



System Management Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x

First Published: 2017-09-01

Last Modified: 2018-03-30

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 NON-INFRINGEMENT 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)

© 2018 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 6.3.x 1

CHAPTER 2

Configuring Manageability 3

Information about XML Manageability 3

How to Configure Manageability 3

Configuring the XML Agent 3

Configuration Examples for Manageability 4

Enabling VRF on an XML Agent: Examples 4

CHAPTER 3

Configuring Physical and Virtual Terminals 7

Prerequisites for Implementing Physical and Virtual Terminals 7

Information About Implementing Physical and Virtual Terminals 7

Line Templates 7

Line Template Configuration Mode 8

Line Template Guidelines 8

Terminal Identification 9

vtty Pools 9

How to Implement Physical and Virtual Terminals on Cisco IOS XR Software 9

Modifying Templates 9

Creating and Modifying vtty Pools 11

Monitoring Terminals and Terminal Sessions 13

Configuration Examples for Implementing Physical and Virtual Terminals	14
--	----

CHAPTER 4

Configuring Simple Network Management Protocol 17

Prerequisites for Implementing SNMP	17
Restrictions for SNMP use on Cisco IOS XR Software	17
Information about Implementing SNMP	18
SNMP Functional Overview	18
SNMP Manager	18
SNMP Agent	18
MIB	18
SNMP Versions	20
Comparison of SNMPv1, v2c, and v3	20
Security Models and Levels for SNMPv1, v2, v3	21
SNMPv3 Benefits	22
SNMPv3 Costs	22
User-Based Security Model	23
View-Based Access Control Model	23
IP Precedence and DSCP Support for SNMP	24
Session MIB support on subscriber sessions	24
SNMP Notifications	24
Session Types	25
How to Implement SNMP on Cisco IOS XR Software	25
Configuring SNMPv3	26
Configure to Drop Error PDUs	28
Configuring SNMPv3: Examples	29
Configuring SNMP Trap Notifications	32
Configure to Drop Error PDUs	34
Configuring Trap Notifications: Example	35
Setting the Contact, Location, and Serial Number of the SNMP Agent	36
Defining the Maximum SNMP Agent Packet Size	37
Changing Notification Operation Values	38
Setting IP Precedence and DSCP Values	39
Setting an IP Precedence Value for SNMP Traffic: Example	40
Setting an IP DSCP Value for SNMP Traffic: Example	41

Displaying SNMP Context Mapping	41
Monitoring Packet Loss	41
Configuring MIB Data to be Persistent	42
Configuring LinkUp and LinkDown Traps for a Subset of Interfaces	43

CHAPTER 5

Configuring Object Tracking 47

Configuring Object Tracking	47
Prerequisites for Implementing Object Tracking	47
Information about Object Tracking	48
How to Implement Object Tracking	48
Tracking the Line Protocol State of an Interface	48
Tracking IP Route Reachability	50
Building a Track Based on a List of Objects	51
Building a Track Based on a List of Objects - Threshold Percentage	53
Building a Track Based on a List of Objects - Threshold Weight	55
Tracking IPSLA Reachability	57
Configuration Examples for Configuring Object Tracking	58
Additional References	60

CHAPTER 6

Configuring Cisco Discovery Protocol 63

Prerequisites for Implementing CDP	63
Information About Implementing CDP	63
How to Implement CDP on Cisco IOS XR Software	65
Enabling CDP	65
Modifying CDP Default Settings	66
Monitoring CDP	67
Examples	68
Configuration Examples for Implementing CDP	71

CHAPTER 7

Configuring Periodic MIB Data Collection and Transfer 73

Prerequisites for Periodic MIB Data Collection and Transfer	73
Information About Periodic MIB Data Collection and Transfer	73
SNMP Objects and Instances	73
Bulk Statistics Object Lists	74

Bulk Statistics Schemas	74
Bulk Statistics Transfer Options	74
Benefits of Periodic MIB Data Collection and Transfer	74
How to Configure Periodic MIB Data Collection and Transfer	75
Configuring a Bulk Statistics Object List	75
Configuring a Bulk Statistics Schema	76
Configuring Bulk Statistics Transfer Options	78
Periodic MIB Data Collection and Transfer: Example	81

CHAPTER 8

Configuring Flexible Command Line Interface	83
Flexible CLI Configuration Groups	83
Flexible Configuration Restrictions	83
Configuring a Configuration Group	85
Simple Configuration Group: Example	86
Configuration Group Applied to Different Places: Example	87
Verifying the Configuration of Configuration Groups	87
Regular Expressions in Configuration Groups	89
Configuration Examples Using Regular Expressions	96
Configuration Group with Regular Expression: Example	96
Configuration Group Inheritance with Regular Expressions: Example	98
Layer 2 Transport Configuration Group: Example	99
Configuration Group Precedence: Example	99
Changes to Configuration Group are Automatically Inherited: Example	100
Configuration Examples for Flexible CLI Configuration	100
Basic Flexible CLI Configuration: Example	100
Interface MTU Settings for Different Interface Types: Example	102
ACL Referencing: Example	104
Local Configuration Takes Precedence: Example	105
ISIS Hierarchical Configuration: Example	106
OSPF Hierarchy: Example	110
Link Bundling Usage: Example	113

CHAPTER 9

Configuring Network Time Protocol	115
Prerequisites for Implementing NTP on Cisco IOS XR Software	115

Information About Implementing NTP	115
NTP-PTP Interworking	117
Configuring Poll-Based Associations	117
Configuring Broadcast-Based NTP Associates	119
Configuring NTP Access Groups	121
Configuring NTP Authentication	123
Disabling NTP Services on a Specific Interface	125
Configuring the Source IP Address for NTP Packets	126
Configuring the System as an Authoritative NTP Server	128
Configuring NTP-PTP Interworking	129
Updating the Hardware Clock	131
Verifying the Status of the External Reference Clock	132
Examples	133
Configuration Examples for Implementing NTP	134
Configuring NTP server inside VRF interface	137

CHAPTER 10

Configuring Precision Time Protocol	139
PTP Overview	139
Restrictions for PTP	142
PTP Support Information	142
Timing Hardware Support Matrix	143
ITU-T Telecom Profiles for PTP	144
G.8265.1	145
G.8275.1	146
Configuring PTP	147
Configuring Global G.8275.1 Profile	147
Configuring PTP Master Interface	148
Configuring PTP Slave Interface	149
Configuring PTP Hybrid Mode	149
Configuring PTP Telecom Profile Interface	151
Configuring PTP Telecom Profile Clock	153
Configuration Examples	155
Slave Configuration Example	155
Master Configuration Example	155

PTP Hybrid Mode Configuration Example	155
ITU-T Telecom Profile Examples:	156
G.8265.1 Profile Configuration Examples	156
G.8275.1 Profile Configuration Examples	157

CHAPTER 11
Configuring Smart Licensing 161

What is Smart Licensing?	161
What is Flexible Consumption Model?	162
How Does Smart Licensing Work?	166
What is Cisco Smart Software Manager?	167
Smart Licensing Deployment Options	167
Configuring Smart Licensing	169
Prerequisites for Configuring Smart Licensing	169
Setting up the Router for Smart Licensing	169
Configuring a Communications Connection Between the Router and Cisco Smart Software Manager	170
Configuring a Direct Cloud Connection	170
Configuring a Connection Through an HTTP Proxy	171
Connecting to CSSM On-Premise	174
Installing CSSM On-Premise	176
Registering and Activating Your Router	176
Generating a New Token from CSSM	176
Registering Your Device With the Token	179
Renewing Your Smart Licensing Registration	180
Deregistering Your Router from CSSM	180
Verifying the Smart Licensing Configuration	181
Smart Licensing Configuration Examples	183
Example: Viewing the Call Home Profile	183
Example: Viewing License Information Before Registration	183
Example: Registering the Router	186
Example: Viewing License Information After Registration	186

CHAPTER 12
Configuring Zero Touch Provisioning 189

Manual ZTP Invocation	191
-----------------------	-----

[ZTP Bootscript](#) 192

[ZTP Utilities](#) 193

[Examples](#) 194



Preface

This product has reached end-of-life status. For more information, see the [End-of-Life and End-of-Sale Notices](#).

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
September 2017	Initial release of this document.
March 2018	Republished for Release 6.3.2.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact 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 6.3.x, on page 1](#)

System Management Features Added or Modified in IOS XR Release 6.3.x

Feature	Description	Changed in Release	Where Documented
Increase in Throttle Memory Range	In IOS XR 64-bit OS, the high range of memory usage per session by the XML agent is increased from 600 MB to 1024 MB.	Release 6.3.2	<i>Configuring Manageability</i> chapter. Configuring the XML Agent, on page 3.
IP-MIB Support for IPv4	From Release 6.3.2 onwards, IOS-XR implementation of IP-MIB supports IPv4 statistics as per RFC4293.	Release 6.3.2	<i>Configuring Simple Network Management Protocol</i> chapter. MIB section.
Smart License	Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks.	Release 6.3.2	<i>Configuring Smart License</i> chapter #unique_9



CHAPTER 2

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 3](#)
- [How to Configure Manageability, on page 3](#)
- [Configuration Examples for Manageability, on page 4](#)

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* | **default** } [*ipv4 access-list access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	xml agent [<i>ssl</i>] 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 <i>iteration-size</i> 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 <i>timeout</i> 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 { <i>memory size</i> <i>process-rate tags</i> } Example: RP/0/RP0/CPU0:router(config-xml-agent)# throttle memory 300	Configures the XML agent processing capabilities. <ul style="list-style-type: none"> Specify the memory size in Mbytes. Values can range from 100 to 600. In IOS XR 64 bit, the values range from 100 to 1024. 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 { <i>vrfname</i> default } [<i>ipv4 access-list access-list-name</i>] 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 3

Configuring Physical and Virtual Terminals

Line templates define standard attribute settings for incoming and outgoing transport over physical and virtual terminal lines (vty). 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 7](#)
- [Information About Implementing Physical and Virtual Terminals, on page 7](#)
- [How to Implement Physical and Virtual Terminals on Cisco IOS XR Software, on page 9](#)
- [Configuration Examples for Implementing Physical and Virtual Terminals, on page 14](#)

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.

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.

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 **vtty 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-line)# end or RP/0/RP0/CPU0:router(config-line)# commit	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> • 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. **vtty-pool {default | pool-name | eem} first-vty last-vty [line-template {default | template-name}]**
7. Use the **commit** or **end** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
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	vtty-pool {default pool-name eem} first-vty last-vty [line-template {default template-name}]	Creates or modifies vty pools.

