for NTP messages.

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

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

Preventing Issues due to GPS Week Number Rollover (WNRO)

- If there are no GPS sources in the NTP source chain or server chain, there is no impact of GPS Week Number Rollover (WNRO).
- GPS WNRO affects only the system clock and not user traffic.
- Contact your GPS manufacturer to fix the GPS source for this condition.

To mitigate impact of GPS sources that are subject to GPS WNRO perform the following optional workarounds:

- If the GPS source has been identified to be a cause of potential disruption on April 6, 2019 (or after), configure ntp master in the Cisco that is device connected to this source, and its clock on the Stratum 1 device to preventively isolate it. This configuration enables the device to present its own clock for synchronization to downstream NTP clients.

Note The usage of ntp master command as mentioned above is only a workaround to this condition. Use this command until the GPS source-related conditions are resolved, and to prevent the distribution of incorrect clock values throughout the network.

- Configure multiple NTP servers (ideally 4, but more than 3) at Stratum 2 level of the network, to enable NTP clients at Stratum 2 level to get clock from more than one Stratum 1 server. This way, WNRO affected Stratum 1 servers are staged to be marked as ‘false ticker’ or ‘outlier’ clock sources as compared to other non-WNRO affected Stratum 1 servers.

Note To configure day light saving time (DST) on your IOS XR 64-bit device, select the appropriate country and city. The device will automatically update the DST based on the internal mappings at kernel level. The *DST* keyword is not available in the configuration CLI, since manual configuration of DST is not supported on IOS XR 64-bit devices.

PTP-NTP Interworking

Table 6: Feature History Table

Feature Name	Release Information	Feature Description
PTP-NTP Interworking	Release 24.1.1	Introduced in this release on:NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) We have improved NTP synchronization and reliability to achieve nanosecond-level accuracy for applications that require high-precision timing. This is achieved by enabling NTP-PTP interworking which allows the use of PTP as the reference clock. As in previous releases, the NTP client continues to support polling NTP protocol-based external time servers to synchronize the local system clock and achieve accuracy within the millisecond range.

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

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

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

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

Enable PTP-NTP Interworking

Prerequisites for PTP-NTP Interworking

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

Configuration Example for PTP-NTP Interworking

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

- Setting NTP Primary Reference Clock as PTP

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

- Configuring NTP Server with IP address

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

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

Verification

```
Router#show ntp status

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

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

Configuring Poll-Based Associations

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

You can configure the following types of poll-based associations between the router and other devices (which may also be routers):

- 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 then picks a host from all the polled time servers to synchronize with. Because the relationship that is established in this case is a client-host relationship, the host does 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 **server** 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 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 also retains time-related information about the local networking device that it is communicating with. This mode should be used when there are several mutually redundant servers that are interconnected via diverse network paths. Most stratum 1 and stratum 2 servers on the Internet today adopt this form of network setup. Use the **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.

When the router polls several other devices for the time, the router selects one device with which to synchronize.

Note To configure a peer-to-peer association between the router and another device, you must also configure the router as a peer on the other device.

You can configure multiple peers and servers, but you cannot configure a single IP address as both a peer and a server at the same time.

To change the configuration of a specific IP address from peer to server or from server to peer, use the **no** form of the **peer** or **server** command to remove the current configuration before you perform the new configuration. If you do not remove the old configuration before performing the new configuration, the new configuration does not overwrite the old configuration.

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **server** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**source** *type interface-path-id*] [**prefer**] [**burst**] [**iburst**]
4. **peer** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**source** *type interface-path-id*] [**prefer**]
5. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**server** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**source** *type interface-path-id*] [**prefer**] [**burst**] [**iburst**] **Example:** `RP/0/RP0/CPU0:router(config-ntp)# server 172.16.22.44`	Forms a server association with another system. This step can be repeated as necessary to form associations with multiple devices.

Step 4	**peer** *ip-address* [**vrf** *vrf*] [**version** *number*] [**key** *key-id*] [**minpoll** *interval*] [**maxpoll** *interval*] [**source** *type interface-path-id*] [**prefer**]
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# peer 192.168.22.33`
	`source tengige 0/0/0/1`
		Forms a peer association with another system. This step can be repeated as necessary to form associations with multiple systems.
		Note
		To complete the configuration of a peer-to-peer association between the router and the remote device, the router must also be configured as a peer on the remote device.

Step 5	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Broadcast-Based NTP Associates

In a broadcast-based NTP association, an NTP server propagates NTP broadcast packets throughout a network. Broadcast clients listen for the NTP broadcast packets propagated by the NTP server and do not engage in any polling.

Broadcast-based NTP associations should be used when time accuracy and reliability requirements are modest and if your network is localized and has a large number of clients (more than 20). Broadcast-based NTP associations also are recommended for use on networks that have limited bandwidth, system memory, or CPU resources. Time accuracy is marginally reduced in broadcast-based NTP associations because information flows only one way.

Use the **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. The time server that is transmitting NTP broadcast packets must be enabled on the interface of the given device using the **broadcast** command.

Use the **broadcast** command to set your networking device to send NTP broadcast packets.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. (Optional) **broadcastdelay** *microseconds*
4. **interface** *type interface-path-id*
5. **broadcast client**
6. **broadcast** [**destination** *ip-address*] [**key** *key-id*] [**version** *number*]
7. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:**	Enters NTP configuration mode.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(config)# ntp`	
Step 3	(Optional) **broadcastdelay** *microseconds* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# broadcastdelay 5000`	Adjusts the estimated round-trip delay for NTP broadcasts.
Step 4	**interface** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# interface POS 0/1/0/0`	Enters NTP interface configuration mode.
Step 5	**broadcast client** **Example:** `RP/0/RP0/CPU0:router(config-ntp-int)# broadcast client`	Configures the specified interface to receive NTP broadcast packets. **Note** Go to the next step to configure the interface to send NTP broadcast packets.
Step 6	**broadcast** [**destination** *ip-address*] [**key** *key-id*] [**version** *number*] **Example:** `RP/0/RP0/CPU0:router(config-ntp-int)# broadcast destination 10.50.32.149`	Configures the specified interface to send NTP broadcast packets. **Note** Go to previous step to configure the interface to receive NTP broadcast packets.

Step 7	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp-int)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp-int)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

	Command or Action	Purpose
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring NTP Access Groups

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

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. NTP communication consists of time requests and control queries. A *time request* is a request for time synchronization from an NTP server. A *control query* is a request for configuration information from an NTP server.

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

1. **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.
2. **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.
3. **serve-only**—Allows only time requests from a system whose address passes the access list criteria.
4. **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. If no access groups are specified, all access types are granted to all systems. If any access groups are specified, only the specified access types are granted.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **access-group** {**peer** | **query-only** | **serve** | **serve-only**} *access-list-name*
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**access-group** {**peer** | **query-only** | **serve** | **serve-only**} *access-list-name* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# access-group peer access1`	Creates an access group and applies a basic IPv4 or IPv6 access list to it.

Step 4	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring NTP Authentication

This task explains how to configure NTP authentication.

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

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 it carries along is accepted.

The authentication process begins from the moment an NTP packet is created. A message authentication code (MAC) is computed using the MD5 Message Digest Algorithm and the MAC is embedded into an NTP synchronization packet. The NTP synchronization packet together with the embedded MAC and key number are transmitted to the receiving client. If authentication is enabled and the key is trusted, the receiving client computes the MAC in the same way. If the computed MAC matches the embedded MAC, the system is allowed to sync to the server that uses this key in its packets.

After NTP authentication is properly configured, your networking device only synchronizes with and provides synchronization to trusted time sources.

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **authenticate**
4. **authentication-key** *key-number* **md5** [**clear** | **encrypted**] *key-name*
5. **trusted-key** *key-number*
6. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:**	Enters NTP configuration mode.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(config)# ntp`	
Step 3	**authenticate** **Example:** `RP/0/RP0/CPU0:router(config-ntp)# authenticate`	Enables the NTP authentication feature.

Step 4	**authentication-key** *key-number* **md5** [**clear** | **encrypted**] *key-name*
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# authentication-key 42 md5 clear key1`
		Defines the authentication keys.
		• Each key has a key number, a type, a value, and, optionally, a name. Starting from Cisco IOS-XR Release 7.5.1 the following authentication types are supported:
		  • cmac CMAC authentication
		  • md5 MD5 authentication
		  • sha1 SHA1 authentication
		  • sha2 SHA2 authentication

Step 5	**trusted-key** *key-number* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# trusted-key 42`	Defines trusted authentication keys. • If a key is trusted, this router only synchronizes to a system that uses this key in its NTP packets.

Step 6	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		  • Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		  • Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		  • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Disabling NTP Services on a Specific Interface

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 turning off NTP on a given interface.

SUMMARY STEPS

1. **configure**
2. **ntp**
3. Use one of the following commands:
   - **no interface** *type interface-path-id*
   - **interface** *type interface-path-id* **disable**
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.

Step 3	Use one of the following commands:
	• **no interface** *type interface-path-id*
	• **interface** *type interface-path-id* **disable**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# no interface pos 0/0/0/1`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# interface POS 0/0/0/1 disable`
		Disables NTP services on the specified interface.

Step 4	Use one of the following commands:	Saves configuration changes.

	Command or Action	Purpose

	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring the Source IP Address for NTP Packets

By default, the source IP address of an NTP packet sent by the router is the address of the interface through which the NTP packet is sent. Use this procedure to set a different source address.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **source** *type interface-path-id*
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**source** *type interface-path-id* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# source POS 0/0/0/1`	Configures an interface from which the IP source address is taken. **Note** This interface is 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 **peer** or **server** command shown in Configuring Poll-Based Associations, on page 123.

Step 4	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring the System as an Authoritative NTP Server

You can configure the router to act as an authoritative NTP server, even if the system is not synchronized to an outside time source.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **master** *stratum*
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**master** *stratum* **Example:** `RP/0/RP0/CPU0:router(config-ntp)# master 9`	`Makes the router an authoritative NTP server.` **Note** Use the **master** 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 **master** command can cause instability in time keeping if the machines do not agree on the time.
Step 4	Use one of the following commands: • **end** • **commit**	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes:

	Command or Action	Purpose

	Example:
	
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	
	or
	
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

FQDN for NTP Server

NTP on Cisco IOS XR Software supports configuration of servers and peers using their Fully Qualified Domain Names (FQDN). While configuring, the FQDN is resolved via DNS into its corresponding IPv4 or IPv6 address and is stored in the running-configuration of the system. NTP supports FQDN for both IPv4 and IPv6 protocols. You can configure FQDN on default vrf.

Configure FQDN for NTP server

Configuration Example for FQDN on NTP Server on Default VRF

Use the **ntp server** command with the FQDN name to configure FQDN on default VRF. You dont need to specify VRF name. In the following example, time.cisco.com is the FQDN.

```
Router#configure
Router(config)#ntp server time.cisco.com
Router(config)#commit
```

Note When you are configuring FQDN over default VRF, you don't need to specify VRF name.

Running Configuration

Use the **show running-config ntp** command to see the ntp running configuration.

```
Router#show running-config ntp
ntp
 server 10.48.59.212
!
```

Verification

Use the **show ntp associations** command to verify that an NTP association has come up.

```
Router#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
 ~10.48.59.212     173.38.201.67     2    42   128     3  196.06  -14.25  3949.4
 * sys_peer, # selected, + candidate, - outlayer, x falseticker, ~ configured
```

Updating the Hardware Clock

On devices that have hardware clocks (system calendars), you can configure the hardware clock to be periodically updated from the software clock. This is advisable for devices using NTP, because the time and date on the software clock (set using NTP) is more accurate than the hardware clock. The time setting on the hardware clock has the potential to drift slightly over time.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **update-calendar**
4. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**update-calendar** **Example:** `RP/0/RP0/CPU0:router(config-ntp)# update-calendar`	Configures the router t o update its system calendar from the software clock at periodic intervals.

	Command or Action	Purpose

Step 4	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Verifying the Status of the External Reference Clock

This task explains how to verify the status of NTP components.

Note The commands can be entered in any order.

SUMMARY STEPS

1. **show ntp associations** [**detail**] [**location** *node-id*]
2. **show ntp status** [**location** *node-id*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show ntp associations** [**detail**] [**location** *node-id*] **Example:** `RP/0/RP0/CPU0:router# show ntp associations`	Displays the status of NTP associations.

	Command or Action	Purpose
Step 2	**show ntp status** [**location** *node-id*] **Example:** `RP/0/RP0/CPU0:router# show ntp status`	Displays the status of NTP.

Examples

The following is sample output from the **show ntp associations** command:

```
RP/0/RP0/CPU0:router# show ntp associations

Tue Oct  7 11:22:46.839 JST

      address         ref clock     st  when  poll reach  delay  offset    disp
*~192.168.128.5    10.81.254.131     2     1    64  377    7.98  -0.560   0.108
+~dead:beef::2 vrf testAA
                   171.68.10.80      3    20    64  377    6.00  -2.832   0.046
* sys_peer, # selected, + candidate, - outlayer, x falseticker, ~ configured


RP/0/RP0/CPU0:router# show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
+~127.127.1.1      127.127.1.1       5     5  1024   37     0.0    0.00   438.3
*~172.19.69.1      172.24.114.33     3    13  1024    1     2.0   67.16     0.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

The following is sample output from the **show ntp status** command:

```
RP/0/RP0/CPU0:router# show ntp status

Tue Oct  7 11:22:54.023 JST

Clock is synchronized, stratum 3, reference is 192.168.128.5
nominal freq is 1000.0000 Hz, actual freq is 1000.2725 Hz, precision is 2**24
reference time is CC95463C.9B964367 (11:21:48.607 JST Tue Oct  7 2008)
clock offset is -1.738 msec, root delay is 186.050 msec
root dispersion is 53.86 msec, peer dispersion is 0.09 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.0002724105 s/s
system poll interval is 64, last update was 66 sec ago


RP/0/RP0/CPU0:router# show ntp status

Clock is synchronized, stratum 4, reference is 172.19.69.1
nominal freq is 1000.0000 Hz, actual freq is 999.9988 Hz, precision is 2**26
reference time is C54C131B.9EECF6CA (07:26:19.620 UTC Mon Nov 24 2008)
clock offset is 66.3685 msec, root delay is 7.80 msec
root dispersion is 950.04 msec, peer dispersion is 3.38 msec
```

Configuration Examples for Implementing NTP

Configuring Poll-Based Associations: Example

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

```
ntp
  server 10.0.2.1
  peer 192.168.22.33

  server 172.19.69.1
```

Configuring Broadcast-Based Associations: Example

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

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

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

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

Configuring Multicast-Based Associations: Example

The following example shows an NTP multicast client configuration where 10-Gigabit Ethernet interface 0/1/1/0 is configured to be a multicast client and to join the default multicast group (IPv4 address 224.0.1.1):

```
ntp interface TenGigE 0/1/1/0
  multicast client
```

The following example shows an NTP multicast server configuration where 10-Gigabit Ethernet interface 0/1/1/0 is configured to be a multicast server:

```
ntp interface TenGigE 0/1/1/0
```

```
  multicast destination 224.0.1.1
```

Configuring NTP Access Groups: Example

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

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

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

Configuring NTP Authentication: Example

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

- NTP authentication is enabled.

- Two authentication keys are configured (key 2 and key 3).
- The router is configured to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 10.3.32.154 using authentication key 2.
- The router is configured to allow its software clock to be synchronized with the clock by the device at IP address 10.32.154.145 using authentication key 3.
- The router is configured to synchronize only to systems providing authentication key 3 in their NTP packets.

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

Disabling NTP on an Interface: Example

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

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

Configuring the Source IP Address for NTP Packets: Example

The following example shows an NTP configuration in which Ethernet management interface 0/0/CPU0/0 is configured as the source address for NTP packets:

```
ntp
  authentication-key 2 md5 encrypted 06120A2D40031D1008124
  authentication-key 3 md5 encrypted 1311121E074110232621
  authenticate
  trusted-key 3
  server 10.3.32.154 key 3
  peer 10.32.154.145 key 2
  source MgmtEth0/0/CPU0/0
```

Configuring the System as an Authoritative NTP Server: Example

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

```
ntp
  master 6
```

Updating the Hardware Clock: Example

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

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

Configuring NTP server inside VRF interface

This task explains how to configure NTP server inside VRF interface.