	Command or Action	Purpose
	<p>Example:</p> <pre>RP/0/RP0/CPU0:router(config)#vty-pool default 0 5 line-template default</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config)#vty-pool pool1 5 50 line-template template1</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config)#vty-pool eem 100 105 line-template template1</pre> <pre>RP/0/RP0/CPU0:router(config)#vty-pool default 0 5 line-template template1</pre>	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. • eem —Configures the embedded event manager pool. <ul style="list-style-type: none"> • 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 <i>template-name</i> —Configures the vty pool to reference a user-defined template.
Step 7	Use the commit or end command.	<p>commit —Saves the configuration changes and remains within the configuration session.</p> <p>end —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> • 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* | **vtty** *number*]
2. (Optional) **show terminal**
3. (Optional) **show users**

DETAILED STEPS

	Command or Action	Purpose
Step 1	(Optional) show line [aux location <i>node-id</i> console location <i>node-id</i> vtty <i>number</i>] Example: <pre>RP/0/RP0/CPU0:router# show line</pre>	Displays the terminal parameters of terminal lines. <ul style="list-style-type: none"> Specifying the show line aux location <i>node-id</i> EXEC command displays the terminal parameters of the auxiliary line. Specifying the show line console location <i>node-id</i> EXEC command displays the terminal parameters of the console. <ul style="list-style-type: none"> For the location <i>node-id</i> keyword and argument, enter the location of the Route Processor (RP) on which the respective auxiliary or console port resides. The <i>node-id</i> argument is expressed in the format of <i>rack/slot/module</i>. Specifying the show line vtty <i>number</i> EXEC command displays the terminal parameters for the specified vty.
Step 2	(Optional) show terminal Example: <pre>RP/0/RP0/CPU0:router# show terminal</pre>	Displays the terminal attribute settings for the current terminal line.
Step 3	(Optional) show users Example: <pre>RP/0/RP0/CPU0:router# show users</pre>	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 4

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 17](#)
- [Restrictions for SNMP use on Cisco IOS XR Software, on page 17](#)
- [Information about Implementing SNMP, on page 18](#)
- [Session MIB support on subscriber sessions , on page 24](#)
- [How to Implement SNMP on Cisco IOS XR Software, on page 25](#)

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.

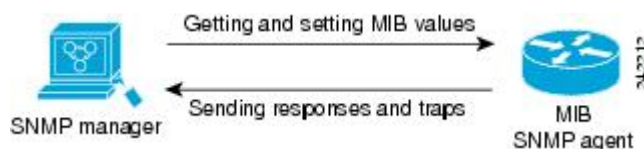
MIB

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





Note A few exceptions while performing SNMP walk on the NC55-6X200-DWDM-S line card on the NCS 5500 Series Routers are as follows:

1. Though the below mentioned OIDs are valid, they are marked as inaccessible in the OTN MIB standard. Hence they will not be polled during MIB walk.
 - OtnNearEndCurIntervalType : .1.3.6.1.4.1.9.9.639.1.2.3.1.1
 - OtnNearEndCurrentMonType : .1.3.6.1.4.1.9.9.639.1.2.3.1.2
 - OtnFarEndCurIntervalType : .1.3.6.1.4.1.9.9.639.1.2.4.1.1
 - OtnFarEndCurrentMonType : .1.3.6.1.4.1.9.9.639.1.2.4.1.2
2. OtnStatus : .1.3.6.1.4.1.9.9.639.1.1.1.1.5 OID is implicitly enabled for the interfaces of NC55-6X200-DWDM-S line card. Hence a MIB walk corresponding to the OtnStatus is not supported.

IP-MIB Support

RFC4293 IP-MIB was specifically designed to provide IPv4 and IPv6 statistics individually. The **ipIfStatsTable** defined in RFC 4293, lists the interface specific statistics. IPv6 statistics support in ipIfStatsTable was added earlier but, IOS-XR implementation of IP-MIB did not support IPv4 statistics as per RFC4293 in earlier releases.

From Release 6.3.2 onwards, IOS-XR implementation of IP-MIB supports IPv4 statistics as per RFC4293. This will enable you to collect the IPV4 and IPv6 statistics separately for each interface. The **ipIfStatsTable** is indexed by two **sub-ids address type (IPv4 or IPv6)** and the **interface ifindex[1]**. The implementation of IP-MIB support for IPv4 and IPv6 is separated from Release 6.3.2 for better readability and maintainability.

The list of OIDs added to the **ipIfStatsTable** for IPv4 statistics are:

- ipIfStatsInReceives
- ipIfStatsHCInReceives
- ipIfStatsInOctets
- ipIfStatsHCInOctets
- ipIfStatsOutTransmits
- ipIfStatsHCOutTransmits
- ipIfStatsOutOctets
- ipIfStatsHCOutOctets
- ipIfStatsDiscontinuityTime

For more information on the list of new OIDs added for IPv4 statistics, see [SNMP OID Navigator](#).

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 21](#) 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**

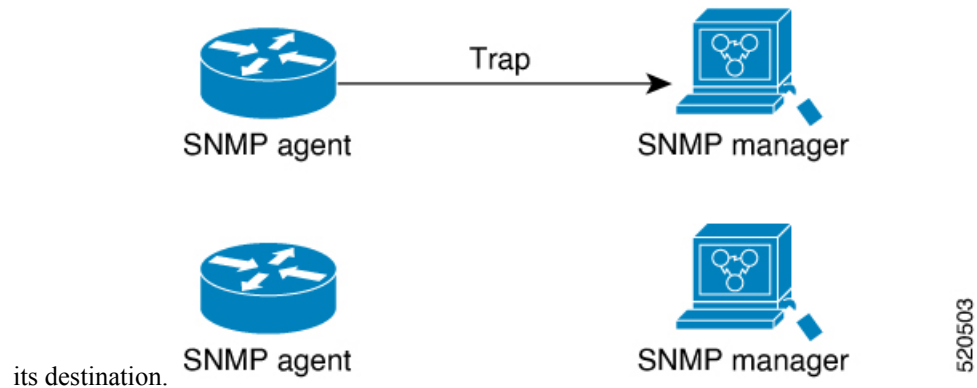
Inform requests (inform operations) are supported in Cisco IOS XR software.

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.

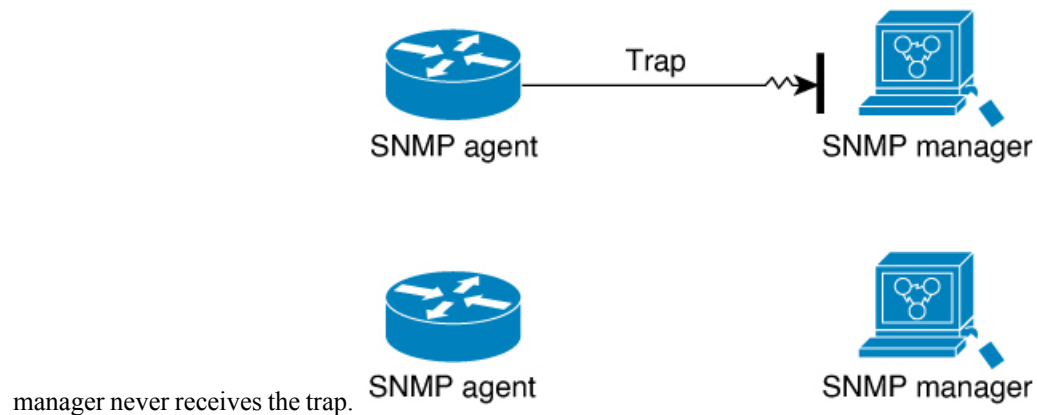
However, traps are often preferred because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, and an inform 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

**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



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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	(Optional) snmp-server engineid local <i>engine-id</i> 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	snmp-server view <i>view-name oid-tree</i> { included excluded } Example:	Creates or modifies a view record.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config)# snmp-server view view_name 1.3.6.1.2.1.1.5 included	
Step 4	snmp-server group <i>name</i> { 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 5	snmp-server user <i>username groupname</i> { 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 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: <ul style="list-style-type: none"> • 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 Example: RP/0/RP0/CPU0:router# show snmp	Displays information about the status of SNMP.
Step 8	(Optional) show snmp engineid Example: RP/0/RP0/CPU0:router# show snmp engineid	Displays information about the local SNMP engine.
Step 9	(Optional) show snmp group Example: RP/0/RP0/CPU0:router# show snmp group	Displays information about each SNMP group on the network.

	Command or Action	Purpose
Step 10	(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 11	(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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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: <ul style="list-style-type: none"> • Yes — Saves configuration changes and exits the configuration session. • No —Exits the configuration session without committing the configuration changes.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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

vldefault 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: vldefault
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: localSnmID
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_52` if you have already completed the steps documented under the `#unique_52` 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	snmp-server group <i>name</i> { v1 v2 v3 { auth noauth priv }} [read view] write view] [notify view] [<i>access-list-name</i>] Example: RP/0/RP0/CPU0:router(config)# snmp-server group <i>group_name</i> v3 noauth read view_name1 writer <i>view_name2</i>	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
Step 3	snmp-server user <i>username</i> <i>groupname</i> { v1 v2c v3 { auth md5 sha } { clear encrypted } <i>auth-password</i>] [priv des56 { clear <i>access-list-name</i> }] Example: RP/0/RP0/CPU0:router(config)# snmp-server group <i>group_name</i> v3 noauth read view_name1 writer <i>view_name2</i>	Configures a new SNMP group or a table that maps SNMP users to SNMP views.
Step 4	[snmp-server host <i>address</i> [traps] [version { 1 2c 3 [auth priv }}] <i>community-string</i> [udp-port port] [<i>notification-type</i>] 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.

	Command or Action	Purpose
Step 5	snmp-server traps [<i>notification-type</i>] 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. <ul style="list-style-type: none"> • If a trap is not specified with the <i>notification-type</i> 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: <ul style="list-style-type: none"> • 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

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

	Command or Action	Purpose
Step 2	snmp-server drop unknown-user Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server drop unknown-user</pre>	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: <ul style="list-style-type: none"> • 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 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** command 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

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

	Command or Action	Purpose
Step 2	(Optional) snmp-server contact <i>system-contact-string</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server contact Dial System Operator at beeper # 27345</pre>	Sets the system contact string.
Step 3	(Optional) snmp-server location <i>system-location</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server location Building 3/Room 214</pre>	Sets the system location string.
Step 4	(Optional) snmp-server chassis-id <i>serial-number</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server chassis-id 1234456</pre>	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: <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	(Optional) snmp-server packetsize <i>byte-count</i> 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: <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	(Optional) snmp-server trap-source <i>type interface-path-id</i> 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 <i>length</i> 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 <i>seconds</i> 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: <ul style="list-style-type: none"> • 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.

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

	Command or Action	Purpose
Step 1	configure Example: <pre>RP/0/RP0/CPU0:router# configure</pre>	Enters mode.
Step 2	Use one of the following commands: <ul style="list-style-type: none"> • snmp-server ipv4 precedence <i>value</i> • snmp-server ipv4 dscp <i>value</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server dscp 24</pre>	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: <ul style="list-style-type: none"> • 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.

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

	Command or Action	Purpose
Step 1	show snmp context-mapping Example: RP/0/RP0/CPU0:router# show snmp context-mapping	Displays the SNMP context mapping table.

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

	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	<p>Generates SNMP EVENT-MIB traps for the interface when the packet loss exceeds the specified thresholds. Up to 100 interfaces can be monitored.</p> <p>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.</p> <p>interval sampling-interval —Specifies how often packet loss statistics are polled. This is a value between 5 and 1440 minutes, in multiples of 5.</p> <p>rising upper-threshold —Specifies the upper threshold. When packet loss between two intervals increases above this threshold, an SNMP mteTriggreRising trap is generated. This trap is not generated until the packet loss drops below the lower threshold and then rises above the upper threshold.</p>

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

	Command or Action	Purpose
Step 1	(Optional) snmp-server entityindex persist Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server entityindex persist</pre>	Enables the persistent storage of ENTITY-MIB data.
Step 2	(Optional) snmp-server mibs cbqosmib persist Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib persist</pre>	Enables persistent storage of the CISCO-CLASS-BASED-QOS-MIB data.
Step 3	(Optional) snmp-server cbqosmib cache refresh time <i>time</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib cache refresh time 45</pre>	Enables QoS MIB caching with a specified cache refresh time.
Step 4	(Optional) snmp-server cbqosmib cache service-policy count <i>count</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server mibs cbqosmib cache service-policy count 50</pre>	Enables QoS MIB caching with a limited number of service policies to cache.
Step 5	snmp-server ifindex persist Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server ifindex persist</pre>	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

	Command or Action	Purpose
Step 1	configure Example: <pre>RP/0/RP0/CPU0:router# configure</pre>	Enters mode.
Step 2	snmp-server interface subset <i>subset-number</i> regular-expression <i>expression</i> Example: <pre>RP/0/RP0/CPU0:router(config)# snmp-server interface subset 10 regular-expression "^Gig[a-zA-Z]+[0-9/]+\."</pre> <pre>RP/0/RP0/CPU0:router(config-snmp-if-subset)#</pre>	<p>Enters snmp-server interface mode for the interfaces identified by the regular expression.</p> <p>The <i>subset-number</i> 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.</p> <p>The <i>expression</i> argument must be entered surrounded by double quotes.</p> <p>Refer to the <i>Understanding Regular Expressions, Special Characters, and Patterns</i> module in for more information regarding regular expressions.</p>
Step 3	notification linkupdown disable Example: <pre>RP/0/RP0/CPU0:router(config-snmp-if-subset)# notification linkupdown disable</pre>	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.	<p>commit —Saves the configuration changes, and remains within the configuration session.</p> <p>end —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
Step 5	(Optional) show snmp interface notification subset <i>subset-number</i> Example: <pre>RP/0/RP0/CPU0:router# show snmp interface notification subset 10</pre>	Displays the linkUp and linkDown notification status for all interfaces identified by the subset priority.
Step 6	(Optional) show snmp interface notification regular-expression <i>expression</i> Example: <pre>RP/0/RP0/CPU0:router# show snmp interface notification regular-expression "^Gig[a-zA-Z]+[0-9/]+\."</pre>	Displays the linkUp and linkDown notification status for all interfaces identified by the regular expression.
Step 7	(Optional) show snmp interface notification type <i>interface-path-id</i> Example: <pre>RP/0/RP0/CPU0:router# show snmp interface notification tengige 0/4/0/3.10</pre>	Displays the linkUp and linkDown notification status for the specified interface.



CHAPTER 5

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 47](#)
- [Prerequisites for Implementing Object Tracking, on page 47](#)
- [Information about Object Tracking, on page 48](#)
- [How to Implement Object Tracking, on page 48](#)
- [Configuration Examples for Configuring Object Tracking, on page 58](#)
- [Additional References, on page 60](#)

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

	Command or Action	Purpose
Step 1	configure Example: <pre>RP/0/RP0/CPU0:router# configure</pre>	Enters mode.
Step 2	track track-name Example: <pre>RP/0/RP0/CPU0:router(config)# track track1</pre>	Enters track configuration mode. <ul style="list-style-type: none"> • <i>track-name</i>—Specifies a name for the object to be tracked.
Step 3	type line-protocol state Example: <pre>RP/0/RP0/CPU0:router(config-track)# type line-protocol state</pre>	Creates a track based on the line protocol of an interface.
Step 4	interface type interface-path-id Example: <pre>RP/0/RP0/CPU0:router(config-track-line-prot)# interface atm 0/2/0/0.1</pre>	Specifies the interface to track the protocol state. <ul style="list-style-type: none"> • <i>type</i>—Specifies the interface type. For more information, use the question mark (?) online help function. • <i>interface-path-id</i>—Identifies a physical interface or a virtual interface. <p>Note Use the show interfaces command to see a list of all possible interfaces currently configured on the router.</p> <p>Note The loopback and null interfaces are always in the up state and, therefore, cannot be tracked.</p>
Step 5	exit Example: <pre>RP/0/RP0/CPU0:router(config-track-line-prot)# exit</pre>	Exits the track line protocol configuration mode.
Step 6	(Optional) delay {up seconds down seconds} Example: <pre>RP/0/RP0/CPU0:router(config-track)# delay up 10</pre>	Schedules the delay that can occur between tracking whether the object is up or down.
Step 7	Use one of the following commands: <ul style="list-style-type: none"> • end • commit Example: <pre>RP/0/RP0/CPU0:router(config-track)# end</pre>	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre>

	Command or Action	Purpose
	or RP/0/RP0/CPU0:router(config-track) # commit	<ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	track <i>track-name</i> Example:	Enters track configuration mode.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config)# track track1	<ul style="list-style-type: none"> • <i>track-name</i>—Specifies a name for the object to be tracked.
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: <ul style="list-style-type: none"> • vrf <i>vrf-table-name</i> • route ipv4 <i>IP-prefix/mask</i> 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: <ul style="list-style-type: none"> • <i>vrf-table-name</i>—A VRF table name. • <i>IP-prefix/mask</i>—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: <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	track <i>track-name</i> Example: RP/0/RP0/CPU0:router(config)# track track1	Enters track configuration mode. <ul style="list-style-type: none"> • <i>track-name</i>—Specifies a name for the object to be tracked.
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. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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 <i>object-name</i> [not] Example: <pre>RP/0/RP0/CPU0:router(config-track-list)# object 3 not</pre>	Specifies the object to be tracked by the list <ul style="list-style-type: none"> • <i>object-name</i>—Name of the object to track. • not—Negates the state of the object.
Step 5	exit Example: <pre>RP/0/RP0/CPU0:router(config-track-line-prot)# exit</pre>	Exits the track line protocol configuration mode.
Step 6	(Optional) delay { up <i>seconds</i> down <i>seconds</i> } Example: <pre>RP/0/RP0/CPU0:router(config-track)# delay up 10</pre>	Schedules the delay that can occur between tracking whether the object is up or down.
Step 7	Use one of the following commands: <ul style="list-style-type: none"> • end • commit Example: <pre>RP/0/RP0/CPU0:router(config-track)# end</pre> or <pre>RP/0/RP0/CPU0:router(config-track)# commit</pre>	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	track <i>track-name</i> Example: RP/0/RP0/CPU0:router(config)# track track1	Enters track configuration mode. • <i>track-name</i> —Specifies a name for the object to be tracked.
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 <i>object-name</i> 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 <i>percentage</i> down <i>percentage</i> 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.

	Command or Action	Purpose
Step 6	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-track)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-track)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	<p>configure</p> <p>Example:</p>	Enters mode.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router# configure	
Step 2	track <i>track-name</i> Example: RP/0/RP0/CPU0:router(config)# track track1	Enters track configuration mode. <ul style="list-style-type: none"> • <i>track-name</i>—Specifies a name for the object to be tracked.
Step 3	type list threshold weight Example: RP/0/RP0/CPU0:router(config-track)# type list threshold weight	Configures a track of type, threshold weighted list.
Step 4	object <i>object-name</i> weight <i>weight</i> 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: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-track)# end or RP/0/RP0/CPU0:router(config-track)# commit	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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
		<ul style="list-style-type: none"> 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	track <i>track-name</i> Example: RP/0/RP0/CPU0:router(config)# track t1	Enters track configuration mode.
Step 3	type rtr <i>ipsla-no</i> 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 <i>ipsla-no</i> can range from 1 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: <ul style="list-style-type: none"> 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
!

```

Configuring IPSLA based Object Tracking: Configuration Example

This example shows the configuration of IPSLA based object tracking, including the ACL and IPSLA configuration:

ACL configuration:

```

RP/0/RP0/CPU0:router(config)# ipv4 access-list abf-track
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit any nexthop track track1 1.2.3.4

```

Object tracking configuration:

```

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

```

IPSLA configuration:

```

RP/0/RP0/CPU0:router(config)# ipsla
RP/0/RP0/CPU0:router(config-ipsla)# operation 1
RP/0/RP0/CPU0:router(config-ipsla-op)# type icmp echo
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# source address 2.3.4.5
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# destination address 1.2.3.4
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# frequency 60
RP/0/RP0/CPU0:router(config-ipsla-icmp-echo)# exit
RP/0/RP0/CPU0:router(config-ipsla-op)# exit
RP/0/RP0/CPU0:router(config-ipsla)# schedule operation 1
RP/0/RP0/CPU0:router(config-ipsla-sched)# start-time now
RP/0/RP0/CPU0:router(config-ipsla-sched)# life forever

```

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	<i>Implementing IP Service Level Agreements on module in System Monitoring Configuration Guide for Cisco NCS 5500 Series Routers</i>

Related Topic	Document Title
IP SLA commands	<i>IP Service Level Agreement Commands on</i> module in <i>System Monitoring Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 and NCS 560 Series Routers</i>
Object tracking commands	<i>Object Tracking Commands on</i> 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: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC 2401	<i>Security Architecture for the Internet Protocol</i>

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 6

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 63](#)
- [Information About Implementing CDP, on page 63](#)
- [How to Implement CDP on Cisco IOS XR Software, on page 65](#)
- [Configuration Examples for Implementing CDP, on page 71](#)

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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	cdp Example: RP/0/RP0/CPU0:router(config)# cdp	Enables CDP globally.
Step 3	interface <i>type interface-path-id</i> 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: <ul style="list-style-type: none"> • Yes — Saves configuration changes and exits the configuration session.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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. <ul style="list-style-type: none"> • 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.
Step 3	cdp holdtime <i>seconds</i> 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> By default, when CDP is enabled, the receiving networking device holds a CDP packet for 180 seconds before discarding it. <p>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.</p> <ul style="list-style-type: none"> In this example, the value of hold-time for the <i>seconds</i> argument is set to 30.
Step 4	cdp timer <i>seconds</i> Example: <pre>RP/0/RP0/CPU0:router(config)# cdp timer 20</pre>	<p>Specifies the frequency at which CDP update packets are sent.</p> <ul style="list-style-type: none"> By default, when CDP is enabled, CDP update packets are sent at a frequency of once every 60 seconds. <p>Note A lower timer setting causes CDP updates to be sent more frequently.</p> <ul style="list-style-type: none"> 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.	<p>commit —Saves the configuration changes and remains within the configuration session.</p> <p>end —Prompts user to take one of these actions:</p> <ul style="list-style-type: none"> 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: <pre>RP/0/RP0/CPU0:router# show cdp</pre>	<p>Displays global CDP information.</p> <p>The output displays the CDP version running on the router, the hold time setting, and the timer setting.</p>

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

	Command or Action	Purpose
Step 1	show cdp entry <i>{* entry-name}</i> [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 [<i>type interface-path-id</i> 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 [<i>type interface-path-id</i> 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 7

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 73](#)
- [Information About Periodic MIB Data Collection and Transfer, on page 73](#)
- [How to Configure Periodic MIB Data Collection and Transfer, on page 75](#)
- [Periodic MIB Data Collection and Transfer: Example, on page 81](#)

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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	snmp-server mib bulkstat object-list <i>list-name</i> 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 <i>object-name</i> } 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.
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:

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	snmp-server mib bulkstat schema <i>schema-name</i> 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.

	Command or Action	Purpose
Step 3	object-list <i>list-name</i> 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: <ul style="list-style-type: none"> • instance exact {interface <i>interface-id</i> [sub-if] oid <i>oid</i>} • instance wild {interface <i>interface-id</i> [sub-if] oid <i>oid</i>} • instance range start <i>oid</i> end <i>oid</i> • instance repetition <i>oid</i> max <i>repeat-number</i> 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: <ul style="list-style-type: none"> • 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 <i>minutes</i> 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: <ul style="list-style-type: none"> • 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 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	snmp-server mib bulkstat transfer-id <i>transfer-id</i> Example: RP/0/RP0/CPU0:router(config)# snmp-server mib bulkstat transfer bulkstat1	Identifies the transfer configuration with a name (<i>transfer-id</i> argument) and enters bulk statistics transfer configuration mode.
Step 3	buffer-size <i>bytes</i> 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.

	Command or Action	Purpose
		<p>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.</p>
Step 4	<p>format {bulkBinary bulkASCII schemaASCII}</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# format schemaASCII</pre>	<p>(Optional) Specifies the format of the bulk statistics data file (VFile). The default is schemaASCII.</p> <p>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.</p>
Step 5	<p>schema <i>schema-name</i></p> <p>Example:</p> <pre>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</pre>	<p>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).</p>
Step 6	<p>transfer-interval <i>minutes</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# transfer-interval 20</pre>	<p>(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.</p>
Step 7	<p>url <i>primary url</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# url primary ftp://user:password@host/folder/bulkstat1</pre>	<p>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.</p>
Step 8	<p>url <i>secondary url</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# url secondary tftp://10.1.0.1/tftpboot/user/bulkstat1</pre>	<p>(Optional) Specifies a backup transfer destination and protocol for use in the event that transfer to the primary location fails. FTP or TFTP can be used for the bulk statistics file transfer.</p>
Step 9	<p>retry <i>number</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# retry 1</pre>	<p>(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.</p>

	Command or Action	Purpose
		<p>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.</p> <p>If all retries fail, the next normal transfer occurs after the configured transfer-interval time.</p>
Step 10	<p>retain <i>minutes</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# retain 60</pre>	<p>(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.</p> <p>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.</p>
Step 11	<p>enable</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# enable</pre>	<p>Begins the bulk statistics data collection and transfer process for this configuration.</p> <ul style="list-style-type: none"> 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).
Step 12	<p>commit <i>minutes</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-bulk-tr)# retain 60</pre>	<p>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.</p>

	Command or Action	Purpose
		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/dumppdcm
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 8

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 83](#)
- [Flexible Configuration Restrictions, on page 83](#)
- [Configuring a Configuration Group, on page 85](#)
- [Verifying the Configuration of Configuration Groups, on page 87](#)
- [Regular Expressions in Configuration Groups, on page 89](#)
- [Configuration Examples for Flexible CLI Configuration, on page 100](#)

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

Step 1 **configure**

Example:

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

Enters 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 98](#). 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

	Command or Action	Purpose
Step 1	show running-config group [<i>group-name</i>] Example: <pre>RP/0/RP0/CPU0:router# show running-config group group g-int-ge interface 'GigabitEthernet.*' mtu 1000 negotiation auto ! end-group</pre>	Displays the contents of a specific or all configured configuration groups.
Step 2	show running-config Example: <pre>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 !</pre>	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: <pre>RP/0/RP0/CPU0:router# show running-config inheritance . . group G-INTERFACE-MTU interface 'GigabitEthernet.*' mtu 1500 ! end-group . . interface interface GigabitEthernet0/4/1/0 ## Inherited from group G-INTERFACE-MTU mtu 1500 ! interface interface GigabitEthernet0/4/1/1</pre>	Displays the inherited configuration where ever a configuration group has been applied.

	Command or Action	Purpose
	<pre>mtu 2000 !</pre>	
Step 4	<p>show running-config interface x/y/z inheritance detail</p> <p>Example:</p> <pre>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</pre>	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 OSPF 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 inheritance** 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 GigabitEthernet0/0/0/21
!
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 ahref

```

3. Check the inheritance view of the ISIS configuration:

```

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

router isis vink
net 49.0011.2222.2222.00
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
    !
    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 9

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 115](#)
- [Information About Implementing NTP, on page 115](#)
- [Configuration Examples for Implementing NTP, on page 134](#)
- [Configuring NTP server inside VRF interface, on page 137](#)

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.

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 polling host servers
- By listening to NTP broadcasts

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.

NTP-PTP Interworking

NTP-PTP interworking provides the ability to use PTP, as well as 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. Prior to the support of NTP-PTP interworking, only backplane time was supported for the operating system time.

NTP-PTP 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 startup, switchovers or card and process failures.

For information regarding configuring NTP-PTP interworking, refer to *System Management Configuration Guide for Cisco NCS 5500 Series Routers*. For information regarding commands, refer to .

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* [**version number**] [**key key-id**] [**minpoll interval**] [**maxpoll interval**] [**source type interface-path-id**] [**prefer**] [**burst**] [**iburst**]
4. **peer** *ip-address* [**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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example: RP/0/RP0/CPU0:router(config)# ntp	Enters NTP configuration mode.

	Command or Action	Purpose
Step 3	<p>server <i>ip-address</i> [version number] [key key-id] [minpoll interval] [maxpoll interval] [source type interface-path-id] [prefer] [burst] [iburst]</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# server 172.16.22.44 minpoll 8 maxpoll 12</pre>	Forms a server association with another system. This step can be repeated as necessary to form associations with multiple devices.
Step 4	<p>peer <i>ip-address</i> [version number] [key key-id] [minpoll interval] [maxpoll interval] [source type interface-path-id] [prefer]</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# peer 192.168.22.33 minpoll 8 maxpoll 12 source tengige 0/0/0/1</pre>	<p>Forms a peer association with another system. This step can be repeated as necessary to form associations with multiple systems.</p> <p>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.</p>
Step 5	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example: RP/0/RP0/CPU0:router(config)# ntp	Enters NTP configuration mode.
Step 3	(Optional) broadcastdelay <i>microseconds</i> Example: RP/0/RP0/CPU0:router(config-ntp)# broadcastdelay 5000	Adjusts the estimated round-trip delay for NTP broadcasts.

	Command or Action	Purpose
Step 4	interface <i>type interface-path-id</i> Example: <pre>RP/0/RP0/CPU0:router(config-ntp)# interface POS 0/1/0/0</pre>	Enters NTP interface configuration mode.
Step 5	broadcast client Example: <pre>RP/0/RP0/CPU0:router(config-ntp-int)# broadcast client</pre>	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 <i>ip-address</i>] [key <i>key-id</i>] [version <i>number</i>] Example: <pre>RP/0/RP0/CPU0:router(config-ntp-int)# broadcast destination 10.50.32.149</pre>	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: <ul style="list-style-type: none"> • end • commit Example: <pre>RP/0/RP0/CPU0:router(config-ntp-int)# end</pre> or <pre>RP/0/RP0/CPU0:router(config-ntp-int)# commit</pre>	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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:	Saves configuration changes.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# commit</pre>	<ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example: RP/0/RP0/CPU0:router(config)# ntp	Enters NTP configuration mode.
Step 3	authenticate Example: RP/0/RP0/CPU0:router(config-ntp)# authenticate	Enables the NTP authentication feature.
Step 4	authentication-key <i>key-number</i> md5 [clear encrypted] <i>key-name</i> Example: RP/0/RP0/CPU0:router(config-ntp)# authentication-key 42 md5 clear key1	Defines the authentication keys. <ul style="list-style-type: none"> • Each key has a key number, a type, a value, and, optionally, a name. Currently the only key type supported is md5.
Step 5	trusted-key <i>key-number</i> Example: RP/0/RP0/CPU0:router(config-ntp)# trusted-key 42	Defines trusted authentication keys. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-ntp)# end or	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre>

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config-ntp)# commit	<ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example:	Enters NTP configuration mode.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config)# ntp	
Step 3	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • no interface <i>type interface-path-id</i> • interface <i>type interface-path-id</i> disable <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# no interface pos 0/0/0/1</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# interface POS 0/0/0/1 disable</pre>	Disables NTP services on the specified interface.
Step 4	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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 117.
Step 4	Use one of the following commands: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-ntp)# end or RP/0/RP0/CPU0:router(config-ntp)# commit	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	configure Example: <pre>RP/0/RP0/CPU0:router# configure</pre>	Enters mode.
Step 2	ntp Example: <pre>RP/0/RP0/CPU0:router(config)# ntp</pre>	Enters NTP configuration mode.
Step 3	master <i>stratum</i> Example:	Makes the router an authoritative NTP server.

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config-ntp)# master 9</pre>	<p>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.</p>
Step 4	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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-PTP Interworking

Use this task to configure NTP to use PTP as the time source.

Before you begin

PTP must be supported and enabled on the router before NTP-PTP interworking can be configured. If PTP is not enabled, you receive an error message similar to the following when you try to commit the configuration:

```
RP/0/RP0/CPU0:router(config)# ntp master primary-reference-clock
RP/0/RP0/CPU0:router(config)# commit

% Failed to commit one or more configuration items. Please issue
'show configuration failed' from this session to view the errors