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

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **vrf** *vrf-name*
4. **source** *interface-type interface-instance*
5. Use one of the following commands:
   - **end**
   - **commit**

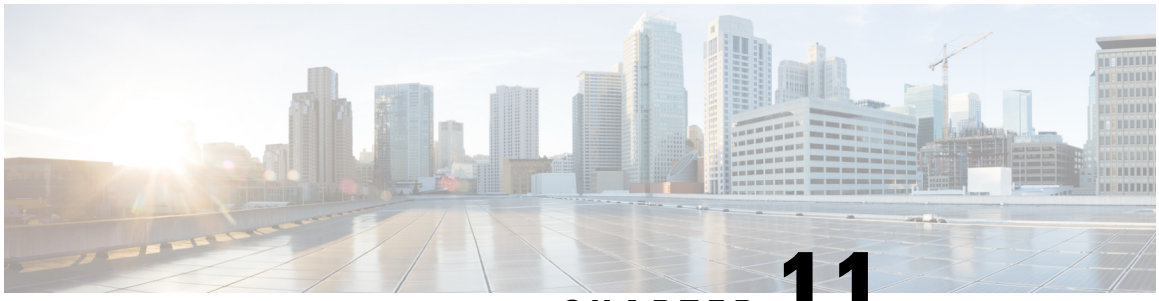
DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router# configure`	
Step 2	**ntp** **Example:** `RP/0/RP0/CPU0:router(config)# ntp`	Enters NTP configuration mode.
Step 3	**vrf** *vrf-name* **Example:** `RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A`	Specify name of a VRF (VPN- routing and forwarding) instance to configure.
Step 4	**source** *interface-type interface-instance* **Example:** `RP/0/RP0/CPU0:router(config)# ntp vrf Customer_A source bvi 70`	Configures an interface from which the IP source address is taken. This allows IOS-XR to respond to NTP queries on VRF interfaces, in this case the source is BVI. **Note** This interface is 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 **peer** or **server** command shown in Configuring Poll-Based Associations, on page 123.

Step 5	Use one of the following commands:
	• **end**
	• **commit**
	Example:
	`RP/0/RP0/CPU0:router(config-ntp)# end`
	or
	`RP/0/RP0/CPU0:router(config-ntp)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.



CHAPTER 11

Configuring Precision Time Protocol

Precision Time Protocol (PTP) is a protocol that defines a method to distribute time around a network. PTP support is based on the IEEE 1588-2008 standard. This module describes the concepts around this protocol and details the various configurations involved.

This module contains the following topics:

- PTP Overview, on page 145
- ITU-T Telecom Profiles for PTP, on page 158
- Configure PTP , on page 162
- IEEE Default Profile , on page 174
- Performance Monitoring for PTP Networks, on page 176
- Configuration Examples, on page 181

PTP Overview

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 are organized into a master-slave hierarchy. PTP identifies the port that is connected to a device with the most precise clock. This clock is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as members. Constantly exchanged timing messages ensure continued synchronization. PTP ensures that the best available clock is selected as the source of time (the grandmaster clock) for the network and that other clocks in the network are synchronized to the grandmaster.

Table 7: PTP Clocks

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

Network Element	Description
Ordinary Clock (OC)	An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes: • Master mode—Distributes timing information over the network to one or more slave clocks, thus allowing the slave to synchronize its clock to the master. • Slave mode—Synchronizes its clock to a master clock. You can enable the slave mode on up to two interfaces simultaneously in order to connect to two different master clocks.
Boundary Clock (BC)	The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected. Boundary clock starts its own PTP session with a number of downstream slaves. The boundary clock mitigates the number of network hops and packet delay variations in the packet network between the Grand Master and Slave.
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.

PTP consists of two parts:

- The port State machine and Best Master Clock Algorithm: This provides a method to determine state of the ports in the network that will remain passive (neither master nor slave), run as a master (providing time to other clocks in the network), or run as slaves (receiving time from other clocks in the network).
- Delay-Request/Response mechanism and a Peer-delay mechanism: This provides a mechanisms for slave ports to calculate the difference between the time of their own clocks and the time of their master clock.

Note Transparent Clock (TC) is not supported.

Frequency and Time Selection

The selection of the source to synchronize the device clock frequency is made by frequency synchronization, and is outside of the scope of PTP. The Announce, Sync, and Delay-request frequencies must be the same on the master and slave.

Delay-Response Mechanism

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

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

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

Hybrid Mode

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

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

The steps involved in configuring PTP hybrid mode is described in a subsequent section in this chapter.

Time of Day (ToD) Support

The router receives GPS ToD messages in serial ASCII stream through the RS422 interface in any of the following formats:

- NTP Type 4
- Cisco
- NMEA - GPZDA

Note You can refer to the below support information in context of the current release and see relevant *Release Notes* for more information on supported features and hardware.

Port States

State machine indicates the behavior of each port. The possible states are:

State	Description
INIT	Port is not ready to participate in PTP.

State	Description
LISTENING	First state when a port becomes ready to participate in PTP: In this state, the port listens to PTP masters for a (configurable) period of time.
PRE-MASTER	Port is ready to enter the MASTER state.
MASTER	Port provides timestamps for any Slave or boundary clocks that are listening.
UNCALIBRATED	Port receives timestamps from a Master clock but, the router's clock is not yet synchronized to the Master.
SLAVE	Port receives timestamps from a Master clock and the router's clock is synchronized to the Master.
PASSIVE	Port is aware of a better clock than the one it would advertise if it was in MASTER state and is not a Slave clock to that Master clock.

Restrictions for PTP

The following PTP restrictions apply to the Cisco NCS 5500 Series Router:

- NCS55-RP does not support PTP
- NC55-18H18F line card does not support PTP
- SyncE is not supported on a 1GE copper SFP.
- SyncE is not supported on 25 GE or 100 GE interfaces when they are used in 1G mode.
- Sync2 interface is supported only if 10 MHz, 1 Pulse per Second (PPS) and time-of-day (ToD) ports are configured.
- PTP is not supported with MACSec.
- G.8273.2 Class-A performance is met if CFP2-DCO is configured on either Slave or Master port on the node.
- Transparent Clock is not supported.
- PTP over MPLS is not supported.

Note

- We recommend you to configure, and enable Frequency Synchronization selection input on two interfaces per line card.
- For link aggregation, you must configure and enable Frequency Synchronization selection input on a single bundle member.

PTP Support Information

This table lists different types of support information related to PTP:

Transport Media	• UDP over IPv4 • Ethernet
Messages	• Signaling • Announce • Sync • Follow-up • Delay-request • Delay-response • Management
Transport Modes	• Unicast: This is the default mode. All packets are sent as unicast messages. Unicast is applicable only for PTP over IP profiles. • Multicast: All packets are sent as multicast messages. Multicast is the only mode for PTP over ethernet profiles.

PTP Hardware Support

Note The table also contains support details of upcoming releases. You can read this table in context of the current release and see relevant *Release Notes* for more information on supported features and hardware.

This table provides a detailed information on the timing features that are supported on the following hardware variants.

Hardware Variant	Features	Cisco IOS XR Release	Comments	
RP:NC57-MOD-RP2-E-HX with NCS-57C3-MOD-HX	G.8265.1	Release 25.4.1		
	G.8273.2	Release 25.4.1	Class C supported on ports numbered from 8-47. Class B supported on ports numbered from 0-7 and 48-55.	
	NCS-57B1-6D24-SYS NCS-57B1-5DSE-SYS NCS-57D2-18DD-SYS	Default profile	Release 7.11.1	With this release, PTP Class C performance and QSFP-DD optics are now supported on 400G port speed.
		G.8265.1		
		G.8275.1		
		G.8275.2		
NC57-48Q2D-S NC57-48Q2D-SE-S	G8275.1	Release 7.10.1	With this release, SyncE and PTP Class-C, Class-B performance is supported on 1G, 10G, 25G, 40G and 100G port speeds. On 50G and 400G ports speeds, only timing functionality is supported. PTP support is available on compatible mode. PTP with Class-C is not achieved with macsec on any interface speed. **Note** For 1G Class C port speed, only port 32 and 40 are supported. It is not recommended to plug in 1G optics to ports greater than or equal to port 32.	

Hardware Variant	Features	Cisco IOS XR Release	Comments
NC57-36H6D-S	G8265.1 G8275.1 G8275.2 Default Profile	Release 7.10.1	With this release, timing support for PTP and SyncE is extended to 4x10G and 4x25G breakout ports of NC57-36H6D-S in native mode. Class B and Class C performances are supported on 4x10G and 4x25G breakout ports in native mode. Route Processor: NC55-RP2-E
NC57-36H-SE	G8265.1 G8275.1 G8275.2 Default Profile	Release 7.10.1	With this release, timing support for PTP and SyncE is extended to 4x10G breakout port of NC57-36H-SE is in native mode. Class B performance is supported on 4x10G breakout port in native mode. Route Processor: NC55-RP2-E
NCS-57C1-48Q6-SYS	G.8265.1 G.8275.1 G.8275.2 Default Profile	Release 7.10.1	G.8273.2 Class C is supported on 400G interfaces with the following optics modules: • Cisco QSFPDD 400G FR4 Pluggable Optics Module • Cisco QSFPDD 400G LR4 Pluggable Optics Module

Hardware Variant	Features	Cisco IOS XR Release	Comments
NCS-57D2-18DD-SYS	G.8265.1	Release 7.8.1	With this release,PTP is supported on 400G, 100G and 40G ports. Class C performance on 100G and 40G ports.
	G.8275.1	Release 7.8.1	
	G.8275.2	Release 7.8.1	
	Default Profile	Release 7.8.1	
NCS-57C3-MOD-SYS NCS-57C3-MODS-SYS	Timing support for PTP and SyncE over Breakout port	Release 24.3.1	With this release, the timing support for PTP and SyncE is extended to 4x10G and 4x25G breakout ports in NCS-57C3-MOD and NCS-57C3-MODS-SYS routers with 8 fixed port number 24 to 31 and 4x10G. Class A and Class B performances are supported on 4x10G and 4x25G breakout ports of NCS-57C3-MOD and NCS-57C3-MODS-SYS routers.
NCS-57C3-MOD-SYS NCS-57C3-MODS-SYS	PTP Virtual Port and APTS	Release 7.7.1	
C57-MPA-2D4H-S	Timing support for PTP and SyncE over Breakout port	Release 24.3.1	With this release, the timing support for PTP and SyncE is extended to 4x25G breakout ports in NC57-MPA-2D4H-S router. Class A and Class B performances are supported on 4x25G breakout ports of NC57-MPA-2D4H-S router.
NCS-57B1-6D24-SYS	PTP Virtual Port and APTS	Release 7.7.1	

Hardware Variant	Features	Cisco IOS XR Release	Comments
NCS-57C1-48Q6-SYS	Default profile	Release 7.5.1	
	G.8265.1	Release 7.5.1	
	G.8275.1	Release 7.5.1	
	G.8275.2	Release 7.5.1	
RP:NC57-MOD-RP-2E with NCS573-MODS-SYS and NCS-573-MOD-SYS	G.8275.1	Release 7.4.1	
	G.8273.2	Release 7.4.1	
	GNSS	Release 7.4.1	
NCS-57B1-5DSE-SYS NCS-57B1-6D24-SYS	Default profile	Release 7.3.1	
	G.8265.1	Release 7.3.1	
	G.8275.1	Release 7.3.1	
	G.8275.2	Release 7.3.1	
RP: NC55-RP2-E Line card: NC57-36H6D-S	G.8275.1	Release 7.3.2	• Release 7.3.2 - Supports Compatible Mode only • Release 7.7.1 - Supports both Native and Compatible mode.
	G.8273.2	Release 7.3.2	• Release 7.3.2 - Supports Compatible Mode only • Release 7.7.1 - Supports both Native and Compatible mode.

Hardware Variant	Features	Cisco IOS XR Release	Comments
RP:NC55-RP-E with Line cards: NC55-MOD-A-S and NC55-32T16Q4H-AT	BITS	Release 7.1.1	
	G8275.1	Release 7.1.1	For the profile G8275.1 NC55-32T16Q4H-AT supports only T-BCand does not support T-GM. 25G/100G/40G is supported from IOSXR release 7.2.2 onwards.
	G8273.2	Release 7.1.1	Class B
RP:NC55-RP2-E with Line cards: NC55-MOD-A-S and NC55-32T16Q4H-AT	BITS	Release 7.1.1	
	G.8275.1	Release 7.1.1	For the profile G8275.1 NC55-32T16Q4H-AT supports only T-BC and does not support T-GM. 25G/100G/40G is supported from IOSXR release 7.2.2 onwards.
	G.8273.2	Release 7.1.1	Class B
RP:NC55-RP2-E with Line card:NC55-32T16Q4H-AT	BITS	Release 7.1.1	
	G8275.1	Release 7.1.1	For the profile G8275.1 NC55-32T16Q4H-AT supports only T-BCand does not support T-GM. 25G/100G/40G is supported from IOSXR release 7.2.2 onwards.
	G.8273.2	Release 7.1.1	Class C
NCS-55A1-36H-SE-S	G.8265.1	Release 7.0.1	
	G.8275.1	Release 7.0.1	
	G.8275.2	Release 7.0.1	
	G.8273.2	Release 7.0.1	Class B

Hardware Variant	Features	Cisco IOS XR Release	Comments
NCS-55A1-36H-S	G.8265.1	Release 7.0.1	
	G.8275.1	Release 7.0.1	
	G.8275.2	Release 7.0.1	
	G.8273.2	Release 7.0.1	Class B
NCS-55A1-24Q6H-S NCS-55A1-24Q6H-SS	G.8265.1	Release 6.6.25	
	G.8275.1	Release 6.6.25	
	G.8275.2	Release 6.6.25	From Release 7.7.1, support is available for PTP over IPv6 for ports 10G-25G and 40G-100G
	G.8273.2	Release 6.6.25	Class B
NCS-55A1-48Q6H	G.8265.1	Release 6.6.25	
	G.8275.1	Release 6.6.25	
	G.8275.2	Release 6.6.25	
	G.8273.2	Release 6.6.25	Class B
NCS-55A1-24H	G.8265.1	Release 6.5.2	
	G.8275.1	Release 6.5.2	
	G.8275.2	Release 6.5.2	
	G.8273.2	Release 6.5.2	Class B
NCS55A2-MOD	G.8265.1	Release 6.5.1	
	G.8275.1	Release 6.5.1	
	G.8275.2	Release 6.5.1	
	G.8273.2	Release 6.5.1	Class B

Hardware Variant	Features	Cisco IOS XR Release	Comments
RP:NC55-RP-E Linecard:NC55-MOD-A-S	BITS	Release 6.5.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
	G.8265.1	Release 6.5.1	
	G.8275.1	Release 6.5.1	
	G.8275.2	Release 6.5.1	This profile is supported from Release 6.5.1 for Ipv4.
	G.8273.2	Release 6.5.1	Class B
RP:NC55-RP-E Linecard:NC55-36X100G-A-SE	G.8273.2	Release 6.3.2	Class B
	BITS	Release 6.3.2	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
	G.8265.1	Release 6.3.2	
	G.8275.1	Release 6.3.2	
	G.8275.2	NA	
	G.8273.2	Release 6.3.2	Class B
NCS5501-SE	G.8265.1	Release 6.3.2	
	G.8275.1	Release 6.3.2	Class B
	G.8275.2	Release 6.3.2	
	GNSS External	Release 6.3.2	

Timing features are supported on the following MPAs:

- NC55-MPA-2TH-S
- NC55-MPA-1TH2H-S
- NC55-MPA-1TH2H-HD-S
- NC55-MPA-4H-S
- NC55-MPA-4H-HD-S
- NC55-MPA-12T-S

Breakout Timing Support

PTP Profiles 8275.1 and 8275.2 are supported on breakout ports on the following hardware PIDs:

Table 8: Breakout Timing Support Hardware Matrix

Hardware PID	Client Port	Server Port
NCS-57C3-MOD NCS-57C3-MODS-SYS	100G	25G Breakout
NC57-MPA-2D4H-S	40G	10G Breakout
NCS-55A1-36H-S	100G	25G Breakout
NCS-55A1-36H-S	100G	10G Breakout
NCS-55A1-48Q6H	10G	25G Breakout
NCS-55A1-48Q6H	100G	25G Breakout
NCS55A1-24Q6H-S	1G	25G Breakout
NCS55A1-24Q6H-S	10G	25G Breakout
NCS55A1-24Q6H-S	100G	25G Breakout
NCS-5501-SE	1G	10G Breakout
NCS-5501-SE	1G	25G Breakout
NCS-5501-SE	10G	10G Breakout
NCS-5501-SE	10G	25G Breakout
NC57-36H6D-S	25G	25G Breakout
NC57-36H6D-S	25G	10G Breakout
NC57-36H6D-S	10G	25G Breakout
NC57-36H6D-S	10G	10G Breakout
NC57-36H-SE	10G	10G Breakout

Note The server ports 100G and 40G are used as breakout for 4x25G and 4x10G respectively. The client ports are used as direct ports of different port speeds as presented in the table, *Breakout Timing Support Hardware Matrix*.

ITU-T Telecom Profiles for PTP

Cisco IOS XR software supports ITU-T Telecom Profiles for PTP as defined in the ITU-T recommendations. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

PTP lets you define separate profiles to adapt itself for use in different scenarios. A telecom profile differs in several ways from the default behavior defined in the IEEE 1588-2008 standard and the key differences are mentioned in the subsequent sections.