RP/0/RP0/CPU0:router(config)# show configuration failed
[:::]
ntp
```

```

master primary-reference-clock
!!% 'ip-ntp' detected the 'fatal' condition 'PTP is not supported on this platform'
!
end

```

SUMMARY STEPS

1. **configure**
2. **ntp**
3. **master primary-reference-clock**
4. Use one of the following commands:
 - **end**
 - **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example: RP/0/RP0/CPU0:router(config)# ntp	Enters NTP configuration mode.
Step 3	master primary-reference-clock Example: RP/0/RP0/CPU0:router(config-ntp)# master primary-reference-clock	Specifies PTP to be the NTP time source.
Step 4	Use one of the following commands: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-ntp)# end or RP/0/RP0/CPU0:router(config-ntp)# commit	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre> Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: </pre> <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 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.

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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters 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 to update its system calendar from the software clock at periodic intervals.

	Command or Action	Purpose
Step 4	<p>Use one of the following commands:</p> <ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# end</pre> <p>or</p> <pre>RP/0/RP0/CPU0:router(config-ntp)# commit</pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> • 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

	Command or Action	Purpose
Step 1	<p>show ntp associations [detail] [location node-id]</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router# show ntp associations</pre>	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 (syncd), # master (unsyncd), + 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 minpoll 5 maxpoll 7
 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

	Command or Action	Purpose
Step 1	configure Example: RP/0/RP0/CPU0:router# configure	Enters mode.
Step 2	ntp Example: RP/0/RP0/CPU0:router(config)# ntp	Enters NTP configuration mode.

	Command or Action	Purpose
Step 3	vrf <i>vrf-name</i> 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 <i>interface-type interface-instance</i> 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 117 .
Step 5	Use one of the following commands: <ul style="list-style-type: none"> • end • commit Example: RP/0/RP0/CPU0:router(config-ntp)# end or RP/0/RP0/CPU0:router(config-ntp)# commit	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> • 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 10

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 139](#)
- [ITU-T Telecom Profiles for PTP, on page 144](#)
- [Configuring PTP , on page 147](#)
- [Configuration Examples, on page 155](#)

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 6: 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)	<p>An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes:</p> <ul style="list-style-type: none"> • 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)	<p>The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected.</p> <p>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.</p>
Transparent Clock (TC)	<p>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.</p>

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
- 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.
- Transparent Clock is not supported.

PTP Support Information

This table lists different types of support information related to PTP:

Transport Media	<ul style="list-style-type: none"> • UDP over IPv4 • Ethernet
-----------------	---

Messages	<ul style="list-style-type: none"> • Signaling • Announce • Sync • Follow-up • Delay-request • Delay-response • Management
Transport Modes	<ul style="list-style-type: none"> • 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.

Timing Hardware Support Matrix

This table provides a detailed information on the timing features that are supported on the following hardware PIDs.

Hardware Variant	Features	Cisco IOS XR Release	Comments
RP: NC55-RP-E Line card: NC55-36X100G-A-SE	BITS	Release 6.3.2	
	SyncE	Release 6.3.2	SyncE is not supported on 25GE or 100GE interfaces, when they are used in 1G mode.
	Dedicated 1588 Port (RP)	Release 6.3.2	
	G.8265.1	Release 6.3.2	
	G.8275.1	Release 6.3.2	
	G.8275.2	NA	
	GNSS External	Release 6.3.2	

Hardware Variant	Features	Cisco IOS XR Release	Comments
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.
	G.8265.1	Release 6.3.2	
	G.8275.1	Release 6.3.2	
	G.8275.2	Release 6.3.2	
	GNSS External	Release 6.3.2	

**Note**

Cisco NCS 5500 Series Routers support 64 PTP clients at 64 PPS sync packet rate.

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

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:

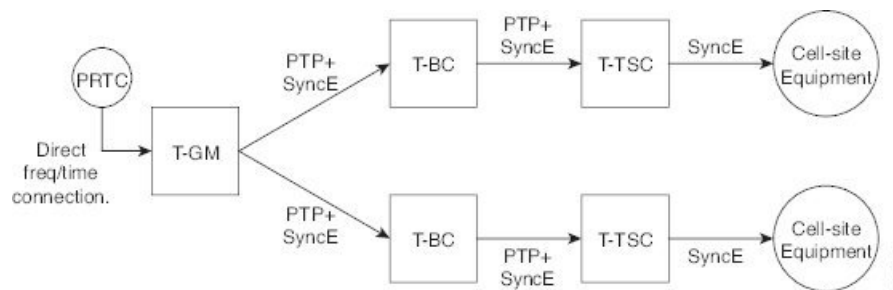
- **Synchronization Model:** G.8275.1 profile adopts hop-by-hop synchronization model. Each network device in the path from master to slave synchronizes its local clock to upstream devices and provides synchronization to downstream devices.
- **Clock Selection:** G.8275.1 profile also defines an alternate 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



Configuring 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.

Configuring 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:

```
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
!

```

Configuring 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
!
```

Configuring 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
!
```

Configuring 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.

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

```

Configuring 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** *interface-path-id* command in the configuration mode.

```
RP/0/RP0/CPU0:router(config)# interface gigabitethernet 0/1/0/1
```

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
```


- 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 Name	Port Number	Port State	Encap	Line 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
  !
```

Configuring 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.

- To enter the PTP configuration mode, use **ptp** command in the configuration mode.

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

- To enter the PTP-clock configuration mode, use **clock** command in the ptp-configuration mode.

```
RP/0/RP0/CPU0:router(config-ptp)# clock
```

- 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
```

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

Master Global Configuration:

```
ptp
clock
domain 24
profile g.8275.1
!
profile master
transport ethernet
sync frequency 16
announce interval 1
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
clock operation two-step
!
ipv4 address 17.1.1.1/24

```

Slave Global Configuration:

```

ptp
clock
domain 24
profile g.8275.1 clock-type T-TSC
!
profile slave
transport ethernet
sync frequency 16
announce interval 1
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
!
clock operation two-step
!
ipv4 address 18.1.1.2/24

```

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 interval 1
delay-request frequency 16
exit
profile slave
transport ethernet
sync frequency 16
announce interval 1
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
!
clock operation two-step
!
ipv4 address 17.1.1.2/24
interface gi 0/2/0/0
ptp
profile master
transport ethernet
multicast target-address ethernet 01-1B-19-00-00-00
clock operation two-step

```

```
!  
ipv4 address 18.1.1.1/24
```




CHAPTER 11

Configuring Smart Licensing

This module describes the configuration related to the Smart Licensing.

Table 7: Feature History for Smart License

Release	Modification
Release 6.3.2	Smart Licensing was introduced.
Release 6.5.2	Flexible Consumption License Model was introduced.

This module contains the following topics:

- [What is Smart Licensing?, on page 161](#)
- [What is Flexible Consumption Model?, on page 162](#)
- [How Does Smart Licensing Work?, on page 166](#)
- [What is Cisco Smart Software Manager?, on page 167](#)
- [Configuring Smart Licensing, on page 169](#)
- [Registering and Activating Your Router, on page 176](#)
- [Verifying the Smart Licensing Configuration , on page 181](#)

What is Smart Licensing?

Smart Licensing is a cloud-based, flexible software licensing model that enables you to activate and manage Cisco software licenses across their organization. Smart Licensing solution allows you to easily track the status of your license and software usage trends. Cisco Smart Licensing establishes a pool of licenses or entitlements that can be used across the entire organization in a flexible and automated manner. Smart Licensing helps simplify four core functions:

- **Purchase**—Creates a Smart Account (and optionally, your Virtual Account). Licenses are added to your Smart Account and are immediately available for use.
- **Install**—Register your product with your Smart Account using an account-based Registration Token. Thereafter, the entire process is automatic. Product Activation Keys (PAKs) and license files are no longer needed.
- **Management**—Make changes to license consumption by updating your configuration; any license change is automatically reflected in your Smart Account. You can share licenses in your Virtual Account through the license pooling option. License pools (logical grouping of licenses) can reflect your organization

structure. Smart Licensing solution also offers Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website.

- **Visibility and Asset Management**—Cisco Smart Software Manager (CSSM) portal offers an integrated view of the licenses you own and have deployed. You can use this data to make better purchase decisions, based on your consumption.

What is Flexible Consumption Model?

The Flexible Consumption Model (FCM) provides the capability and flexibility to purchase software capacity as needed. FCM delivers the following:

- **Pay-as-you-grow**—Enables you to lower initial costs and add more capacity over time.
- **Simplify operations**—FCM delivers the carrier-class IOS-XR software feature set with two software suites, Essentials and Advanced, that simplify license management.
- **Utilize capital efficiently**—License pooling enables an efficient way to share licenses across the network.

To enable Flexible Consumption model licensing on routers running Cisco IOS XR :

```
Router(config)# license smart flexible-consumption enable
Router(config)# commit
```

To verify the Flexible Consumption Model configuration:

```
Device# show running-config license smart flexible-consumption enable
```

The following table provides information about FCM licenses for NCS 5500 Series routers:

Table 8: Flexible Consumption Model Licensing Usage Pattern

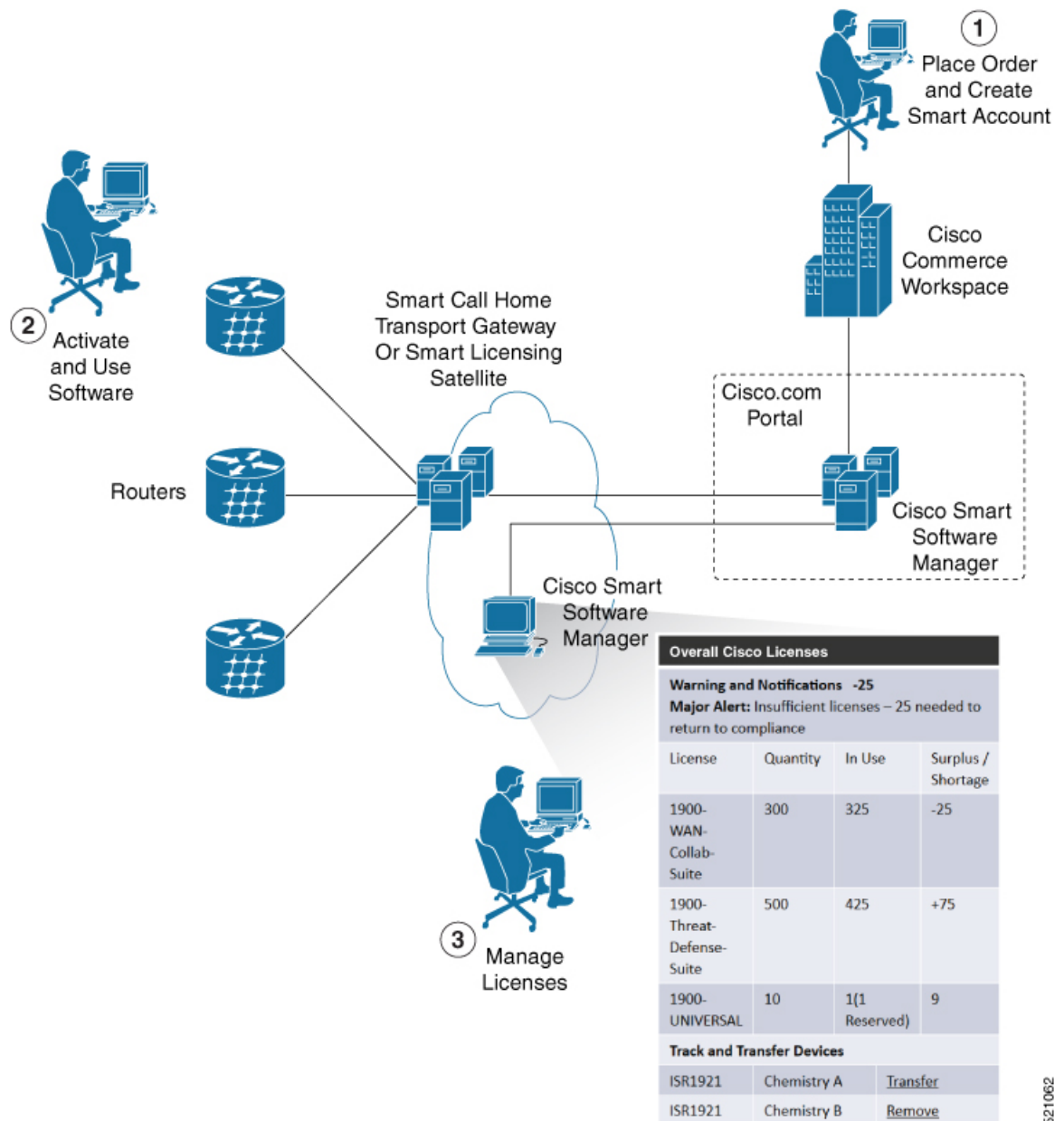
License Name	Hardware Supported	Consumption Pattern
Essential and Advanced Licenses: <ul style="list-style-type: none"> • ESS-100G-RTU-1 • ADV-100G-RTU-1 	<ul style="list-style-type: none"> • Routers with fixed chassis unit: NCS 5501, NCS 5501-SE, NCS 5502, NCS 5502-SE, NCS 55A1-24H, NCS 55A1-36H-S, NCS-55A2-MOD-HD-S, NCS-55A2-MOD-SE-S, and NCS-55A2-MOD-S • Routers with modular chassis unit: NCS 5504, NCS 5508-, NCS-5516, NC55-MOD-A-S, and NC-55-MOD-A-SE-S • Line cards: NC-55-36X100G, NC-55-36X100GA-SE, NC-55-18H18F, NC-55-24H12F-SE, NC-55-24X100G-SE, NCS-55A1-36H-SE-S, NC55-6X200-DWDM-S, NCS-55A1-48Q6H, and NC55-36X100G-S 	The number of essential or advanced licenses consumed depends on the number of active ports and is reported on per chassis basis.