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

G.8265.1

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

- Clock advertisement: G.8265.1 profile specifies changes to values used in Announce messages for advertising PTP clocks. The clock class value is used to advertise the quality level of the clock, while the other values are not used.
- Clock Selection: G.8265.1 profile also defines an alternate Best Master Clock Algorithm (BMCA) to select port states and clocks is defined for the profile. This profile also requires to receive Sync messages (and optionally, Delay-Response messages) to qualify a clock for selection.
- Port State Decision: The ports are statically configured to be Master or Slave instead of using state machines to dynamically set port states.
- Packet Rates: The packet rates higher than rates specified in the IEEE 1588-2008 standard are used. They are:
  - Sync/Follow-Up Packets: Rates from 128 packets-per-second to 16 seconds-per-packet.
  - Delay-Request/Delay-Response Packets: Rates from 128 packets-per-second to 16 seconds-per-packet.
  - Announce Packets: Rates from 8 packets-per-second to 64 packets-per-second.
- Transport Mechanism: G.8265.1 profile only supports IPv4 PTP transport mechanism.
- Mode: G.8265.1 profile supports transport of data packets only in unicast mode.
- Clock Type: G.8265.1 profile only supports Ordinary Clock-type (a clock with only one PTP port).
- Domain Numbers: The domain numbers that can be used in a G.8265.1 profile network ranges from 4 to 23. The default domain number is 4.
- Port Numbers: All PTP port numbers can only be one (1) because all clocks in this profile network are Ordinary Clocks.

G.8265.1 profile defines an alternate algorithm to select between different master clocks based on the local priority given to each master clock and their quality levels (QL). This profile also defines Packet Timing Signal Fail (PTSF) conditions to identify the master clocks that do not qualify for selection. They are:

- PTSF-lossSync condition: Raised for master clocks that do not receive a reliable stream of Sync and Delay-Resp messages. Cisco IOS XR software requests Sync and Delay-Resp grants for each configured master clock to track the master clock with this condition.
- PTSF-lossAnnounce condition: Raised for master clocks that do not receive a reliable stream of Announce messages.
- PTSF-unusable condition: Raised for master clocks that receives a reliable stream of Announce, Sync, and Delay-Resp messages, but not usable by slave clocks. Cisco IOS XR software does not use this condition.

G.8275.1

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

Features of G.8275.1 profile are:

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

- Telecom Grandmaster (T-GM): Provides timing for other network devices and does not synchronize its local clock to other network devices.
- Telecom Time Slave Clock (T-TSC): A slave clock synchronizes its local clock to another PTP clock, but does not provide PTP synchronization to any other network devices.
- Telecom Boundary Clock (T-BC): Synchronizes its local clock to a T-GM or an upstream T-BC clock and provides timing information to downstream T-BC or T-TSC clocks.

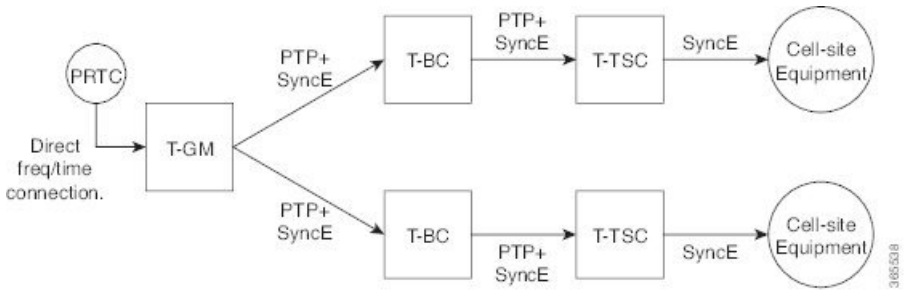
- Domain Numbers: The domain numbers that can be used in a G.8275.1 profile network ranges from 24 to 43. The default domain number is 24.

The G.8275.1 supports the following:

- T-GM: The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock (PRTC).
- T-BC: The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an upstream T-BC, and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster.
- T-TSC: The telecom time slave 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 following figure describes a sample G.8275.1 topology.

Figure 4: A Sample G.8275.1 Topology



G.8275.2

Table 9: Feature History Table

Feature Name	Release Information	Description
ITU-T G.8275.2 and Default PTP profiles over IPv6	Release 7.8.1	For ITU-T G.8275.2 and the IEEE 1588 default PTP profiles, the encapsulation type for PTP packet transport is now extended to IPv6. This feature modifies the **transport** command to include the keyword **ipv6**.

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

Effective Cisco IOS XR Software Release 7.8.1, the G.8275.2 is capable of using PTP over IPv6 as well. You can now use the **transport ipv6** command to set this encapsulation type.

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 fifth generation (5G) of mobile telecommunications technology.

Note G.8275.2 profile is supported on Cisco NCS 5500 Series Routers. However, the performance standards of this profile is not aligned with any of the ITU-T standards because performance specifications for G.8275.2 profile has not yet been made available by ITU-T.

For more information on hardware that supports G.8275.2 profile configurations, refer to Supported Hardware section in this chapter.

Features of G.8275.2 profile are:

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

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

- *Port State Decision*: The port states are selected based on the alternate BMCA algorithm. A port is configured to a **master-only** port state to enforce the port to be a master for unicast transport mode.
- *Packet Rates:*
  - Synchronization/Follow-Up—minimum is one packet-per-second and maximum of 128 packets-per-second.

- Packet rate for Announce packets—minimum of one packet-per-second and maximum of eight packets-per-second.
- Delay-Request/Delay-Response packets—minimum is one packet-per-second and maximum of 128 packets-per-second

- *Transport Mechanism*: G.8275.2 profile supports only IPv4 PTP transport mechanism.
- *Mode*: G.8275.2 profile supports transport of data packets only in unicast mode.
- *Clock Type*: G.8275.2 profile supports the following clock types:
  - *Telecom Grandmaster (T-GM)*: Provides timing for other network devices and does not synchronize its local clock to other network devices.
  - *Telecom Time Slave Clock (T-TSC)*: A slave clock synchronizes its local clock to another PTP clock, but does not provide PTP synchronization to any other network devices.
  - *Telecom Boundary Clock (T-BC)*: Synchronizes its local clock to a T-GM or an upstream T-BC clock and provides timing information to downstream T-BC or T-TSC clocks.
- *Domain Numbers*: The domain numbers that can be used in a G.8275.2 profile network ranges from 44 to 63. The default domain number is 44.

Configure PTP

Precision Time Protocol (PTP) is a protocol that defines a method to distribute time around a network. PTP support is based on the IEEE 1588-2008 standard.

This module describes the tasks you need to configure PTP on Cisco IOS XR software.

Note When a subinterface is configured with encapsulation default or untag configuration, you must configure PTP on that subinterface, instead of the main interface.

Configure Global G.8275.1 Profile

This below configuration describes the steps involved to create a global configuration profile for a PTP interface that can then be assigned to any interface as required. It uses G.8275.1 profile as an example:

Note Prior to Cisco IOS XR Software Release 6.3.3, the default PTP timers for G2875.1 were not set to standard values. This could lead to interoperability issues with other routers running the timers with updated values. Hence, to prevent such issues arising due to difference in packet rates, you must explicitly configure the **announce interval** value to 8, **sync frequency** value to 16 and **delay-request frequency** value to 16 while configuring global g.2875.1 profile.

```
RP/0/RP0/CPU0:router# config terminal
RP/0/RP0/CPU0:router(config)# ptp
```

```
RP/0/RP0/CPU0:router(config-ptp)# clock
RP/0/RP0/CPU0:router(config-ptp-clock)# domain 24
RP/0/RP0/CPU0:router(config-ptp-clock)# profile g.8275.1 clock-type T-BC
RP/0/RP0/CPU0:router(config-ptp-clock)# exit
RP/0/RP0/CPU0:router(config-ptp)# profile slave
RP/0/RP0/CPU0:router(config-ptp-profile)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config-ptp-profile)# transport ethernet
RP/0/RP0/CPU0:router(config-ptp-profile)# sync frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# announce frequency 8
RP/0/RP0/CPU0:router(config-ptp-profile)# delay-request frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# exit
RP/0/RP0/CPU0:router(config-ptp)# profile master
RP/0/RP0/CPU0:router(config-ptp-profile)# multicast target-address ethernet 01-1B-19-00-00-00
RP/0/RP0/CPU0:router(config-ptp-profile)# transport ethernet
RP/0/RP0/CPU0:router(config-ptp-profile)# sync frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# announce frequency 8
RP/0/RP0/CPU0:router(config-ptp-profile)# delay-request frequency 16
RP/0/RP0/CPU0:router(config-ptp-profile)# exit
RP/0/RP0/CPU0:router(config-ptp)# physical-layer-frequency
RP/0/RP0/CPU0:router(config-ptp)# log
RP/0/RP0/CPU0:router(config-ptp-log)# servo events
RP/0/RP0/CPU0:router(config-ptp-log)# commit
```

Verification

To display the configured PTP profile details, use **show run ptp** command.

```
RP/0/RP0/CPU0:router# show run ptp

Wed Feb 28 11:16:05.943 UTC
ptp
 clock
  domain 24
  profile g.8275.1 clock-type T-BC
 !
 profile slave
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 profile master
  multicast target-address ethernet 01-1B-19-00-00-00
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
 !
 physical-layer-frequency
 log
  servo events
!
```

Configure PTP Master Interface

The below configuration describes the steps involved to configure a PTP interface to be a Master.

```
RP/0/RP0/CPU0:router# configure terminal
```

```
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/0
RP/0/RP0/CPU0:router(config-if)# ptp
RP/0/RP0/CPU0:router(config-if-ptp)# profile master
RP/0/RP0/CPU0:router(config-if-ptp)# port state master-only
RP/0/RP0/CPU0:router(config-if-ptp)# commit
```

Verification

To verify the port state details, use **show run interface** *interface-name* command.

```
RP/0/RP0/CPU0:router# show run interface HundredGigE0/0/0/0
interface HundredGigE0/0/0/0
 ptp
  profile master
  port state master-only
!
```

Configure PTP Slave Interface

This procedure describes the steps involved to configure a PTP interface to be a Slave.

```
RP/0/RP0/CPU0:router# configure terminal
RP/0/RP0/CPU0:router(config)# interface HundredGigE0/0/0/1
RP/0/RP0/CPU0:router(config-if)# ptp
RP/0/RP0/CPU0:router(config-if-ptp)# profile slave
RP/0/RP0/CPU0:router(config-if-ptp)# port state slave-only
RP/0/RP0/CPU0:router(config-if-ptp)# commit
```

Verification

To verify the port state details, use **show run interface** *interface-name* command.

```
RP/0/RP0/CPU0:router# show run interface HundredGigE0/0/0/1
interface HundredGigE0/0/0/1
 ptp
  profile slave
  port state slave-only
 !
!
```

Configure PTP Hybrid Mode

This procedure describes the steps involved to configure router in a hybrid mode. You configure hybrid mode by selecting PTP for phase and time-of-day (ToD) and another source for the frequency.

Note

- G.8275.1 PTP profile supports only the hybrid mode. By default, the hybrid mode is used, regardless of the physical-layer-frequency configuration.
- G.8275.2 PTP profile supports both hybrid mode and non-hybrid mode. By default, the non-hybrid mode is used. Hybrid mode is used only when the physical-layer-frequency is configured.
- Configure appropriate clock priorities when using synchronous Ethernet for frequency synchronization. This ensures the system selects the frequency source from the same interface as the PTP source. Aligning both frequency and time synchronization to the same interface helps maintain consistency and reduces configuration complexity.

To configure PTP Hybrid mode:

1. Configure Global Frequency Synchronization

```
RP/0/RP0/CPU0:router(config)# frequency synchronization
RP/0/RP0/CPU0:router(config)# commit
```

2. Configure Frequency Synchronization for an Interface. The time-of-day-priority setting specifies that SyncE to be used as a ToD source if there is no source available with a lower priority.

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

3. Configure Global PTP. To configure PTP as source for ToD, use ToD priority values in the range from 1 (highest priority) to 254 (lowest priority). Use frequency from the physical layer.

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

4. Configure PTP Interface. To enable this interface as a PTP Master, use **master** command in ptp-interface configuration mode.

```
RP/0/RP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.0.1/24
RP/0/RP0/CPU0:router(config-if)# ptp
RP/0/RP0/CPU0:router(config-if-ptp)# master ipv4 10.0.0.2
RP/0/RP0/CPU0:router(config-if-ptp)# commit
```

Verifying PTP Hybrid Mode

```
RP/0/RP0/CPU0:router # show frequency synchronization selection

Tue Feb  6 06:34:17.627 UTC
Node 0/0/CPU0:
==============
Selection point: ETH_RXMUX (1 inputs, 1 selected)
  Last programmed 3d23h ago, and selection made 3d23h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: T0-SEL-B 1588-SEL
    Router scoped : None
```

```
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  GigabitEthernet0/0/0/2    n/a    PRC      1  Available
Selection point: LC_TX_SELECT (1 inputs, 1 selected)
  Last programmed 3d23h ago, and selection made 3d23h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  Used for local line interface output
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  7  GigabitEthernet0/0/0/2    0/RP0/CPU0 T0-SEL-B 1       PRC    1  Available
Node 0/RP0/CPU0:
==============
Selection point: T0-SEL-B (3 inputs, 1 selected)
  Last programmed 1d00h ago, and selection made 00:36:33 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : CHASSIS-TOD-SEL
    Chassis scoped: LC_TX_SELECT
    Router scoped : None
  Uses frequency selection
  Used for local line interface output
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
1  GigabitEthernet0/0/0/2 0/0/CPU0 ETH_RXMUX 1       PRC    1  Locked
   PTP [0/RP0/CPU0]  n/a      SEC  254  Available
   Internal0 [0/RP0/CPU0] n/a      SEC  255  Available

Selection point: 1588-SEL (2 inputs, 1 selected)
  Last programmed 3d23h ago, and selection made 00:36:33 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input         Last Selection Point      QL     Pri  Status
  == ========================  ========================  =====  ===  ===========
  1  GigabitEthernet0/0/0/2    0/0/CPU0 ETH_RXMUX 1      PRC      1  Locked
     Internal0 [0/RP0/CPU0]    n/a      SEC    255  Available

Selection point: CHASSIS-TOD-SEL (2 inputs, 1 selected)
  Last programmed 1d00h ago, and selection made 1d00h ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
PRC    1  Locked
SEC  255  Available
Last Selection Point
QL Pri Status
Uses time-of-day selection
S  Input       Last Selection Point      Pri  Time  Status
== ========================  ========================  ===  ====  ===========
  1  PTP [0/RP0/CPU0]          n/a         100  Yes   Available
     GigabitEthernet0/0/0/2    0/RP0/CPU0 T0-SEL-B 1   100  No    Available
```

Configure PTP for SyncE and PTP Traceability

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

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

If you configure this CLI, note these points:

- A SyncE source among *equal sources* [8] is selected on the same interface on which PTP is selected by the router.
- If the SyncE source on the PTP receiver interface is inferior (in terms of QL and user configured priority) than any other available SyncE source, then the SyncE source is selected using the default criteria (based on the ITU-T G.781 requirements).
- In the event that the selected PTP source goes down or if the PTP source's quality degrades, the system may switch to another PTP source. In such case, use the **synchronous-ethernet prefer-interface ptp-receiver** command so that the SyncE source selection would also switch to the new PTP receiver interface. Here, the preferred switching of SyncE source to the new PTP receiver interface shall happen only if the new interface uses the same SyncE QL and the user configured priority as the previously selected interface.

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

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

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

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

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

Configure PTP for SyncE and PTP Traceability

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

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

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

If you configure this CLI, note these points:

- A SyncE source among *equal sources* [9] is selected on the same interface on which PTP is selected by the router.
- If the SyncE source on the PTP receiver interface is inferior (in terms of QL and user configured priority) than any other available SyncE source, then the SyncE source is selected using the default criteria (based on the ITU-T G.781 requirements).
- In the event that the selected PTP source goes down or if the PTP source's quality degrades, the system may switch to another PTP source. In such case, use the **synchronous-ethernet prefer-interface ptp-receiver** command so that the SyncE source selection would also switch to the new PTP receiver interface. Here, the preferred switching of SyncE source to the new PTP receiver interface shall happen only if the new interface uses the same SyncE QL and the user configured priority as the previously selected interface.

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

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

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

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

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

Configure PTP Telecom Profile Interface

This procedure describes the steps involved to create an interface for PTP ITU-T Telecom Profiles.

Note
- It is also possible to make these definitions within a global PTP profile and attach them to the interface using the profile command in PTP interface configuration mode.

1. To configure an interface, use **interface** *type interface-path-id* command in the configuration mode.

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
```

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

2. To enter the PTP configuration mode for the given interface, use **ptp** command in the interface configuration mode.

```
RP/0/RP0/CPU0:router(config-if)# ptp
```

3. To configure a PTP profile (or specify a previously defined profile), use **profile** *name* command in the ptp-interface configuration mode.

Note Any additional commands entered in ptp-interface configuration mode overrides the global profile settings.

```
RP/0/RP0/CPU0:router(config-if-ptp)# profile slave
```

4. To configure frequency for Sync or Delay-request messages for the given ptp interface, use **sync frequency** *rate* command or **delay-request frequency** *rate* command appropriately in the ptp-interface configuration mode. The valid configurable values are **2, 4, 8, 16, 32, 64 or 128**.