License Name	Hardware Supported	Consumption Pattern
<p>Hardware Tracking Licenses that support chassis:</p> <ul style="list-style-type: none"> • NCS-5501-TRK • NCS-5501-SE-TRK • NCS-5502-TRK • NCS-5502-SE-TRK • NCS-5504-TRK • NCS-5508-TRK • NCS-5516-TRK • NCS-55A1-24H-TRK • NCS-55A1-36H-TRK • NCS-55A1-36HS-TRK • NCS-55A1-48Q6H-TRK • NCS-55A2-MOD-TRK • NCS-55A2-MODH-TRK • NCS-55A2-MODS-TRK • 	<p>These Tracking licenses are named on the basis of the hardware supported. For example, NCS-5501-TRK licenses support NCS 5501 systems.</p>	<p>The number of licenses consumed depends on the number of chassis in use.</p>
<p>Hardware Tracking Licenses that support line cards:</p> <ul style="list-style-type: none"> • NC55-36H-LC-TRK • NC55-36HSE-LC-TRK • NC55-18HF-LC-TRK • NC55-24H12-LC-TRK • NC55-24HSE-LC-TRK • NC55-DWDM-LC-TRK • NC55-MOD-A-SE-TRK • NC55-MOD-A-TRK 	<p>These Tracking licenses are named on the basis of the line card supported. For example, NC55-36H-LC-TRK licenses support NC-55-36X100G line cards.</p>	<p>The number of licenses consumed depends on the number of line cards in use.</p>

License Name	Hardware Supported	Consumption Pattern
Software Tracking license: <ul style="list-style-type: none">• XR-6.3-TRK• XR-6.5-TRK• XR-6.6-TRK• XR-7.0-TRK• XR-7.1-TRK	These Tracking licenses are named on the basis of the software supported. For example, XR-6.3-TRK license supports IOS XR 6.3.x software image.	The number of licenses consumed depends on the software images used.

How Does Smart Licensing Work?

Figure 5: Smart Licensing - Workflow



521062

1. Place Order and Create Smart Account—You must have a Smart Account to set up Smart Licensing.
 - a. Go to <https://software.cisco.com/>.
 - b. Under the **Administration** section, click **Get a Smart Account or Request Access to an Existing Smart Account**.
 - c. Verify or enter your Cisco.com profile details to complete creating a Smart Account.

2. **Activate and Use Software**—Register your product. For more information, see the *Registering your Router* section. After you enable Smart Licensing, you can use either of the following options to communicate with the CSSM:
 - **Smart Call Home**—The Smart Call Home feature is automatically configured after the Smart Licensing is enabled. Smart Call Home is used by Smart Licensing as a medium for communication with the CSSM. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center. The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events. For more information on Smart Call Home feature, see the [Smart Call Home Deployment Guide](#).
 - **Smart Licensing CSSM On-Prem**—The Smart licensing on-premise option provides an on-premises collector that can be used to consolidate and manage Smart license usage, as well as facilitate communications back to the CSSM at Cisco.com.
3. **Manage Licenses**—You can manage and view reports about your overall license usage in the Smart Software Manager portal.

What is Cisco Smart Software Manager?

Cisco Smart Software Manager enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). The Cisco Smart Software Manager allows you to:

- Create, manage, or view virtual accounts
- Create and manage Product Instance Registration Tokens
- Transfer licenses between virtual accounts or view licenses
- Transfer, remove, or view product instances
- Run reports against your virtual accounts
- Modify your email notification settings
- View overall account information

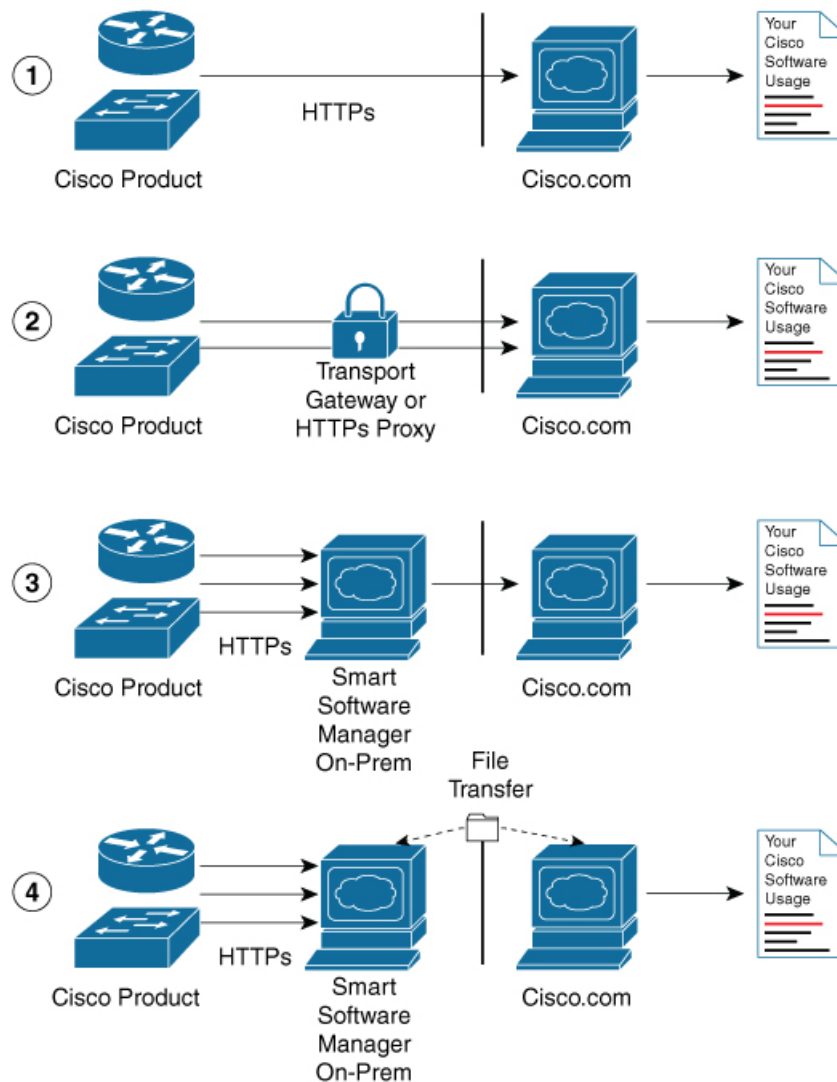
To access the Cisco Smart Software Manager:

- Go to <https://software.cisco.com>.
- Under the **License** section, click **Smart Software Licensing**.

Smart Licensing Deployment Options

The following illustration shows the various options available for deploying Smart Licensing:

Figure 6: Smart Licensing Deployment Options



1. Direct cloud access—In this method, Cisco products send usage information directly over the internet to CSSM on <http://www.cisco.com>; no additional components are needed for deployment.
2. Direct cloud access through an HTTPs proxy—In direct cloud access through an HTTPs proxy deployment method, Cisco products send usage information over the internet through a proxy server—either a Smart Call Home Transport Gateway or off-the-shelf Proxy (such as Apache) to CSSM on <http://www.cisco.com>.
3. Mediated access through an on-premises collector-connected—In mediated access through an on-premises collector-connected deployment method, Cisco products send usage information to a locally connected collector, which acts as a local license authority. Periodically, the information is exchanged to keep the databases in synchronization.
4. Mediated access through an on-premises collector-disconnected—In the mediated access through an on-premises collector-disconnected deployment method, Cisco products send usage information to a local disconnected collector, which acts as a local license authority. Exchange of human-readable information is performed occasionally (once a month) to keep the databases in synchronization.

Options 1 and 2 provide easy deployment options, whereas options 3 and 4 provide secure environment deployment options.


Note

Smart Software On-Premise provides support for options 3 and 4.

The communication between Cisco devices and CSSM is facilitated by the Smart Call Home software.

Configuring Smart Licensing

Prerequisites for Configuring Smart Licensing

Ensure that you have completed the following activities on Cisco Smart Software Manager:

- Set up a Cisco Smart Account. For more information, see the *How Smart Licensing Works* section in this document.
- Set up Virtual Account or accounts. For more information, see the *Virtual Accounts* section in the [Smart Software Manager Help](#).
- Create user roles in the **Users** tab in the **Manage Smart Account** page. Provide the appropriate user access rights.
- Accept the Smart Software Licensing Agreement on Cisco Smart Software Manager to register your router.
- Have a layer 3 connection set up on your router.
- Configure a valid DNS and proper time on the router to connect CSSM or CSSM On-Prem.