```
RP/0/RP0/CPU0:router(config-if-ptp)# sync frequency 128
```

```
RP/0/RP0/CPU0:router(config-if-ptp)# delay-request frequency 128
```

5. To configure duration for different PTP messages, use one of the following commands in the ptp-interface configuration mode: **announce grant-duration** *duration*, **sync grant-duration** *duration*, or **delay-response grant-duration** *duration*. The duration value can be between **60 and 1000 seconds**.

Note This duration value represents the length of grant that is requested by a port in Slave state and represents the maximum grant-duration allowed when the port is in Master state.

```
RP/0/RP0/CPU0:router(config-if-ptp)# announce grant-duration 120
```

```
RP/0/RP0/CPU0:router(config-if-ptp)# sync grant-duration 120
```

```
RP/0/RP0/CPU0:router(config-if-ptp)# delay-response grant-duration 120
```

6. To configure a timeout value, length of time by when a PTP message must be received (before PTSF-lossSync is raised), use one of the following commands in the ptp-interface configuration mode: **sync timeout** *timeout* or **delay-response timeout** *timeout*. The timeout value can be between **100 to 10000 micro seconds**.

```
RP/0/RP0/CPU0:router(config-if-ptp)# sync timeout 120
```

```
RP/0/RP0/CPU0:router(config-if-ptp)# delay-response timeout 120
```

7. To configure a response for unicast-grant invalid-request, use **unicast-grant invalid-request {reduce | deny}** command. The response for requests with unacceptable parameters would either be denied or granted with reduced parameters.

```
RP/0/RP0/CPU0:router(config-if-ptp)# unicast-grant
invalid-request reduce
```

8. To configure IPv4 address for a PTP master, use **master ipv4** *ip-address* command in the ptp-interface configuration mode.

```
RP/0/RP0/CPU0:router(config-if-ptp)# master ipv4 1.7.1.2
```

9. To override the clock-class received in Announce messages from the specified Master, use **clock-class** *class* command in the ptp-master-interface configuration mode. The class values can range from **0 to 255**.

```
RP/0/RP0/CPU0:router(config-if-ptp-master)# clock-class 2
```

Verification

To display the PTP interface details, use **show ptp interfaces brief** command.

```
RP/0/RP0/CPU0:router# show ptp interfaces brief
Fri Feb  9 11:16:45.248 UTC
Intf              Port         Port                  Line
Name              Number       State        Encap    State         Mechanism
-------------------------------------------------------------------------------
Gi0/1/0/0         1            Slave        IPv4     up            1-step DRRM
Gi0/0/0/40        2            Master       IPv4     up            1-step DRRM
```

To verify the configured profile details, use **show run interface** *interface-name* command.

```
RP/0/RP0/CPU0:router# show run interface Gi0/0/0/33

Wed Feb 28 11:49:16.940 UTC
interface GigabitEthernet0/0/0/33
ptp
  profile slave
  transport ipv4
  sync frequency 64
  clock operation one-step
  delay-request frequency 64
  !
 physical-layer-frequency
!
ipv4 address 21.1.1.2 255.255.255.0
frequency synchronization
  selection input
  priority 5
  wait-to-restore 0
!
```

Configure PTP Telecom Profile Clock

This procedure describes the steps involved to configure PTP clock and its settings to be consistent with ITU-T Telecom Profiles for Frequency.

1. To enter the PTP configuration mode, use **ptp** command in the configuration mode.

```
RP/0/RP0/CPU0:router(config)# ptp
```

2. To enter the PTP-clock configuration mode, use **clock** command in the ptp-configuration mode.

```
RP/0/RP0/CPU0:router(config-ptp)# clock
```

3. To configure the domain-number for a PTP profile, use **domain** *number* command in the ptp-configuration mode. The allowed domain number range for G.8265.1 profile is between **4 and 23** and the range for G.8275.1 profile is between **24 and 43**.

```
RP/0/RP0/CPU0:router(config-ptp)# domain 24
```

4. To exit the ptp-clock configuration mode, use **exit** command.

```
RP/0/RP0/CPU0:router(config-ptp-clock)# exit
```

5. To configure the desired telecom profile and the clock type for the profile, use **clock profile {g.8275.1 | g.8275.2} clock-type {T-GM | T-BC | T-TSC}** command in the ptp configuration mode. For **g.8265.1** clock profile, clock type is either master or slave.

Note The **clock-selection telecom-profile** and **clock-advertisement telecom-profile** commands are deprecated from Release 6.1.2. They are replaced by the **clock profile** command.

```
RP/0/RP0/CPU0:router(config-ptp)# clock profile g.8275.1 clock-type T-GM
```

Verification

To display the configured PTP clock profile details, use **show run ptp** command.

```
RP/0/RP0/CPU0:router# show run ptp
ptp
clock
  domain 24
  profile g.8275.1 clock-type T-GM
  timescale PTP
  time-source GPS
  clock-class 6
!
profile master
  transport ethernet
  sync frequency 16
  announce interval 1
  delay-request frequency 16
!
profile master1
  transport ethernet
  sync frequency 64
  announce interval 1
  delay-request frequency 64
!
```

To verify that PTP has been enabled on the router and the device is in LOCKED Phase, use **show ptp platform servo** command.

```
RP/0/RP0/CPU0:router # show ptp platform servo

Fri Feb  9 11:16:54.568 UTC
Servo status: Running
```

```
Servo stat_index: 2
Device status: PHASE_LOCKED
Servo log level: 0
Phase Alignment Accuracy: 1 ns
Sync timestamp updated: 111157
Sync timestamp discarded: 0
Delay timestamp updated: 111157
Delay timestamp discarded: 0
Previous Received Timestamp T1: 1518155252.263409770  T2: 1518155252.263410517  T3:
1518155252.287008362  T4: 1518155252.287009110
Last Received Timestamp T1: 1518155252.325429435  T2: 1518155252.325430194  T3:
1518155252.348938058  T4: 1518155252.348938796
Offset from master:  0 secs, 11 nsecs
Mean path delay   :  0 secs, 748 nsecs
setTime():2  stepTime():1  adjustFreq():10413 adjustFreqTime():0
Last setTime: 1.000000000 flag:1  Last stepTime:-736216, Last adjustFreq:465
```

Configure PTP Delay Asymmetry

Table 10: Feature History Table

Feature Name	Release Information	Description
PTP Delay Asymmetry	Release 7.3.1	Any delays on Precision Time Protocol (PTP) paths can impact PTP accuracy and in turn impact clock settings for all devices in a network. This feature allows you to configure the static asymmetry such that the delay is accounted for and the PTP synchronization remains accurate. The **delay-symmetry** command is introduced for this feature.

Configure PTP delay asymmetry to offset the static delays on a PTP path that occur due to different route selection for forward and reverse PTP traffic. Delays can also be due to any node having different delay for ingress or egress path. These delays can impact PTP accuracy due to the asymmetry in PTP. With this feature, you can enable a higher degree of accuracy in the PTP server performance leading to better synchronization between real-time clocks of the devices in a network.

Configuration of this delay asymmetry provides an option to configure static delays on a client clock for every server clock. You can configure this delay value in microseconds and nanoseconds. Configured PTP delay asymmetry is also synchronized with the Servo algorithm.

Note

- If you configure multiple PTP delay asymmetries for the same PTP profile, the latest PTP delay asymmetry that you configure is applied to the PTP profile.
- For G8275.1 and G8275.2 PTP profiles, PTP delay asymmetry is supported for both, client port and dynamic port that act as a client.
- Fixed delay can be measured by using any test and measurement tool. Fixed delay can be compensated by using the positive or negative values. For example, if the fixed delay is +10 nanoseconds, configure -10 nanoseconds to compensate the fixed delay.

A positive value indicates that the server-to-client propagation time is longer than the client-to-server propagation time, and conversely for negative values.

Supported PTP Profiles

The following PTP profiles support the configuration of PTP delay asymmetry:

- PTP over IP (G8275.2 or default profile)
- PTP over L2 (G8275.1)

Restrictions

- PTP delay asymmetry can be configured only on the PTP port of the grandmaster clock, which can either be a boundary clock or an ordinary clock.
- PTP delay asymmetry is supported for delay compensation of fixed cables and not for variable delay in the network.
- PTP delay asymmetry can be configured within the range of 3 microseconds and -3 microseconds or 3000 nanoseconds and -3000 nanoseconds.

Configuration

To configure PTP delay asymmetry:

1. Configure an interface with PTP.
2. Configure PTP delay asymmetry on the client side.

Configuration Example

```
/* Configure an interface with PTP. */
Router# configure
Router(config)# interface HundredGigE 0/1/0/0
Router(config-if)# ptp

/* Configure PTP delay asymmetry on the client side. */
Router(config-if-ptp)# delay-asymmetry 3 microseconds
Router(config-if-ptp)# commit
```

Running Configuration

```
interface preconfigure HundredGigE 0/1/0/0
 ptp
  delay-asymmetry 3 microseconds
```

Verification

To verify if PTP delay asymmetry is applied, use the **show ptp foreign-masters** command:

```
Router# show ptp foreign-masters
Sun Nov 1 10:19:21.874 UTC
Interface HundredGigE0/1/0/0 (PTP port number 1)
IPv4, Address 209.165.200.225, Unicast
Configured priority: 1
Configured clock class: None
Configured delay asymmetry: 3 microseconds <- configured variable delay asymmetry value
Announce granted: every 2 seconds, 300 seconds
Sync granted: 16 per-second, 300 seconds
Delay-resp granted: 16 per-second, 300 seconds
Qualified for 2 minutes, 45 seconds
Clock ID: 80e01dfffe8ab73f
Received clock properties:
Domain: 0, Priority1: 128, Priority2: 128, Class: 6
Accuracy: 0x22, Offset scaled log variance: 0xcd70
Steps-removed: 1, Time source: GPS, Timescale: PTP
Frequency-traceable, Time-traceable
Current UTC offset: 37 seconds (valid)
Parent properties:
Clock ID: 80e01dfffe8ab73f
Port number: 1
```

To validate the approximate compensated delay value, use the **show ptp platform servo** command:

```
Router# show ptp platform servo
Mon Jun 27 22:32:44.912 UTC
Servo status: Running
Servo stat_index: 2
Device status: PHASE_LOCKED
Servo Mode: Hybrid
Servo log level: 0
Phase Alignment Accuracy: -2 ns
Sync timestamp updated: 18838
Sync timestamp discarded: 0
Delay timestamp updated: 18837
Delay timestamp discarded: 0
Previous Received Timestamp T1: 1657002314.031435081  T2: 1657002314.031436686  T3:
1657002314.026815770  T4: 1657002314.026814372
Last Received Timestamp T1: 1657002314.031435081  T2: 1657002314.031436686  T3:
1657002314.088857790  T4: 1657002314.088856392
Offset from master:  0 secs, 1502 nsecs    <<--compensated value shows 1.5 microseconds
because the asymmetry configured under the interface is
3 microseconds.->>
Mean path delay   :  0 secs, 103 nsecs
setTime():0  stepTime():0 adjustFreq():2
Last setTime: 0.000000000 flag:0  Last stepTime:0 Last adjustFreq:-5093
```

IEEE Default Profile

The IEEE default profile is a PTP configuration profile that

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

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

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

Example: Global PTP Configuration

Global PTP Configuration:

```
ptp
 clock
  domain 0
 !
 profile ptp_node
  transport ipv4
  sync frequency 32
  announce frequency 1
  delay-request frequency 32
 !
 physical-layer-frequency
!
```

Example: PTP Master Configuration

PTP Master Configuration:

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

Example:PTP Slave Configuration

PTP Slave Configuration:

```
interface TenGigE0/0/0/18
 ptp
```

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

Performance Monitoring for PTP Networks

Table 11: Feature History Table

Feature Name	Release Information	Feature Description
Performance Monitoring	Release 24.3.1	Introduced in this release on: NCS 5500 fixed port routers You can now get statistical information with Performance Monitoring in PTP networks, such as clock accuracy, synchronization status, and network delays by defining Performance Monitoring Parameters and Port Specific Parameters. This feature empowers operators with comprehensive performance monitoring and precise time-stamp analysis, offering enhanced granularity for time synchronization in telecommunication networks. By providing detailed insights, it enables operators to make well-informed decisions and take proactive actions to ensure optimal network performance. The feature introduces these changes: **CLI:** • **performance-monitoring** • **show ptp platform performance-counters** • **show ptp dataset performance** **YANG Data Models:** • `Cisco-IOS-XR-ptp-cfg.yang` • `Cisco-IOS-XR-ptp-oper.yang` • `Cisco-IOS-XR-um-ptp-cfg.yang` (see GitHub, YANG Data Models Navigator)

Performance Monitoring in PTP involves tracking and analyzing the performance of PTP networks to ensure accurate time synchronization across devices. This includes monitoring various metrics such as clock accuracy,

synchronization status, and network delays. The goal is to identify and address any issues that may affect the precision and reliability of time synchronization in the network.

Performance Monitoring now has the ability to provide performance monitoring and time-stamp analysis information in a PTP network as per Annex J IEEE 1588-2019. This feature also includes additional monitoring granularity for time synchronization in telecommunication networks as per Annex F from the G8275 standard. For more information on PTP, Best TimeTransmitter Clock Algorithm (BTCA), see PTP Overview.

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

- Performance Monitoring Parameters
- Port Specific Parameters

Performance Monitoring Parameters

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

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

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

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

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

Additional Port Specific Parameters

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

- received (rx) and

- transmitted (tx)

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

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

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

Record format

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

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

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

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

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

Configure PTP Performance Monitoring

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

Procedure

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

Example:

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

Step 2 Run the **sh ptp platform performance-counters** command to display the details of all 123 records.

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

Example:

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

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

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

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

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

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

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

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

==============

….
```

Step 3 Run the **show ptp dataset performance clock** command to display the performance monitoring data-set details in 15 minutes intervals.

Example:

```
Router#show ptp dataset performance clock

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

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

Step 4 Run the **show ptp dataset performance port** to display the Performance Monitoring Port Data-set in 15 minutes intervals.

Example:

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

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

Configuration Examples

Slave Configuration Example

The following example shows a PTP slave configuration:

```
interface TenGigE 0/1/0/5
ptp
 profile slave
 transport ipv4
 port state slave-only
 master ipv4 1.7.1.2
 !
 announce interval 1
 !
ipv4 address 1.7.1.1 255.255.255.0
!
```

Master Configuration Example

This example shows a PTP master configuration:

```
ptp
 profile master
 transport ipv4
 announce interval 1
!
ipv4 address 1.7.1.2 255.255.255.0
```

```
 !
```

PTP Hybrid Mode Configuration Example

This example shows the configuration of PTP hybrid mode:

```
ptp
 time-of-day priority 10
 !
interface GigabitEthernet0/1/1/0
 ptp
  transport ipv4
  port state slave-only
  master ipv4 1.7.1.2
  !
  sync frequency 64
  announce interval 1
  delay-request frequency 64
 !
interface GigabitEthernet 0/1/0/1
 ipv4 address 1.7.1.2 255.255.255.0
 speed 100
 frequency synchronization
  selection input
  priority 10
  wait-to-restore 0
  ssm disable
  time-of-day-priority 100
 !
```

ITU-T Telecom Profile Examples:

G.8265.1 Profile Configuration Examples

Master Global Configuration:

```
ptp
 clock
 domain 4
 profile g.8265.1
 !
  profile master
  transport ipv4
  sync frequency 16
  announce interval 1
  delay-request frequency 16
interface gi 0/2/0/4
 ptp
  profile master
  transport ipv4
  clock operation two-step
 !
 ipv4 address 17.1.1.1/24
```

Slave Global Configuration:

```
ptp
 clock
 domain 4
 profile g.8265.1
 !
  profile slave
  transport ipv4
  sync frequency 16
  announce interval 1
  delay-request frequency 16
interface gi 0/1/0/0
 ptp
  profile slave
  transport ipv4
  Master ipv4 18.1.1.1
  port state slave-only
  !
  clock operation two-step
  !
 ipv4 address 18.1.1.2/24
```

Configuring With Clock Type as T-Boundary Clock (T-BC)

```
ptp
 clock
 domain 4
 profile g.8265.1
 !
  profile master
  transport ipv4
  sync frequency 16
  announce interval 1
  delay-request frequency 16
  exit
  profile slave
  transport ipv4
  sync frequency 16
  announce interval 1
  delay-request frequency 16
  exit
interface gi 0/2/0/4
 ptp
  profile slave
  transport ipv4
  Master ipv4 17.1.1.1
  port state slave-only
  !
  clock operation two-step
  !
ipv4 address 17.1.1.2/24
interface gi 0/2/0/0
 ptp
  profile master
  transport ipv4
  clock operation two-step
  !
 ipv4 address 18.1.1.1/24
```

G.8275.1 Profile Configuration Examples

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

Master Global Configuration:

```
ptp
 clock
 domain 24
 profile g.8275.1
 !
  profile master
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
interface gi 0/2/0/4
 ptp
  profile master
  transport ethernet
  multicast target-address ethernet 01-1B-19-00-00-00
  !
```

Slave Global Configuration:

```
ptp
 clock
 domain 24
 profile g.8275.1 clock-type T-TSC
 !
  profile slave
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
interface gi 0/1/0/0
 ptp
  profile slave
  transport ethernet
  multicast target-address ethernet 01-1B-19-00-00-00
  !
```

Configuring With Clock Type as T-Boundary Clock (T-BC)

```
ptp
 clock
 domain 24
 profile g.8275.1 clock-type T-BC
 !
  profile master
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
  exit
```

```
  profile slave
  transport ethernet
  sync frequency 16
  announce frequency 8
  delay-request frequency 16
  exit
interface gi 0/2/0/4
 ptp
  profile slave
  transport ethernet
  multicast target-address ethernet 01-1B-19-00-00-00
  !
interface gi 0/2/0/0
 ptp
  profile master
  transport ethernet
  multicast target-address ethernet 01-1B-19-00-00-00
```

G.8275.2 Profile Configuration Examples

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

Master Global Configuration:

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

interface GigabitEthernet0/2/0/11
 ptp
  profile master
 !
 ipv4 address 17.1.1.1/24
```

Slave Global Configuration:

```
ptp
 clock
  domain 44
  profile g.8275.2 clock-type T-TSC
 !
 profile slave
  transport ipv4
  port state slave-only
  sync frequency 64
  announce frequency 8
  unicast-grant invalid-request deny
```

```
  delay-request frequency 64
 !
 log
  servo events
  best-master-clock changes
 !
!
interface GigabitEthernet0/2/0/12
 ptp
  profile slave
  master ipv4 18.1.1.1
  !
 !
 ipv4 address 18.1.1.2/24
!
```

Effective Cisco IOS XR Software Release 7.8.1, the encapsulation type for PTP packet transport is now extended to IPv6; you can now use the **transport ipv6** to set this encapsulation type.