Setting up the Router for Smart Licensing

Table 9: Three-step Roadmap to Set up the Router for Smart Licensing

Activity	Communication Connection Options		
Step 1—Configure Communications	See the <i>Configuring a Direct Cloud Connection</i> section.	See the <i>Configuring a Connection through a HTTP Proxy</i> section.	See the <i>Connecting to CSSM On-Premise</i> section.
Step 2—Register and Activate	See the <i>Registering and Activating your Router</i> section.		
Step 3—Verify the Configuration	See the <i>Verifying your Smart Licensing Configuration</i> section.		

Configuring a Communications Connection Between the Router and Cisco Smart Software Manager

Configuring a Direct Cloud Connection

In this deployment option, the **configure call-home profile** is configured by default. Use the **show call-home profile all** command to check the profile status.

Call Home service provides email-based and web-based notification of critical system events to Cisco Smart Software Manager.

To configure and enable Call Home service:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **service active**
4. **contact-email-addr** *email-address*
5. **profile CiscoTAC-1**
6. **destination transport-method** **http**
7. **destination address** **http** *url*
8. **active**
9. **no destination transport-method** **email**
10. **commit**
11. **exit**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 2	call-home Example: Router(config)# <code>call-home</code>	Enters Call Home configuration mode.
Step 3	service active Example: Router(config-call-home)# <code>service active</code>	Activates Call Home service.
Step 4	contact-email-addr <i>email-address</i> Example: Router(config-call-home)# <code>contact-email-addr</code> <code>username@example.com</code>	Assigns the provided email address. You can enter up to 200 characters in email address format. Note Spaces are not allowed in the email address.

	Command or Action	Purpose
Step 5	profile CiscoTAC-1 Example: <pre>Router(config-call-home)# profile CiscoTAC-1</pre>	Enables the CiscoTAC-1 profile to be used with the Call Home service. By default, the CiscoTAC-1 profile is disabled.
Step 6	destination transport-method http Example: <pre>Router(config-call-home-profile)# destination transport-method http</pre>	Enables the Call Home service through an HTTP connection.
Step 7	destination address http url Example: <pre>Router(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/odde/services/DDCEService</pre>	Connects the router to the Cisco Smart Software Manager.
Step 8	active Example: <pre>Router(config-call-home-profile)# active</pre>	Enables the destination profile.
Step 9	no destination transport-method email Example: <pre>Router(config-call-home-profile)# no destination transport-method email</pre>	Disables the email option for the Call Home service.
Step 10	commit Example: <pre>Router(config-call-home-profile)# commit</pre>	Commits the configuration.
Step 11	exit Example: <pre>Router(config-call-home-profile)# exit</pre>	Exits the Call Home destination profile configuration mode and returns to the Call Home configuration mode.
Step 12	exit Example: <pre>Router(config-call-home)# exit Router(config)#</pre>	Exits the Call Home configuration mode and returns to the global configuration mode.

Configuring a Connection Through an HTTP Proxy

The Call Home service can be configured through an HTTPs proxy server.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **service active**

4. **contact-email-address** *email-address*
5. **http-proxy** *proxy-address* **port** *port-number*
6. **profile** **CiscoTAC-1**
7. **no destination transport-method** **email**
8. **exit**
9. **profile** *profile-name*
10. **reporting smart-licensing-data**
11. **destination transport-method** **http**
12. **destination address** **http** *url*
13. **active**
14. **exit**
15. **exit**
16. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	call-home Example: Router(config)# call-home	Enters Call Home configuration mode.
Step 3	service active Example: Router(config-call-home)# service active	Enables the Call Home feature.
Step 4	contact-email-address <i>email-address</i> Example: Router(config-call-home)# contact-email-addr sch-smart-licensing@cisco.com	Configures the default email address.
Step 5	http-proxy <i>proxy-address</i> port <i>port-number</i> Example: Router(config-call-home)# http-proxy 198.51.100.10 port 3128	Provides the proxy server information to the Call Home service.
Step 6	profile CiscoTAC-1 Example: Router(config-call-home)# profile CiscoTAC-1	Enables the CiscoTAC-1 profile to be used with the Call Home service. By default, the CiscoTAC-1 profile is disabled.
Step 7	no destination transport-method email Example:	Disables the email option for the Call Home service.

	Command or Action	Purpose
	<code>Router(config-call-home-profile)# no destination transport-method email</code>	
Step 8	exit Example: <code>Router(config-call-home-profile)# exit</code> <code>Router(config-call-home)#</code>	Exits the Call Home destination profile configuration mode and returns to the Call Home configuration mode.
Step 9	profile <i>profile-name</i> Example: <code>Router(config-call-home)# profile test1</code>	Enters the Call Home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created.
Step 10	reporting smart-licensing-data Example: <code>Router(config-call-home-profile)# reporting smart-licensing-data</code>	Enables data sharing with the Call Home service through the configured transport method, in this case, HTTP.
Step 11	destination transport-method http Example: <code>Router(config-call-home-profile)# destination transport-method http</code>	Enables the HTTP message transport method.
Step 12	destination address http <i>url</i> Example: <code>Router(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/odce/services/DDCEService</code>	Connects the router to the Cisco Smart Software Manager.
Step 13	active Example: <code>Router(config-call-home-profile)# active</code>	Enables the destination profile.
Step 14	exit Example: <code>Router(config-call-home-profile)# exit</code>	Exits the Call Home destination profile configuration mode and returns to the Call Home configuration mode.
Step 15	exit Example: <code>Router(config-call-home)# exit</code> <code>Router(config)#</code>	Exits the Call Home configuration mode and returns to the global configuration mode.
Step 16	commit Example: <code>Router(config)# commit</code>	Commits the configuration.

Connecting to CSSM On-Premise

This section describes how to configure the Call Home service for on-premise smart software through connected or disconnected mode.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *profile-name*
4. **reporting smart-licensing-data**
5. **destination transport-method** **http**
6. **destination address** **http** *url*
7. **no destination address** **http** *url*
8. **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
9. **active**
10. **exit**
11. **exit**
12. **http client source-interface** *ip-version interface-type interface-number*
13. **crypto ca trustpoint** *name*
14. **commit**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	call-home Example: Router(config)# call-home	Enters Call Home configuration mode.
Step 3	profile <i>profile-name</i> Example: Router(config-call-home)# profile test1	Enters the Call Home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created.
Step 4	reporting smart-licensing-data Example: Router(config-call-home-profile)# reporting smart-licensing-data	Enables data sharing with the Call Home service through the configured transport method, in this case, HTTP.
Step 5	destination transport-method http Example: Router(config-call-home-profile)# destination transport-method http	Enables the HTTP message transport method.

	Command or Action	Purpose
Step 6	destination address <i>http url</i> Example: <pre>Router(config-call-home-profile)# destination address http http://209.165.201.15/Transportgateway/services/RouterRequestHandler</pre> Or <pre>Router(config-call-home-profile)# destination address http https://209.165.201.15/Transportgateway/services/RouterRequestHandler</pre>	Configures the destination URL (CSSM) to which Call Home messages are sent. Note Ensure the IP address or the fully qualified domain name (FQDN) in the destination URL matches the IP address or the FQDN as configured for the Host Name on the CSSM On-Prem.
Step 7	no destination address <i>http url</i> Example: <pre>Router(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/odbc/services/DDCEService</pre>	Removes the default destination address.
Step 8	destination preferred-msg-format { <i>long-text</i> <i>short-text</i> <i>xml</i> } Example: <pre>Router(config-call-home-profile)# destination preferred-msg-format xml</pre>	(Optional) Configures a preferred message format. The default message format is XML.
Step 9	active Example: <pre>Router(config-call-home-profile)# active</pre>	Enables the destination profile.
Step 10	exit Example: <pre>Router(config-call-home-profile)# exit</pre>	Exits the Call Home destination profile configuration mode and returns to the Call Home configuration mode.
Step 11	exit Example: <pre>Router(config-call-home)# exit Router(config)#</pre>	Exits the Call Home configuration mode and returns to the global configuration mode.
Step 12	http client source-interface <i>ip-version interface-type interface-number</i> Example: <pre>Router(config)# http client source-interface ipv4 Vlan100</pre>	Configures a source interface for the HTTP client. Note This command is mandatory for a VRF interface.
Step 13	crypto ca trustpoint <i>name</i> Example:	(Optional) Declares the trustpoint and its name.

	Command or Action	Purpose
	Router(config)# crypto ca trustpoint SLA-TrustPoint Router(config-trustp)#	
Step 14	commit Example: Router(config-trustp)# commit	Commits the configuration.
Step 15	end Example: Router(config-trustp)# end Router(config)#	Returns to the global configuration mode.

Installing CSSM On-Premise

For information on installation instructions, see the [Smart Software Manager On-Prem Installation Guide](#).

Registering and Activating Your Router

Product registration securely associates a device with the Smart Account and the Virtual Account of your choice. It also establishes trust between the end product and the CSSM. Tokens are used to register a product with the appropriate Virtual Account on CSSM Cloud (on Cisco.com) or CSSM On-Premise.

A Registration Token:

- Can be either used once or reused multiple times. You can set a limit to the number of times a token can be reused when you create the token.
- Can be created and revoked at any time.
- Expires after a period of time (default is 30 days; minimum is one day; maximum is 365 days)

A Registration Token is not:

- Product specific: The same Registration Token can be used on different product types.
- A license, key, or PAK.
- Stored on the Cisco device and they are not persistent.
- Required after the product is registered. Token expiration has no effect on previously registered products; it simply means that that token can no longer be used to register a new product.

Generating a New Token from CSSM

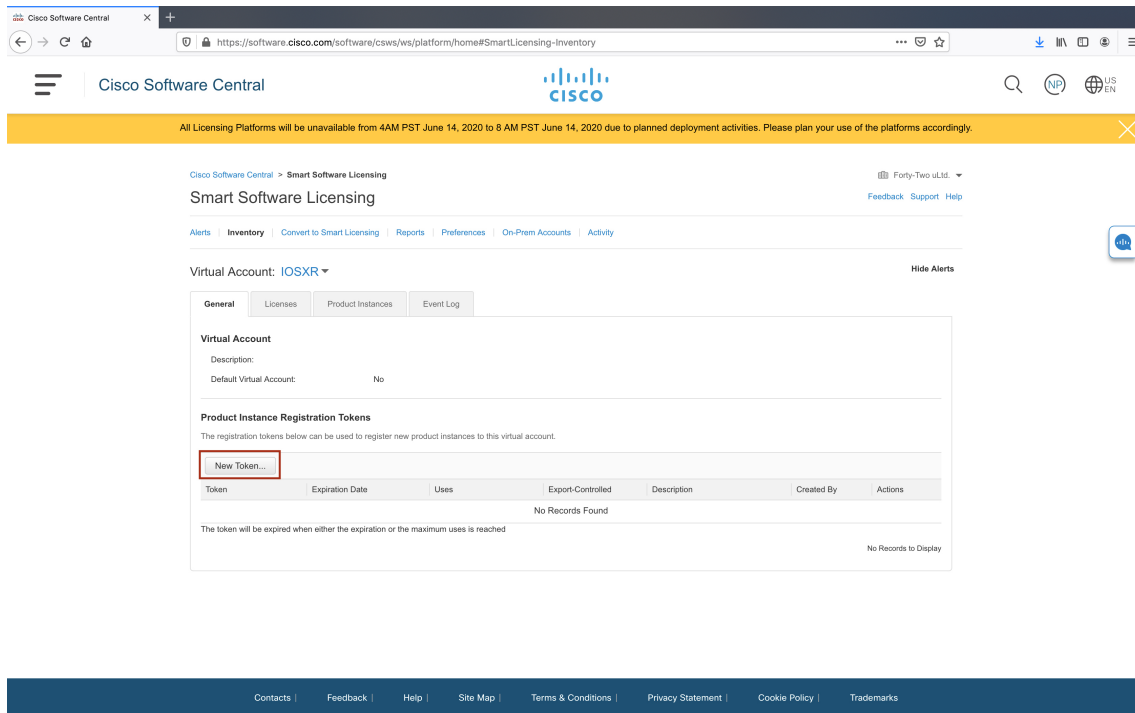
- Step 1** If you choose the direct cloud access deployment option, log in to CSSM from <https://software.cisco.com/#>.
If you chose the mediated access deployment option, log in to CSSM On-Prem from <https://<on-prem-ip-address>:8443>.