Configuring With Clock Type as T-Boundary Clock (T-BC)

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

interface GigabitEthernet0/2/0/11
 ptp
  profile master
 !
 ipv4 address 18.1.1.1/24
!

interface GigabitEthernet0/2/0/12
 ptp
  profile slave
  master ipv4 17.1.1.1
  !
 !
 ipv4 address 17.1.1.2/24
!
```

Effective Cisco IOS XR Software Release 7.8.1, the encapsulation type for PTP packet transport is now extended to IPv6; you can now use the **transport ipv6** command to set this encapsulation type.

Monitor PTP virtual port using PTP timeReceiver ports

Table 12: Feature History Table

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

Monitor PTP virtual port using PTP timeReceiver ports

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

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

Threshold configuration

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

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

Threshold breach

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

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

Sample syslog message

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

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

Supported platforms

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

Alarm conditions

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

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

- the offset value drops below the configured threshold.
- the threshold value is unconfigured.
- the virtual port is no longer the best source of timing for reasons such as configuration or clock rank change.
- all timeTransmitters are lost.

Configure threshold to monitor PTP virtual port using PTP timeReceiver ports

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

Before you begin

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

Procedure

Step 1 Configure PTP.

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

Step 2 Configure the PTP virtual port.

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

Step 3 Configure the threshold for the PTP virtual port.

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

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

Configuration example

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

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

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

```
Router(config-gnss-freqsync)#priority 20
Router(config-gnss-freqsync)#time-of-day-priority 100
Router(config-gnss-freqsync)#quality receive exact itu-t option 1 PRC
Router(config-gnss-freqsync)#commit

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

Verify PTP virtual port using PTP timeReceiver ports

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

Before you begin

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

Procedure

Step 1 Verify local PTP clock information.

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

If no timeTransmitters send timestamps, the show command displays:

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

Step 2 Verify the best timeReceiver clock information.

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

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

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

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

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

Step 3 Verify the timeReceiver clock information.

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

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

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

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

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

Step 4 Verify the generated syslog.

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

Restriction to monitor PTP virtual port using PTP timeReceiver ports

The main restriction to consider while enforcing the threshold:

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

Configure E-SyncE on Primary and Secondary Interface

Primary Interface

The following example shows how you can configure global synce on primary interface:

```
Router#configure terminal
Router(config)#frequency synchronization
Router(config-freqsync)#quality itu-t option 1
Router(config-freqsync)#clock-identity mac-address aaaa.bbbb.cccc
Router(config-freqsync)#clock-interface timing-mode system
Router(config-freqsync)#commit
```

The following example shows how you can configure synce on primary interface:

```
Router#configure terminal
Router(config)# interface HundredGigE0/0/0/11
Router(config-if)# frequency synchronization
Router(config-if)# quality transmit exact itu-t option 1 ePRTC
Router(config-if)# commit
```

Secondary Interface

The following example shows how you can configure global synce on secondary interface:

```
Router#configure terminal
Router(config)#frequency synchronization
Router(config-freqsync)#quality itu-t option 1
Router(config-freqsync)#clock-interface timing-mode system
Router(config-freqsync)#commit
```

The following example shows how you can configure synce on secondary interface:

```
Router#configure terminal
Router(config)# interface HundredGigE0/0/0/10
Router(config-if)# frequency synchronization
Router(config-if-freqsync)# selection input
Router(config-if-freqsync)# priority 10
```

```
Router(config-if-freqsync)# wait-to-restore 0
Router(config-if-freqsync)# commit
```

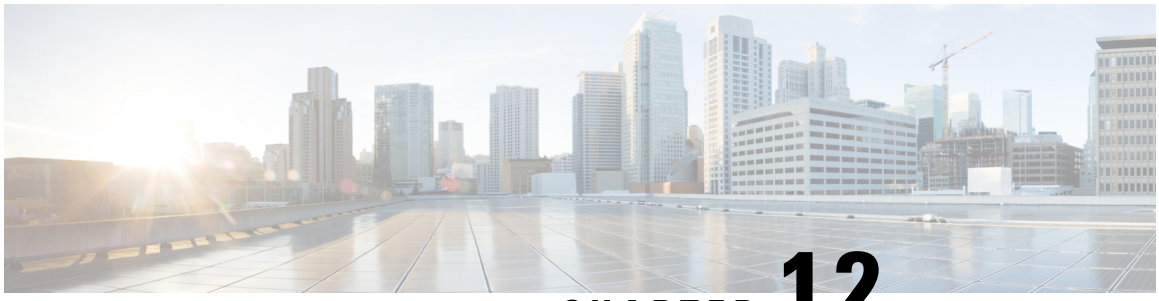
Note If timing mode system is not configured, the major alarm `T4 PLL is in FREERUN mode` is raised. This alarm has no functional impact to the system behavior.

Verification

Use the **show frequency synchronization** command if e-synce is configured.

```
Routerr#show frequency synchronization  interfaces  br
Flags:  > - Up                D - Down              S - Assigned for selection
        d - SSM Disabled      x - Peer timed out    i - Init state
        s - Output squelched
Fl   Interface                QLrcv QLuse Pri QLsnd Output driven by
==== ======================== ===== ===== === ===== ========================
>S   HundredGigE0/0/0/13      ePRTC ePRTC  31 ePRTC HundredGigE0/0/0/18
>S   HundredGigE0/0/0/18      ePRTC ePRTC  30 DNU   HundredGigE0/0/0/18
RP/0/RP0/CPU0:Shadowtower#sh frequency  synchronization  selection
Node 0/RP0/CPU0:
==============
Selection point: T0-SEL-B (3 inputs, 1 selected)
  Last programmed 02:41:55 ago, and selection made 02:41:04 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : CHASSIS-TOD-SEL
    Chassis scoped: LC_TX_SELECT
    Router scoped : None
  Uses frequency selection
  Used for local line interface output
  Used for local clock interface output
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  33 HundredGigE0/0/0/18       0/RP0/CPU0 ETH_RXMUX 33   ePRTC   30  Locked
     HundredGigE0/0/0/13       0/RP0/CPU0 ETH_RXMUX 22   ePRTC   31  Available
     Internal0 [0/RP0/CPU0]    n/a                         SEC  255  Available

Selection point: 1588-SEL (3 inputs, 1 selected)
  Last programmed 02:41:55 ago, and selection made 02:41:04 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ==========
  1  Internal0 [0/RP0/CPU0]    n/a                         SEC  255  Freerun
     HundredGigE0/0/0/18       0/RP0/CPU0 ETH_RXMUX 33   ePRTC   30  Available
     HundredGigE0/0/0/13       0/RP0/CPU0 ETH_RXMUX 22   ePRTC   31  Available

Selection point: CHASSIS-TOD-SEL (1 inputs, 1 selected)
  Last programmed 02:41:44 ago, and selection made 02:41:44 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : None
    Chassis scoped: None
    Router scoped : None
  Uses time-of-day selection
  S  Input                     Last Selection Point      Pri  Time  Status
```

```
  == ========================  ========================  ===  ====  ===========
  1  HundredGigE0/0/0/18       0/RP0/CPU0 T0-SEL-B 33    100  No    Available

Selection point: ETH_RXMUX (2 inputs, 2 selected)
  Last programmed 02:41:55 ago, and selection made 02:41:55 ago
  Next selection points
    SPA scoped    : None
    Node scoped   : T0-SEL-B 1588-SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  33 HundredGigE0/0/0/18       n/a                       ePRTC   30  Available
  22 HundredGigE0/0/0/13       n/a                       ePRTC   31  Available
```



CHAPTER 12

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

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

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

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

The router supports QL-enabled mode.

- Frequency Synchronization Timing Concepts, on page 195
- SyncE Hardware Support, on page 197
- Configuring Frequency Synchronization, on page 200
- SyncE Preference for PTP Receiver Interface, on page 201
- Verifying the Frequency Synchronization Configuration, on page 203
- Verifying the ESMC Configuration, on page 205
- Verifying Controllers Timing LEDs, on page 206

Frequency Synchronization Timing Concepts

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

Sources

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

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

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

Selection Points

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

The input signals to the selection points can be:

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

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

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

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

Note

- We recommend you to configure, and enable Frequency Synchronization selection input on two interfaces per line card.
- For link aggregation, you must configure and enable Frequency Synchronization selection input on a single bundle member.

Restrictions

- SyncE is not supported on Gigabit Ethernet 0/0/0/24 to 0/0/0/31 ports.
- The Precision Time Protocol (PTP) session flaps during Route Processor Failover (RPFO).

SyncE Hardware Support

Note The table also contains support details of upcoming releases. You can read this table in context of the current release and see relevant *Release Notes* for more information on supported features and hardware.

This table provides a detailed information on the timing features that are supported on the following hardware variants.

Hardware Variant	Features	Cisco IOS XR Release	Comments
NCS-57C3-MOD-SYS NCS-57C3-MODS-SYS	E-SyncE	Release 7.9.1	
NC57-24DD	SyncE	Release 7.5.1	
NC57-18DD-SE	SyncE	Release 7.5.1	
NCS-57C1-48Q6-SYS	SyncE	Release 7.5.1	
	E-SyncE	Release 7.9.1	
RP:NC57-MOD-RP2-E with NCS-57C3-MOD-SYS	SyncE	Release 7.4.1	1G Fiber clock recovery is supported from IOS XR Release 7.6.1 on SFP28 ports 0-7, 40-55, and not on MPA.
RP:NC57-MOD-RP2-E with NCS-57C3-MODS-SYS	SyncE	Release 7.4.1	1G Fiber clock recovery is supported from IOS XR Release 7.6.1 on SFP28 ports 0-7, 36-51, and not on MPA.

Hardware Variant	Features	Cisco IOS XR Release	Comments
RP: NC55-RP2-E Line card: NC57-36H6D-S	SyncE	Release 7.3.2	• Release 7.3.2 - Supports Compatible Mode only • Release 7.7.1 - Supports both Native and Compatible mode. • SyncE is not supported on 100GE interfaces, when they are used in 1G mode.
NCS-57B1-5DSE-SYS NCS-57B1-6D24-SYS	SyncE	Release 7.3.1	
	E-syncE	Release 7.9.1	
RP:NC55-RP-E with Line cards: NC55-MOD-A-S and NC55-32T16Q4H-AT	SyncE	Release 7.1.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
RP:NC55-RP2-E with Line cards: NC55-MOD-A-S and NC55-32T16Q4H-AT	SyncE	Release 7.1.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
RP:NC55-RP2-E with Line card:NC55-32T16Q4H-AT	SyncE	Release 7.1.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS-55A1-36H-SE-S	SyncE	Release 7.0.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS-55A1-36H-S	SyncE	Release 7.0.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS-55A1-24Q6H-S NCS-55A1-24Q6H-SS	SyncE	Release 6.6.25	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.

Hardware Variant	Features	Cisco IOS XR Release	Comments
NCS-55A1-48Q6H	SyncE	Release 6.6.25	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS-55A1-24H	SyncE	Release 6.5.2	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS55A2-MOD	SyncE	Release 6.5.1	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
	E-syncE	Release 7.9.1	E-SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
RP:NC55-RP-E Linecard:NC55-MOD-A-S	SyncE	Release 6.5.1	SyncE is not supported on 100GE interfaces, when theyare used in 1G mode.
RP:NC55-RP-E Linecard:NC55-36X100G-A-SE	SyncE	Release 6.3.2	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
NCS5501-SE	SyncE	Release 6.3.2	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode. SyncE is supported on 10G from ports 8 to 15, but it is not supported on these ports in 1G mode.

SyncE features are supported on the following MPAs:

- NC55-MPA-2TH-S
- NC55-MPA-1TH2H-S
- NC55-MPA-1TH2H-HD-S
- NC55-MPA-4H-S
- NC55-MPA-4H-HD-S
- NC55-MPA-12T-S

Configuring Frequency Synchronization

Enabling Frequency Synchronization on the Router

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

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

Configuring Frequency Synchronization on an Interface

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

Before You Begin

You must enable frequency synchronization globally on the router.

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

Configuring Frequency Synchronization on a Clock Interface

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

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

SyncE Preference for PTP Receiver Interface

Table 13: Feature History Table

Feature Name	Release Information	Feature Description
SyncE Preference for PTP Receiver Interface	Release 24.4.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can now mitigate synchronization issues when SyncE and PTP sources come from different, non-traceable origins. This feature ensures that SyncE selection among sources with equal Quality Levels (QL) and user priority prefers the interface on which the PTP receiver is selected. If the PTP source fails or its quality degrades, causing the system to switch to another PTP source, SyncE switches to the new PTP source, provided the new interface has the same SyncE QL and priority as the previously selected interface. This feature introduces **synchronous-ethernet prefer-interface ptp-receiver** command.

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

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

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

Benefits of SyncE Preference for PTP Receiver Interface

- Enhanced Synchronization - Ensures that SyncE and PTP sources are traceable to the same clock source, preventing synchronization issues.
- Improved Reliability - Reduces the risk of PTP synchronization failures caused by rapid clock drifts.
- Simplified Configuration - Automates the selection process of SyncE sources to align with the PTP receiver, simplifying network management.

Restrictions for SyncE Preference for PTP Receiver Interface

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

Configure SyncE Preference for PTP Receiver Interface

Enable SyncE preference for PTP Receiver Interface.

Procedure

Step 1 Enter the frequency synchronization mode.

Example:

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

Step 2 Configure SyncE to prefer the PTP receiver interface.

Example:

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

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

Example:

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

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

```
Router#show frequency synchronization interfaces brief

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

```
>S    TenGigE0/0/0/18          PRC    PRC    100 DNU    TenGigE0/0/0/19
>S    TenGigE0/0/0/19          PRC    PRC    100 PRC    TenGigE0/0/0/19
```

Verifying the Frequency Synchronization Configuration

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

1. **show frequency synchronization selection**

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

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

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

Selection point: ETH_RXMUX (1 inputs, 1 selected)
  Last programmed 3d04h ago, and selection made 3d04h ago
  Next selection points
```

```
    SPA scoped    : None
    Node scoped   : T0-SEL-B 1588-SEL
    Chassis scoped: None
    Router scoped : None
  Uses frequency selection
  S  Input                     Last Selection Point         QL  Pri  Status
  == ========================  ========================  =====  ===  ===========
  4  HundredGigE0/7/0/0        n/a                         PRC   10  Available
```

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

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

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

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

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

3. **show frequency synchronization interfaces brief**

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

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

Verifies the configuration. Note the following points:

- All line interface that have frequency synchronization configured are displayed.
- All clock interfaces and internal oscillators are displayed.

- Sources that have been nominated as inputs (in other words, have selection input configured) have ‘S’ in the Flags column; sources that have not been nominated as inputs do not have ‘S’ displayed.

Note Internal oscillators are always eligible as inputs.

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

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

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

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

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

Verifying the ESMC Configuration

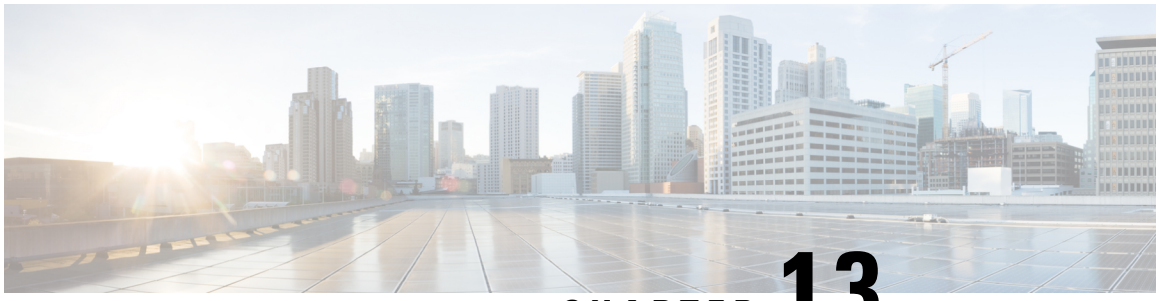
show frequency synchronization interfaces

```
Router# show frequency synchronization interfaces
                    Interface TenGigE0/0/0/0 (up)
                    Assigned as input for selection
                    Wait-to-restore time 0 minutes
                    SSM Enabled
Peer Up for 2d01h, last SSM received 0.320s ago
Peer has come up 1 times and timed out 0 times
ESMC SSMs Total Information Event DNU/DUS
```

```
Sent: HYPERLINK "tel:178479"178479 HYPERLINK "tel:178477"178477 2 HYPERLINK "tel:178463"178463

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

Verifying Controllers Timing LEDs

```
Router# show controllers timing led status location 0/RP0/CPU0
LED Status:
        BITS0: Off
        BITS1: Off
         Sync: Green
         GNSS: Off
          GPS: NA
```



CHAPTER 13

Network Synchronization Design Best Practices

This chapter provides guidelines and best practices to follow when designing timing requirements for your network.

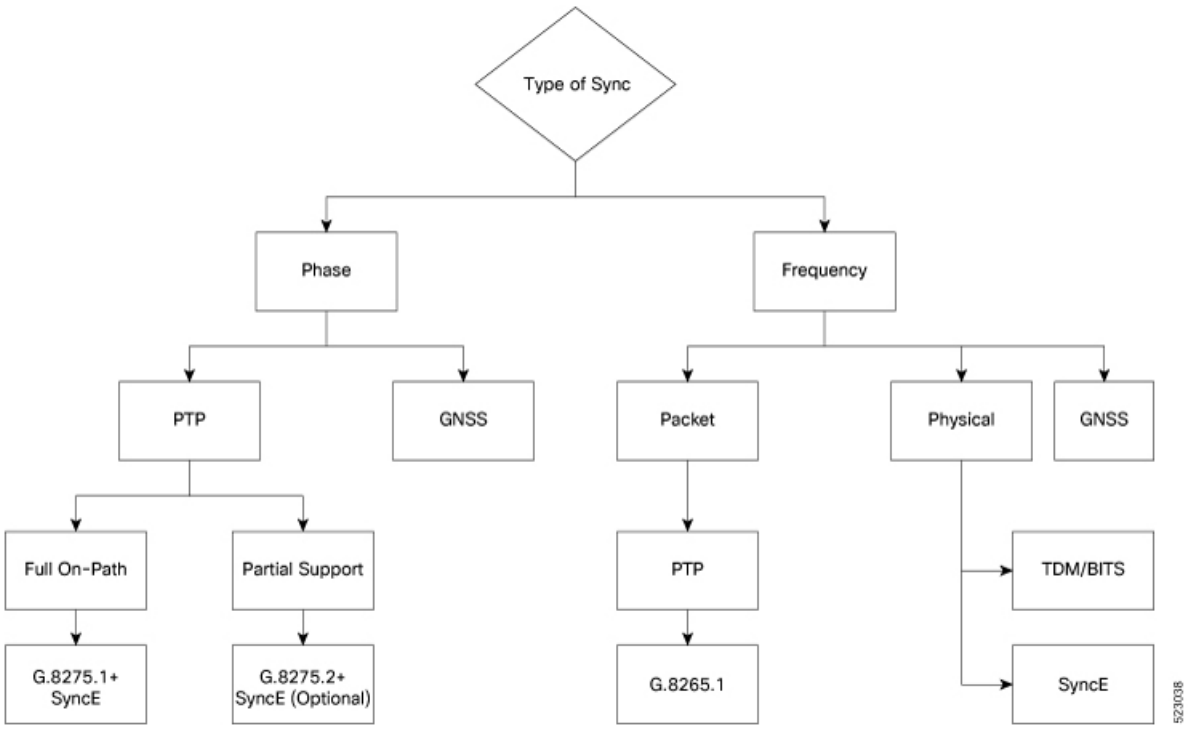
- Network Synchronization Design Best Practices, on page 207

Network Synchronization Design Best Practices

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

Network Synchronization Decision Tree

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



General Guidelines for Successful Synchronization Deployments

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

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

  For more information on SyncE and PTP, refer to *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.
- Set up the synchronization protocols that are required, which includes PTP, Network Time Protocol (NTP), or synchronous Ethernet.
  - NTP uses the system clock for logging events in the system, or to show clock output, whereas PTP and GNSS work on the IEEE 1588 hardware clock in the system.
  - The NTP clock of a node can't be used to synchronize the downstream network using PTP. However, a node can synchronize its NTP clock with the available PTP or GNSS clock.

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

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

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

  For more information on PTP Hybrid Mode, refer to *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.
- Reduce the number of hops:
  - Distribute sources of time to meet the budget. If you have too many hops, install a GNSS receiver further out into the network.
  - Don't centralize two Primary Reference Time Clocks (PRTC) and Telecom Grandmasters (T-GM) in two different locations and try to run a synchronization signal accurately across the whole network.
- Minimize Packet Delay Variation (PDV) and jitter. Ensure that microwaves, Gigabit-capable Passive Optical Networks (GPON), Digital Subscriber Line (DSL), and Dense Wavelength Division Multiplexing (DWDM) are PTP aware.
- Monitor your synchronization deployment to ensure that it's functioning correctly and meeting your desired level of accuracy.

  For more information, refer to Verifying the Frequency Synchronization Configuration in the *System Mangement Configuration Guide for Cisco NCS 5500 Series Routers*.
- Be aware of any relevant industry standards and practices when deploying synchronization.

Guidelines for Phase Synchronization Deployments

Follow these guidelines for phase synchronization deployments.

- Set up the necessary network infrastructure to support phase synchronization. It includes installing timing devices such as GPS receivers, synchronous Ethernet interfaces, and timing servers.

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

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

PTP over IP Network Design

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

- The placement of the telecom grandmaster (T-GM) clock plays an important role in ensuring that the network operates within your timing budget. For example, place a pair of T-GM clocks in a centralized location only if the network has a small number of hops. In larger networks with multiple hops, it may be necessary to distribute T-GM clocks throughout the network to ensure proper timing management at each hop.
- Use a dedicated frequency synchronization protocol such as synchronous Ethernet or 1588v2, which is designed specifically to maintain precise frequency synchronization between devices.

- Use the G.8265.1 standard. Frequency synchronization using the G.8265.1 standard is a way to make sure multiple devices on a network are operating at the same frequency, allowing for more accurate and reliable communication.
- Configure Quality of Service (QoS) policies to prioritize network traffic and reduce delays. This can be done by using traffic shaping, traffic policing, and queue management.

Selecting the Correct Profile For Network Synchronization

G.8275.1 PTPoE

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

For more information, refer to G.8275.1 in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.

G.8275.2 PTPoIP

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

For more information, refer to G.8275.2 in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.

Feature Adaptability on Each Profile

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

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

Feature	G.8275.1 PTPoE	G.8275.2 PTPoIP
PDV/Jitter	Reduced due to T-BC on every node	Optimal when deployed as a T-BC-P

Reducing Asymmetry

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

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

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

To reduce asymmetry in a PTP unaware network:

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

Reducing Packet Delay Variation

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

- Implement Telecom Boundary Clocks (T-BC) in the PTP unaware node. T-BC introduces a time reference to the PTP unaware node, which then synchronizes its clock with the T-BC.
- Use a high-quality network connection between the T-BC and the PTP unaware node. A high-quality network connection, such as a dedicated fiber link, can help reduce PDV due to network impairments.

Remediating Transport Asymmetry

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

- Ensure that your transport layer is PTP aware.

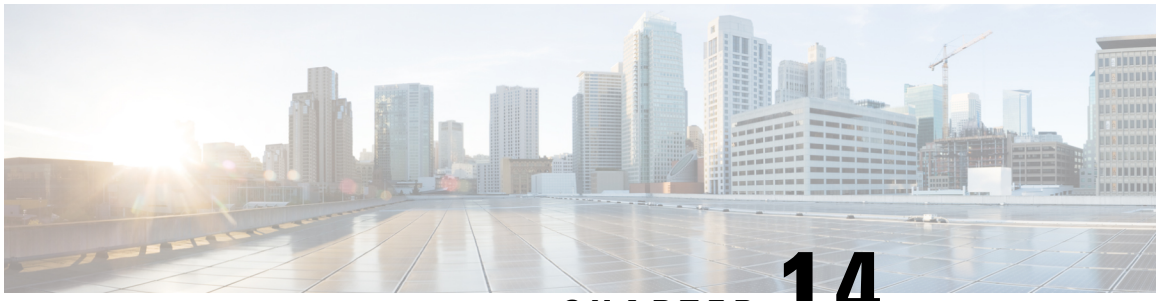
  In optical devices, use a wavelength division multiplexing (WDM) technology such as Optical Service Channel (OSC) for managing your fiber optic infrastructure effectively.

Synchronizing Across Networks

To avoid synchronization issues when connecting to other mobile networks:

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

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



CHAPTER 14

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

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

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

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

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

- Restrictions for Smart SFP, on page 215
- Configuring TPoP and CSoP, on page 217
- VPWS with Smart SFP, on page 219
- Multi Router Automatic Protection Switching, on page 219
- Field-Pluggable Device (FPD) Version Upgrade for Smart SFP, on page 221

Restrictions for Smart SFP

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

- CEM interface configuration isn't supported.
- E1 emulation is supported only on Ethernet pseudowire (VPWS).

- CSoP doesn't support E1-AIS alarm.
- No support to Single Router–Automatic Protection Switching (SR-APS)
- CLI configuration for the E1 controller on a VLAN needs to be mapped to an Ethernet sub-interface (by configuring same VLAN dot1q under the sub-interface). Any xconnect, also must be configured with this ethernet sub-interface.
- Multi Router-Automatic Protection Switching (MR-APS) is supported only by using the VLAN PW.
- Ensure that you have more than one MPLS paths, in core to convergence during core failure scenario.
- Only 8 smart SFPs are supported per router.
- ACR clocking is not supported in TPoP and CSoP unframed SFPs. Only framed to framed connection is supported, so not supported on framed to unframed connections.
- STM1 CSoP:
  - E1 Level shutdown is not supported.
  - Controller shutdown won't inject AIS but injects only LOS towards CE.
  - Bit error rate test (BERT) can be run only on one E1 channelized controller.
- CSoP and TPoP:
  - 25G ports are not supported.
  - Bit error rate is not supported.
- SF or SD threshold is not supported.
- Only 16-byte J0 is supported.
- BERT is not supported in unframed SFP.
- Loopback is supported only on, one of the 63 channels of CSoP SFP.
- Configuration with same ECID for CSoP E1s is not supported. ECID must be unique for each E1 under CSoP.
- The **show alarm conditions** command is not supported in Release 7.5.1.
- High convergence of 100ms is observed for MR-APS for LOS based switchover (for CSoP E1s).
- With smart SFP, high convergence of 4-6 minutes is observed in MR-APS for router reload based switchover.
- CSoP loopback on framed STM1-ch E1 doesn't work over **reload warm** command with smart SFP. Applicable only in Release 7.5.1.
- FPD upgrade is not supported for smart SFP. .
- LCV counter updates are not supported for smart SFP.

Configuring TPoP and CSoP

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

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

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

Table 14: Support on E1 Transmission

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

Table 15: Support on OC3-STM1 Transmission

Feature	OC3-STM1
E1 SATOP	STM-1 Channelized E1
Clock Configuration on Channelised-E1	ACR, DCR, internal, Line
E1 Channel BERT - System/Line channel prbs	Supported (Inverted-PRBS15)
PM-STM1 RS/MS	ES, SES, UAS Far End counters are NOT SUPPORTED
Threshold and its alerts	Supported
Alarms STM1	LOS, LOF, RS-TIM, MS-AIS, MS-RAI

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

Configuring Controller for PDH E1

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

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

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

Verifying Controller for PDH E1

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

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

Configuring Controller for STM1

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

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

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

Verifying Controller for STM1

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

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

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

Configuring Controller for STM1-ch E1

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

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

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

Verifying Controller for STM1-ch E1

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

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

VLAN ID: 200
ecid:1
```

VPWS with Smart SFP

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

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

Multi Router Automatic Protection Switching

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

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

Configuring Xconnect on Sub-Interface

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

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

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


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

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

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

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

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

Before you begin

To upgrade the FPD version on the Cisco NCS 5500 Series Routers, perform the following steps:

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

   Sample output for checking the current FPD version:

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

Thu Dec 15 06:47:08.068 UTC

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

-------------------------------------------------------------------------------------
0/0/1      NC55-MPA-4H-S         1.0   MPAFPGA              CURRENT     0.54      0.54

0/RP0      NCS-55A2-MOD-HD-S     1.0   MB-MIFPGA            NEED UPGD   0.19      0.19

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_12          NEED UPGD   7.01      7.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_13          CURRENT    13.01     13.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_17          NEED UPGD   7.01      7.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_OC3_STM1_0      CURRENT    12.01     12.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   Bootloader           CURRENT     1.18      1.18

0/RP0      NCS-55A2-MOD-HD-S     1.0   CPU-IOFPGA           CURRENT     1.27      1.27

0/RP0      NCS-55A2-MOD-HD-S     1.0   MB-IOFPGA            NEED UPGD   0.18      0.18

0/RP0      NCS-55A2-MOD-HD-S     1.0   SATA-M500IT-MU-A     CURRENT     5.00      5.00

0/PM0      NC55-900W-ACFW-HD     256.0 LIT-PriMCU-ACFW-I    CURRENT     1.04      1.04

0/PM1      NC55-900W-ACFW-HD           LIT-PriMCU-ACFW-I    NOT READY
```

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

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

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

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                          FPD Versions
```

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

-------------------------------------------------------------------------------------------
0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_12          30% UPGD    13.01
0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_4           CURRENT     13.01     13.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_STM1_TSOP_1     CURRENT     13.00     13.00

0/RP0      NCS-55A2-MOD-HD-S     0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      NCS-55A2-MOD-HD-S     0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      NCS-55A2-MOD-HD-S     0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
RP/0/RP0/CPU0:router# show hw-module fpd

Wed Dec 14 07:08:08.424 UTC

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

-------------------------------------------------------------------------------------------
0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-MIFPGA            CURRENT     0.05      0.05

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_12          75% UPGD    13.01
0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_4           CURRENT     13.01     13.01

0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_STM1_TSOP_1     CURRENT     13.00     13.00

0/RP0      NCS-55A2-MOD-HD-S     0.5   Bootloader           NEED UPGD   1.14      1.14

0/RP0      NCS-55A2-MOD-HD-S     0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07

0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-IOFPGA            NEED UPGD   0.23      0.23

0/RP0      NCS-55A2-MOD-HD-S     0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```

Procedure

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

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

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

b) Insert the Smart SFP on the same port.

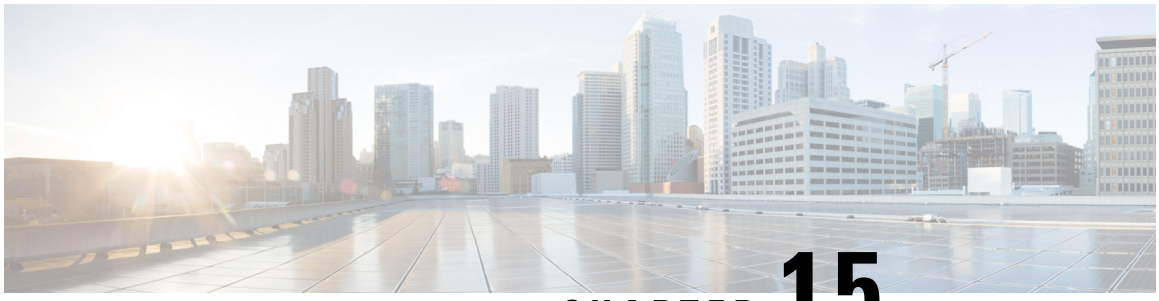
This step recreates the controller with all its configurations.

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

Example

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

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

Wed Dec 14 07:08:08.424 UTC

Auto-upgrade:Disabled
                                                                          FPD Versions
                                                                          ==============
Location   Card type              HWver FPD device       ATR Status    Running   Programd
-------------------------------------------------------------------------------------------
0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-MIFPGA            CURRENT     0.05      0.05
0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_12          CURRENT    13.01     13.01
0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_E1F_4           CURRENT    13.01     13.01
0/RP0      NCS-55A2-MOD-HD-S     1.0   SSFP_STM1_TSOP_1     CURRENT    13.00     13.00
0/RP0      NCS-55A2-MOD-HD-S     0.5   Bootloader           NEED UPGD   1.14      1.14
0/RP0      NCS-55A2-MOD-HD-S     0.5   CPU-IOFPGA           NEED UPGD   0.07      0.07
0/RP0      NCS-55A2-MOD-HD-S     0.5   MB-IOFPGA            NEED UPGD   0.23      0.23
0/RP0      NCS-55A2-MOD-HD-S     0.5   SATA-M500IT-MU-B     CURRENT     4.00      4.00
```



CHAPTER 15

Upgrading Field-Programmable Device

An FPD is a field programmable logic device which contains non-volatile, re-programmable memory to define its internal wiring and functionality. The contents of this non-volatile memory are called the FPD image or FPD firmware. Over the lifespan of an FPD, FPD firmware images may need upgrades for bug fixes or functionality improvements. These upgrades are performed in the field with minimum system impact.

- Prerequisites for FPD Image Upgrades, on page 225
- Overview of FPD Image Upgrade Support, on page 225
- FPD upgrade service, on page 226

Prerequisites for FPD Image Upgrades

- You must install the FPD pie before you install the SMUs or Service Packs. If you install the SMU or Service Packs before the FPD pie, the FPDs on the line card may not upgrade. In such cases, you must remove the SMUs and Service Packs and reload the router.
- When upgrading ASR 9006 router from a 32-bit IOS-XR to 64-bit IOS-XR, the corresponding RSPs and line cards must have ROMMON version 18.33 or later and a compatible FPD version (18.30 or later). If upgrading from a 32-bit IOS XR release, an intermediate upgrade (for example, IOS XR 7.1.2) may be required to update the line card ROMMON and FPD before proceeding to newer 64-bit IOS XR releases.

Overview of FPD Image Upgrade Support

An FPD image is used to upgrade the software on an FPD.

FPD versions must be compatible with the Cisco IOS XR software that is running on the router; if an incompatibility exists between an FPD version and the Cisco IOS XR software, the device with the FPGA may not operate properly until the incompatibility is resolved.

Note

- It is mandatory to upgrade all the required FPDs before doing a reload when you are upgrading FPDs on line cards. This is because, partial FPD component upgrades might result in booting errors (in some cases).
- You must not reload any line card or the router before all FPD image upgrades are completed successfully.

Note Cisco NCS5500 routers do not support auto upgrade for PSU FPDs.

FPD upgrade service

The main tasks of the FPD upgrade service are:

- Check FPD image version to decide if a specific firmware image needs an upgrade or not.
- Manual FPD Image Upgrade using the **upgrade hw-module fpd** command.
- Invoke the appropriate device driver with a name of the new image to load.

An FPD image package is used to upgrade FPD images. The **install activate** command is used to place the FPD binary files into the expected location on the boot devices.

Supported Upgrade Methods

Method	Remarks
Manual Upgrade	Upgrade using CLI, force upgrade supported.

Determining Upgrade Requirement

Use the **show hw-module fpd** command to determine if an FPD upgrade is required. Check for NEED UPGD in the Status column.

Example

```
Router: #show hw - module fpd

Wed Dec 14 07:08:08.424 UTC

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

0/0        NC55-18H18F           1.0   MIFPGA               NEED UPGD   7.01      7.01

0/0        NC55-18H18F           1.0   Bootloader           CURRENT     1.14      1.14
0/0        NC55-18H18F           1.0   IOFPGA               CURRENT     0.07      0.07
0/0        NC55-18H18F           1.0   SATA-M600-MCT        CURRENT     0.23      0.23
```

Use the **show fpd package** command to find out which FPGAs are supported with your current software release and minimum hardware requirements for each module.

Manual FPD Upgrade

Manual FPD upgrade is performed using the **upgrade hw-module fpd** command. All cards or all FPGA in a card can be upgraded. If reload is required to activate FPD, the upgrade should be complete. Line-cards, fabric cards and RP cards cannot be reloaded during the process of the FPD upgrade.

FPD upgrade is transaction-based:

- Each fpd upgrade CLI execution is one transaction.
- Only one transaction is allowed at any given time.
- One transaction may include one or many FPD upgrades

The **force** option can be used to forcibly upgrade the FPD (regardless of whether it is required or not). It triggers all FPDs to be upgraded or downgraded. The **force** option can also be used to downgrade or upgrade the FPGAs even after the version check.

Note

- Sometimes, FPDs can have primary and backup images.
- Force FPD upgrade with **upgrade hw-module location all fpd all force** command affects forwarding over BVI interface. You must reload involved locations to recover.
- The use of the **force** option when performing an FPD upgrade is not recommended except under explicit direction from Cisco engineering or TAC for a one-time purpose only.
- FPD upgrade should be performed in Admin mode only.
- A new FPD upgrade should be issued only when previous FPD upgrades have been completed on the same FPD with the following syslog message:

```
RP/0/RP0/CPU0:May 10 10:11:44.414 UTC: fpd-serv[205]: %INFRA-FPD_Manager-1-UPGRADE_ALERT
 : FPD Upgrade Completed (use "show hw-module fpd" to check upgrade status)
```

How to Upgrade FPD Images

You must determine if an FPD image upgrade is needed using the **show hw-module fpd** command and perform the upgrade, if needed, under the following circumstances:

- Migrate the software to a later Cisco IOS XR software release.
- Swap line cards from a system running a different Cisco IOS XR software release.
- Insert a new line card.

In the event of an FPD incompatibility with your card, you might receive the following error message:

```
LC/0/0/CPU0:Jul 5 03:00:18.929 UTC: optics_driver[220]: %L2-OPTICS-3-BAD_FPGA_IMAGE :
Detected bad MI FPGA image programmed in MI FPGA SPI flash in 0/0/CPU0 location: Failed to
 validate meta data CRC
LC/0/0/CPU0:Jul 5 03:00:19.019 UTC: optics_driver[220]: %L2-OPTICS-3-BACKUP_FPGA_LOADED :
Detected Backup FPGA image running on 0/0/CPU0 - primary image corrupted (@0x8c = 0x44)
RP/0/RP0/CPU0:Jul 5 03:00:48.987 UTC: fpd-serv[301]: %PKT_INFRA-FM-3-FAULT_MAJOR : ALARM_MAJOR
 :FPD-NEED-UPGRADE :DECLARE :0/0:
```

Upgrades to the Cisco IOS XR software might result in an FPD incompatibility. Ensure that you perform the FPD upgrade procedure and resolve all incompatibilities, for the cards to function properly.

Note The use of the **force** option when performing a FPD upgrade is not recommended except under explicit direction from Cisco engineering or TAC for a one-time purpose only.

Note Starting with Cisco IOS XR Release 24.1.1, line card reload after PSU FPD upgrade is no longer needed.

Before you begin

- Use the Admin console to run upgrade commands instead of the common console. Also, ensure that you reload from the Admin console and not from the common console.
- You must have a redundant PSU available before upgrading the FPD image for the PSU.
- The FPD upgrade procedure is performed while the card is online. At the end of the procedure the card must be reloaded before the FPD upgrade is complete. To reload the card, you can use the **hw-module location <location> reload** command in Admin mode, during the next maintenance window. The upgrade procedure is not complete until the card is reloaded.
- During the FPD upgrade, you *must not* do the following:
  - Reload, perform an online insertion and removal (OIR) of a line card (LC), or power down the chassis. Doing so may cause the node to enter an unusable state.
  - Press **Ctrl-C** if the console appears to hang without any output. Doing so may abort the upgrade.
- If you are not sure whether a card requires an FPD upgrade, you can install the card and use the **show hw-module fpd** command to determine if the FPD image on the card is compatible with the currently running Cisco IOS XR software release.

Procedure

	Command or Action	Purpose

Step 1	**show hw-module location** {**all** | *node-id*} **fpd**
	Example:
	`RP/0/RP0/CPU0:router# show hw-module location all fpd`
	or
	`RP/0/RP0/CPU0:router# show hw-module location 0/4/cpu0 fpd`
		Displays the current FPD image versions for the specified card or all cards installed in the router. Use this command to determine if you must upgrade the FPD image on your card.

Step 2	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters mode.
Step 3	(Optional) **show fpd package** **Example:**	Displays which cards are supported with your current Cisco IOS XR software release, which FPD image you need for each card, and what the minimum hardware requirements are for the various modules. (A minimum hardware

	Command or Action	Purpose
		requirement version of 0.0 indicates that all hardware can support this FPD image version.) If there are multiple FPD images for your card, use this command to determine which FPD image to use if you want to upgrade only a specific FPD type.

Step 4	**upgrade hw-module fpd** {**all** | *fpga-type*} [**force**] **location** [**all** | *node-id*]
	Example:
	`# upgrade hw-module fpd all location 0/3/1`
	`.`
	`.`
	`.`
	`Successfully upgraded 1 FPD for SPA-2XOC48POS/RPR on location 0/3/1`
		Upgrades all the current FPD images that must be upgraded on the specified card with new images.
		Before continuing to the next step, wait for confirmation that the FPD upgrade has successfully completed. Status messages, similar to these, are displayed to the screen until the FPD upgrade is completed:
		`FPD upgrade started.`
		`FPD upgrade in progress..`
		`FPD upgrade in progress..`
		`FPD upgrade sent to location xxxx`
		`FPD upgrade sent to location yyyy`
		`FPD upgrade in progress..`
		`FPD upgrade finished for location xxx`
		`FPD upgrade in progress..`
		`FPD upgrade finished for location yyyy`
		`FPD upgrade completed.`
		The “FPD upgrade in progress.” message is printed every minute. These logs are information logs, and as such, are displayed if the **logging console informational** command is configured.
		If Ctrl-C is pressed while the FPD upgrade is in progress, the following warning message is displayed:
		`FPD upgrade in progress on some hardware, aborting now is not recommended as it might cause HW programming failure and result in RMA of the hardware.`
		`Do you want to continue? [Confirm(y/n)]`
		If you confirm that you want to abort the FPD upgrade procedure, this message is displayed:
		`FPD upgrade process has been aborted, please check the status of the hardware and reissue the upgrade command if required.`
		Note
		• If your card supports multiple FPD images, you can use the **show fpd package** admin command to determine what specific image to upgrade in the **upgrade hw-module fpd** command.

	Command or Action	Purpose
		• A message is displayed when router modules cannot get upgraded during upgrade with **location all** option indicating that the FPGA is intentionally skipped during upgrade. To upgrade such FPGAs, you can use the CLI command with a particular location explicitly specified. For example, **upgrade hw-module fpd all location 0/3/1**. • It is recommended to upgrade all FPGAs on a given node using the **upgrade hw-module fpd all location** {**all** | *node-id*} command. Do not upgrade the FPGA on a node using the **upgrade hw-module fpd** <*individual-fpd*> **location** {**all** | *node-id*} as it may cause errors in booting the card.
Step 5	**exit** **Example:** `sysadmin-vm:0_RP0# exit`	
Step 6	**hw-module location**{ *node-id* | **all** } **reload**	Use the **hw-module location reload** command to reload a line card. `sysadmin-vm:0_RP0# hw-module location 0/3 reload`
Step 7	**exit**	
Step 8	**show hw-module fpd**	Verifies that the FPD image on the card has been successfully upgraded by displaying the status of all FPDs in the system.

Configuration Examples for FPD Image Upgrade

The following examples indicates the use of commands associated with the FPD image upgrade procedure.

show fpd package Command Output: Example

Use the **show fpd package** command in System Admin EXEC mode to find out which line cards are supported with your current Cisco IOS XR software release, which FPD image package you need for each line card, and what the minimum hardware requirements are for each module. If multiple FPD images are available for your card, they are listed as Subtype fpga2, fpga3, and so on.

Note The FPD name used in the FPD Description column of the output of the `show fpd package` command includes the last ten characters of DCO-PID. Depending on the slot and port numbers, the FPD name is appended with DCO_0, DCO_1, or DCO_2. For example, the FPD names for `CFP2-WDM-D-1HL` in port 0 and port 1 are `-WDM-D-1HL_DCO_0` and `WDM-D-1HL_DCO_1` respectively.

The following example shows sample output from the **show fpd package** command:

```
show fpd package
Tue Jan 22 13:56:00.212 UTC

================================ ==============================================
                                        Field Programmable Device Package
                                 ==============================================
                                                Req     SW      Min Req   Min Req
Card Type            FPD Description            Reload  Ver     SW Ver  Board Ver
=================== ========================== ====== ======= ======== =========
-------------------------------------------------------------------------------
NC55-1200W-ACFW      LIT-PriMCU-ACFW(A)         NO      2.09    2.09    0.0
-------------------------------------------------------------------------------
NC55-900W-ACFW-I     LIT-PriMCU-ACFW-I(A)       NO      1.04    1.04    0.0
-------------------------------------------------------------------------------
NC55-900W-DCFW-I     LIT-PriMCU-DCFW-I(A)       NO      2.260   2.260   0.0
-------------------------------------------------------------------------------
NC55-930W-DCFW-C     LIT-PriMCU-DCFW-C(A)       NO      2.259   2.259   0.0
-------------------------------------------------------------------------------
NC55-MPA-12T-S       MPAFPGA                    YES     0.27    0.27    0.0
-------------------------------------------------------------------------------
NC55-MPA-1TH2H-S     -WDM-D-1HL_DCO_2           NO     38.518  38.518   0.1
                     MPAFPGA                    YES     0.53    0.53    0.0
                     WDM-DE-1HL_DCO_2           NO     38.518  38.518   0.1
                     WDM-DS-1HL_DCO_2           NO     38.268  38.268   0.1
-------------------------------------------------------------------------------
NC55-MPA-2TH-HX-S    -WDM-D-1HL_DCO_0           NO     38.518  38.518   0.1
                     -WDM-D-1HL_DCO_1           NO     38.518  38.518   0.1
                     MPAFPGA                    YES     0.53    0.53    0.0
                     WDM-DE-1HL_DCO_0           NO     38.518  38.518   0.1
                     WDM-DE-1HL_DCO_1           NO     38.518  38.518   0.1
                     WDM-DS-1HL_DCO_0           NO     38.268  38.268   0.1
                     WDM-DS-1HL_DCO_1           NO     38.268  38.268   0.1
-------------------------------------------------------------------------------
NC55-MPA-2TH-S       -WDM-D-1HL_DCO_0           NO     38.518  38.518   0.1
                     -WDM-D-1HL_DCO_1           NO     38.518  38.518   0.1
                     MPAFPGA                    YES     0.53    0.53    0.0
                     WDM-DE-1HL_DCO_0           NO     38.518  38.518   0.1
                     WDM-DE-1HL_DCO_1           NO     38.518  38.518   0.1
                     WDM-DS-1HL_DCO_0           NO     38.268  38.268   0.1
                     WDM-DS-1HL_DCO_1           NO     38.268  38.268   0.1
-------------------------------------------------------------------------------
NC55-MPA-4H-HD-S     MPAFPGA                    YES     0.53    0.53    0.0
-------------------------------------------------------------------------------
NC55-MPA-4H-HX-S     MPAFPGA                    YES     0.53    0.53    0.0
-------------------------------------------------------------------------------
NC55-MPA-4H-S        MPAFPGA                    YES     0.53    0.53    0.0
-------------------------------------------------------------------------------
NC55A2-MOD-SE-H-S    Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     1.18    1.18    0.1
                     MB-IOFPGA(A)               YES     0.18    0.18    0.1
                     MB-MIFPGA                  YES     0.19    0.19    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
-------------------------------------------------------------------------------
NCS-55A2-MOD-HD-S    Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     1.18    1.18    0.1
                     MB-IOFPGA(A)               YES     0.18    0.18    0.1
                     MB-MIFPGA                  YES     0.19    0.19    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
-------------------------------------------------------------------------------
NCS-55A2-MOD-HX-S    Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     1.18    1.18    0.1
                     MB-IOFPGA(A)               YES     0.18    0.18    0.1
                     MB-MIFPGA                  YES     0.19    0.19    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
```

```
--------------------------------------------------------------------------------
NCS-55A2-MOD-S       Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     1.18    1.18    0.1
                     MB-IOFPGA(A)               YES     0.18    0.18    0.1
                     MB-MIFPGA                  YES     0.19    0.19    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
--------------------------------------------------------------------------------
NCS-55A2-MOD-SE-S    Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     1.18    1.18    0.1
                     MB-IOFPGA(A)               YES     0.18    0.18    0.1
                     MB-MIFPGA                  YES     0.19    0.19    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
                     STATSFPGA                  YES     0.01    0.01    0.0
```

This table describes the significant fields shown in the display:

Table 16: show fpd package Field Descriptions

Field	Description
Card Type	Module part number.
FPD Description	Description of all FPD images available for the line card.
Type	Hardware type. Possible types can be: • spa—Shared port adapter • lc—Line card
Subtype	FPD subtype. These values are used in the **upgrade hw-module fpd** command to indicate a specific FPD image type to upgrade.
SW Version	FPD software version recommended for the associated module running the current Cisco IOS XR software.
Min Req SW Vers	Minimum required FPD image software version to operate the card. Version 0.0 indicates that a minimum required image was not programmed into the card.
Min Req HW Vers	Minimum required hardware version for the associated FPD image. A minimum hardware requirement of version 0.0 indicates that all hardware can support this FPD image version.

upgrade hw-module fpd Command Output: Example

Use the **upgrade hw-module fpd** command to upgrade the FPD image on a line card. The upgrade can be executed for all FPDs or for specific FPDs that need an upgrade. To upgrade all FPDs, use **upgrade hw-module fpd all location all** command. To upgrade a specific FPD image type, use the FPD subtype value in the **upgrade hw-module fpd** command.

show platform Command Output: Example

Use the **show platform** command to verify that the line card is up and running.

Auto FPD Upgrade

Table 17: Feature History Table

Feature Name	Release Information	Feature Description
Auto FPD Upgrade	Release 7.3.2	This functionality enables automatic upgrade and reload for field-programmable devices (FPDs) whenever the Cisco IOS XR image has a newer FPD version. This functionality upgrades all route processors and line card FPDs simultaneously while displaying upgrade triggers on the console.

Effective Cisco IOS XR Release 7.3.2, you can enable automatic upgrade of FPD by using the "fpd auto-upgrade enable" command.

To automatically upgrade all FPDs, use:

```
RP/0/RP0/CPU0:IOS(config)#fpd auto-upgrade enable
```

To reload the interface modules following the fpd auto-upgrade, use:

```
RP/0/RP0/CPU0:IOS(config)#fpd auto-reload enable
```

Limitations and Usage Guidelines

Limitations

- FPD auto-upgrade should be enabled only in the XR VM and *not* in the System Admin VM.
- With auto-upgrade enabled, if any card is in RELOAD REQUIRED state, auto-upgrade is re-triggered during any SSO or FPD-serv process restart.
- When an interface module (IM) or route processor (RP) is in RELOAD REQUIRED state and auto-upgrade is enabled, FPD upgrades are triggered again.
- With auto-upgrade enabled, if line card is inserted, an auto-upgrade is triggered. During this phase optics alarms are generated. If auto-reload is not enabled, you must reload the line cards manually to clear these alarms.
- SATA allows you to upgrade or downgrade when an FPD version change is available. Therefore, when auto-upgrade is enabled, the system automatically downgrades if lower versions are available. This behavior is specific only to SATA FPDs.
- FPD auto-reload is applicable for line cards only. Line cards are automatically reloaded after the fpd auto-upgrade process is completed.
- You must disable auto-upgrade during XR ISSU; otherwise, the router goes into a state where redundancy cannot be achieved. In this case, standby RP must be reloaded to achieve redundancy.
- Cisco NCS 5500 Series Routers do not support ISSU.
- TimingICs do not support **auto fpd upgrade** on NCS5500 Series Routers as the TimingIC requires a card reload immediately after upgrade. For the same reason, the TimingICs are not upgraded if the user

specifies **location all** in the **auto fpd upgrade** command. To upgrade a TimingIC FPD, specify the FPD name along with the card location. For example, **upgrade hw-module fpd TimngIC-A location 0/RP0/CPU0**

- Auto FPD upgrade is not supported on the following line cards that support QDD-400G-ZR-S and QDD-400G-ZRP-S modules:
  - NC57-24DD
  - NC57-18DD-SE
  - NC57-36H6D-S
  - NC57-48Q2D-S
  - NC57-MPA-2D4H-S
  - NC57-MOD-S
  - NC57-MPA-1FH1D-S

Usage Guidelines—Online Insertion of Line Cards

When a line card with a lower FPD version is inserted, one of the following scenarios apply:

- If fpd auto-upgrade and auto-reload are enabled, and a new line card is inserted, the system upgrades the line card FPDs automatically with the latest FPDs and reloads the line cards.
- If fpd auto-upgrade and auto-reload are both disabled, no action is required.
- If fpd auto-upgrade is enabled and auto-reload is disabled, the following alarms are displayed on the console:

```
RP/0/RP1/CPU0:Jun 1 10:05:46.095 UTC: optics_driver[231]: %PKT_INFRA-FM-3-FAULT_MAJOR
: ALARM_MAJOR :OPTICS SUPPORTED_ERROR :DECLARE : Optics0/5/0/6: Optics0/5/0/6
RP/0/RP1/CPU0:Jun 1 10:05:46.096 UTC: optics_driver[231]: %PKT_INFRA-FM-2-FAULT_CRITICAL
 : ALARM_CRITICAL :OPTICS NOT SUPPORTED :DECLARE : Optics0/5/0/6: Optics0/5/0/6
```

  You must reload the line cards manually to clear these alarms

Usage Guidelines—Online Insertion of RPs

When fpd auto-upgrade is enabled and a new RP is inserted, the system upgrades the RP FPDs automatically with the latest FPDs.

Note RPs are not reloaded automatically. You must manually reload the RP or chassis for the latest FPD version to reflect.

Note Reload of active RPs and line cards impacts the network traffic.

Table 18: Action Required on FPDs After Auto Upgrade

FPD	Action Required
IOFPGA	Manual reload required
ADM	Upgraded version available immediately
PRIMARY-BIOS	Manual reload required
SATA	Upgraded version available immediately
PSOC	Upgraded version available immediately
IMFPGA	Manual reload required, if auto-reload is not configured

Automatic FPD Upgrade for PSU

During the Power Supply Unit (PSU) insertion and installation process, the routers can now automatically upgrade the Field-Programmable Devices (FPD) associated with the PSUs.

Starting with Cisco IOS-XR Release 7.5.2, the automatic FPD upgrade includes the FPDs associated with the PSUs by default. This means that when automatic FPD upgrade is enabled, the FPDs associated with the PSUs will also be upgraded. The upgrades for the PSUs will occur sequentially, so the FPD upgrades for the PSUs will take longer than for other components.

You can choose to exclude PSUs from the automatic upgrade process to reduce the time taken for FPD automatic upgrade by preventing them from being upgraded upon insertion or during a system upgrade using the **fpd auto-upgrade exclude pm** command.

Configuration example for excluding PSUs from automatic FPD upgrade:

Configuration

```
Router# config
Router(config)# fpd auto-upgrade enable
Router(config)# fpd auto-upgrade exclude pm
Router(config)# commit
```

Show Running Configuration

```
Router# show running-config fpd auto-upgrade
fpd auto-upgrade enable
fpd auto-upgrade include pm
```

Upgrade Failure

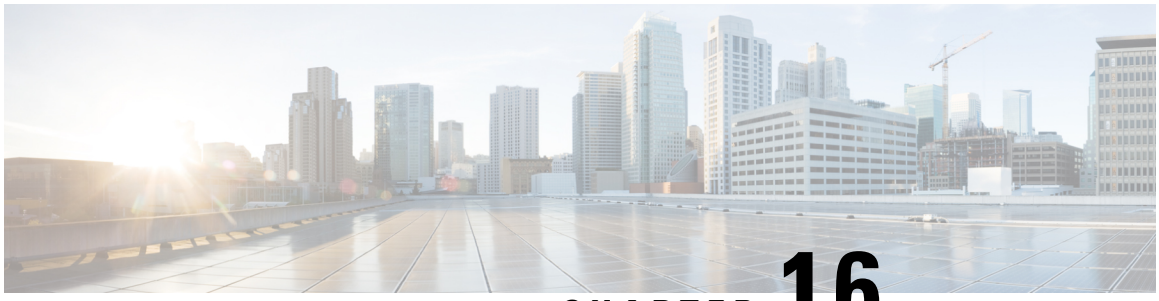
On failure of an FPD upgrade, you get a warning with the following syslog message:

```
LC/0/5/CPU0:Jun 27 05:02:25.742 UTC: optics_driver[216]: %INFRA-FPD_Driver-1-UPGRADE_ALERT
 : FPD MIFPGA@0/5 image programming completed with UPGD FAIL state Info: [Image verification
 failed at offset 0x5c8, flash value = 0x0, image value = 0x40, image size = 4194304]
LC/0/5/CPU0:Jun 27 05:02:26.570 UTC: optics_driver[216]: %INFRA-FPD_Driver-1-UPGRADE_ALERT
 : FPD MIFPGA@0/5 image programming completed with UPGD FAIL state Info: [Image verification
 failed at offset 0x1e, flash value = 0x56, image value = 0xff, image size = 4194304]
```

When you use the **show hw-module fpd** command, the status column displays **UPGD FAIL** to indicate failure of the FPD upgrade.

Note

- Do not reload the line card with a failed FPD upgrade image.
- Upgrade failed FPDs will be fixed with a manual upgrade.
- Contact Cisco TAC or your account representative if the FPD upgrade failure is not repaired.



CHAPTER 16

Configuration and File System Management

This module describes methods for configuration management and file transfer enhancements.

- Auto-Save Configuration, on page 237
- Increasing Commit Limit, on page 237

Auto-Save Configuration

You can configure the router to automatically take the backup of the running configuration by using **configuration commit auto-save** command. This auto-save feature saves the configuration to the specified location on the router after every **commit** is made. These auto-save files are stored in the form of Linux files.

Configure Auto-Save

Use the **configuration commit auto-save** command to auto save the configuration.

```
Router#configure
Router(config)#configuration commit auto-save
Router(config-cfg-autosave)#commit
```

When filename is accessed through VRF, you can specify filename in **filename** <protocol>://<user>@<host>:<port>;<vrf name>/<url-path>/<file-name> format.

Increasing Commit Limit

Table 19: Feature History Table

Feature Name	Release Information	Feature Description
Increasing Commit Limit on NCS 5700 fixed port routers	Release 24.2.11	Introduced in this release on: NCS 5700 fixed port routers This feature support is now extended to NCS 5700 fixed port routers.

Feature Name	Release Information	Feature Description
Increasing Commit Limit	Release 24.2.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards). The maximum number of commits is increased in the router that allows you to configure complex topology changes without interruptions caused by the default blocking of commit changes during rebase or ASCII backup operations. You can prevent the commit operation from getting blocked by using the **cfs check** command, which increases the commit (pacount) count from 20 to 40, and the commit file diff size (configuration data) from 2 MB to 4 MB, and by using the **clear configuration ascii inconsistency** command, which performs an ASCII backup after 55 minutes. The feature modifies the following commands: • **cfs check** • **clear configuration ascii inconsistency**

The Cisco IOS XR Routers use a two-stage configuration model. The first stage is target configuration, where you build the configurations using the necessary commands in the command line interface. The second stage is the commit, where the configuration made in the target stage is added to the router configuration using the **commit** command. After each commit, the router generates a file for the newly configured changes and adds it to its running configuration, making it an integral part of the running configuration.

Note This target configuration doesn’t impact the router's running configuration.

The Cisco IOS XR routers perform rebase and ASCII backup operations to maintain the real time configuration in the backup copy. The rebase and ASCII backup operations block you from committing configurations to the router.

Note Starting with Release 24.3.1, the rebase operation no longer blocks the commit operation.

This allows you to configure complex topology changes without being interrupted by the default blocking of commit changes during the rebase operation. For more information, see the section Concurrent Configuration Rebase during Commit, on page 241.

In rebase, the router automatically saves your changes to the backup binary configuration file after 20 commits, or 2 MB of configuration data. The router blocks the commit while saving the configuration to the backup file. The router takes a few seconds to complete the rebase operation, during which, if you terminate the CLI session, the router loses the target configurations in the blocked commit.

In ASCII backup, the router automatically saves a copy of its running configuration in the ASCII format. This backup process takes place if there has been a commit to the router configuration and when the ASCII backup timer completes a 55-minute window after the previous backup event. However, if there was no commit when the ASCII backup timer completes 55 minutes, the counter is reset without any backup. During the ASCII backup, the router blocks the configuration commits.

Starting with Release 24.2.1, we have made the following enhancements:

- You can use the **cfs check** command to increase the rebase limits in the router from 20 to 40 commits and the configuration data from 2 MB to 4 MB. When configuring the router, you can check the current commit count and configuration data size using the **show cfgmgr commitdb** command. If the commit count is 20 or higher, or the configuration data size is 2 MB or above, the router initiates a rebase within 10 seconds. By using the **cfs check** command to increase the commit count to 40 and the configuration data to 4 MB, you can commit without delay.
- You can use the **clear configuration ascii inconsistency** command to perform an ASCII backup and reset the ASCII backup timer to zero. Once the backup is complete, the router will automatically initiate the next periodic ASCII backup operation only after 55 minutes from the time the **clear configuration ascii inconsistency** command is executed.

Guidelines and Restrictions for Increasing the Commit Limit

- The **cfs check** command increases the rebase limits only for one instance. After executing the **cfs check** command, the router will perform a rebase operation after 40 commits or when the configuration data reaches 4 MB. Once the router performs a rebase operation, the limits will reset to the default values of 20 commits and 2 MB configuration data. To enable 40 commits and 4 MB configuration data, you must perform the **cfs check** command again.
- After executing the **cfs check** command, if a router switches over to standby RP, the rebase limits are retained as 40 commits and configuration data of 4 MB. However, if the router reloads, the rebase limits are reset to 20 commits and 2 MB of configuration data. For example, after executing the **cfs check** command, if the router switches over to standby RP after 30 commits, it will still have ten more commits before a rebase. However, if the router reloads, the rebase limits are reset to default 20 commits and 2 MB of configuration data.
- The **clear configuration ascii inconsistency** command initiates an ASCII backup and resets the ASCII backup timer count to zero. Following this, the router will automatically initiate the next periodic ASCII backup operation only after 55 minutes from the time **clear configuration ascii inconsistency** command is executed. For example, if you execute a commit operation after executing a **clear configuration ascii inconsistency** command, the router will perform an ASCII backup operation 55 minutes after the**clear**

configuration ascii inconsistency command was executed, and merge the new commit into ASCII backup. Hence, before the next 55 minutes, you must execute the **clear configuration ascii inconsistency** command again to reset the ASCII backup timer to zero.

- When the router enters standby mode or reloads, the ASCII timer does not reset to zero, and the router performs an ASCII backup operation 55 minutes after the first commit operation before the standby mode or reload.
- Cisco does not recommend executing **clear configuration inconsistency** and **clear configuration ascii inconsistency** commands regularly after each commit, as it causes hard disk wear and tear. You should execute these commands only before a commit or sequence of commits that must be done within a specific timeframe and without being delayed by rebase and ASCII backup operations. As these commands perform disk input and output operations in the background, frequent execution of these commands causes frequent access to the hard disk, which increases the wear and tear on the hard disk.

Increasing the Rebase Limits

You can increase the rebase limits as follows:

1. Use the **cfs check** command to increase the commit count to 40 and the configuration data to 4 MB.

```
Router# cfs check
Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing commit database with running configuration...OK
```

2. Verify if the **cfs check** command is executed using the **show configuration history** command.

```
Router# show configuration history last 5
Sno.  Event      Info                          Time Stamp
~~~~  ~~~~~      ~~~~                          ~~~~~~~~~~
1     cfs check  completed                     Wed Jan 10 11:42:21 2024
2     commit     id 1000000001                 Wed Jan 10 11:39:26 2024
3     startup    configuration applied         Wed Jan 10 11:39:02 2024
```

Perform ASCII Backup and Rest ASCII Backup Timer

You can perform ASCII backup and rest ASCII backup timer as follows:

1. Use the **clear configuration ascii inconsistency** command to perform ASCII backup at that instance and reset the ASCII backup timer count to zero.

```
Router# clear configuration ascii inconsistency
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! It is recommended to run this command only when all nodes in router      !!!!
!!!! are in IOS-XR RUN state. To determine node state, run following command: !!!!
!!!! 'show platform'.                                                         !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Proceed with the command ?[confirm] y
 Ascii configuration backup is in progress...
Configuration ascii backup complete
```

2. Verify if the **clear configuration ascii inconsistency** command is executed using the **show configuration history** command.

```
Router# show configuration history last 5
Sno.  Event      Info                          Time Stam
~~~~  ~~~~~      ~~~~                          ~~~~~~~~~~
```

```
1      backup      Periodic ASCII backup          Wed Jan 10 11:48:20 2024
2      cfs check   completed                      Wed Jan 10 11:42:21 2024
3      commit      id 1000000001                  Wed Jan 10 11:39:26 2024
4      startup     configuration applied          Wed Jan 10 11:39:02 2024
```

Concurrent Configuration Rebase during Commit

Table 20: Feature History Table

Feature Name	Release Information	Feature Description
Concurrent Configuration Rebase during Commit	Release 24.3.1	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) The router performs the commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation. This removes the need to use the **cfs check** command to increase the commit count and the commit file diff size.

Cisco IOS XR routers use a two-stage configuration model. In the first stage, configurations are built using necessary commands in the command line interface, and in the second stage, the configurations are committed to the router.

During rebase and ASCII backup operations, the router blocks configuration commits. However, the "Concurrent Configuration Rebase during Commit" feature allows the router to perform commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation.

The Cisco IOS XR routers perform rebase and ASCII backup operations to maintain the real time configuration in the backup copy.

Before Release 24.3.1,

- The rebase and ASCII backup operations block you from committing configurations to the router.
- You can increase the maximum number of commits and reset the ASCII backup timer to allow the router to configure complex topology changes without interruptions caused by the default blocking of commit changes during rebase or ASCII backup operations. For more information, see the section Increasing Commit Limit, on page 237.

From Release 24.3.1,

- The router performs the commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation. This removes the need to use the **cfs check** command to increase the commit count and the commit file diff size.

- However, the ASCII backup operations still block the commit operation. You can reset the ASCII backup timer using the **clear configuration ascii inconsistency** command. This allows the router to perform an ASCII backup after 55 minutes and perform commit operations without being blocked by ASCII backup operations. For more information on ASCII backup, see the section Increasing Commit Limit, on page 237.