Step 2 Select the **Inventory** tab.

Step 3 From the Virtual Account drop-down list, choose the virtual account to which you want to register your product.

Step 4 Select the **General** tab.

Step 5 Click **New Token**.



The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description.

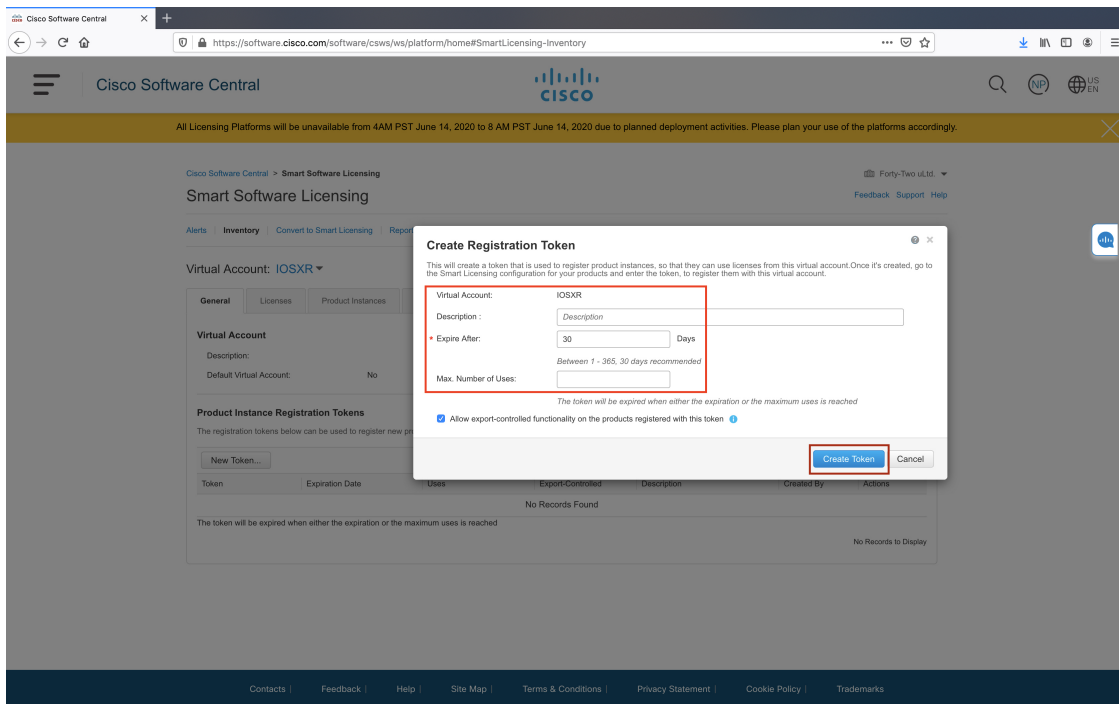
In the **Expire After** field, enter the number of days the token must be active. The default value is 30 days.

In the **Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Select the **Allow export-controlled functionality on the products registered with this token** checkbox to ensure Cisco compliance with US and country-specific export policies and guidelines. For more information, see <https://www.cisco.com/c/en/us/about/legal/global-export-trade.html>.

521050

Generating a New Token from CSSM

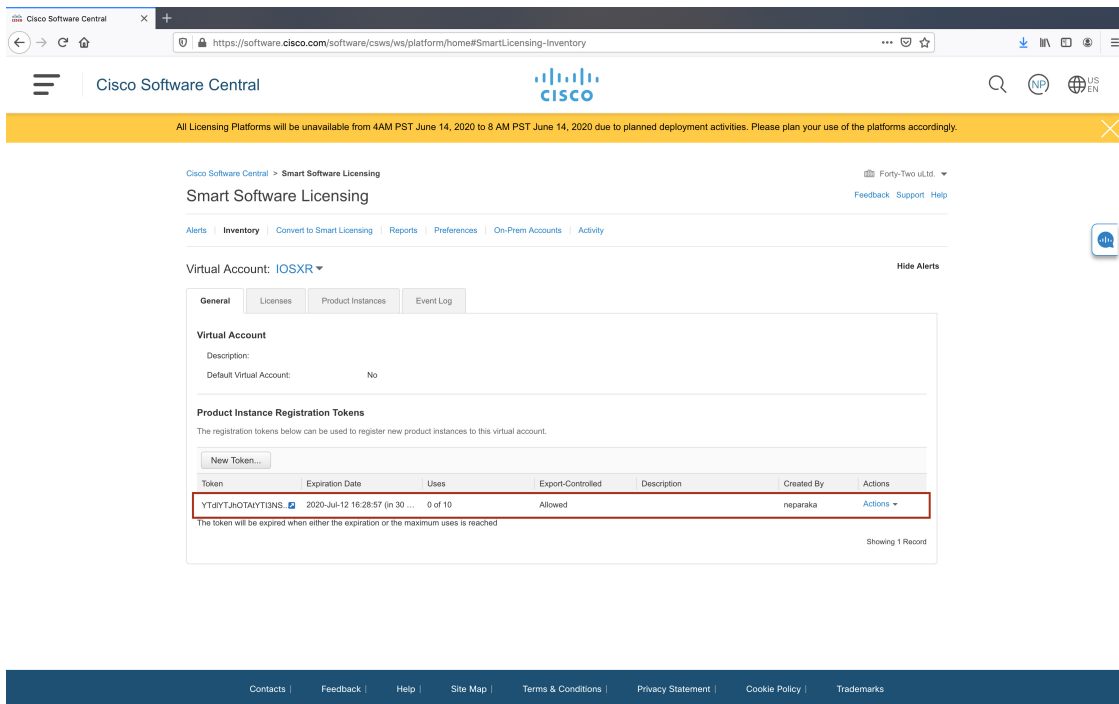


521051

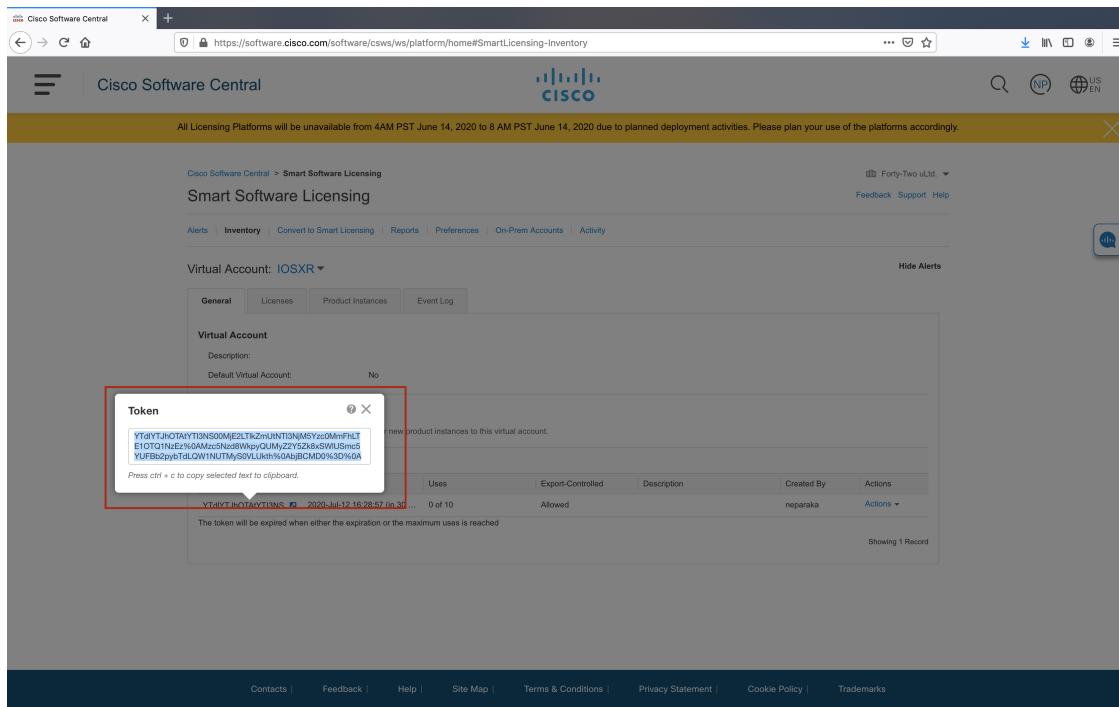
Click **Create Token**.

Step 7

After the token is created, select and copy the token to a text file.



521052



You need this token to register your router.

What to do next

See the *Registering Your Device With the Token* section.

Registering Your Device With the Token

SUMMARY STEPS

1. `license smart register idtoken token-ID`

DETAILED STEPS

	Command or Action	Purpose
Step 1	license smart register idtoken token-ID Example: <pre>license smart register idtoken \$Tl4UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0Ab1RM0z0%3D%0A</pre>	Registers Smart Licensing on the router using the registration token created in the CSSM. On successful registration, the product instance is created in the CSSM virtual account and its license usage is displayed on the CSSM.

Renewing Your Smart Licensing Registration

Your registration is automatically renewed every six months. To find the status of the license, use the **license smart renew auth** command.

As long as the license is in an 'Authorized' or 'Out-of-compliance' (OOC) state, the authorization period is renewed. Grace period starts when an authorization period expires. During the grace period or when the grace period is in the 'Expired' state, the system continues to try to renew the authorization period. If a retry is successful, a new authorization period starts.

**Note**

If the smart license renewal fails, then the product instance goes to an unidentified state and starts consuming the evaluation period.

Before you begin

Ensure that the following conditions are met to renew your smart license:

- Smart licensing is enabled.
- The router is registered.

SUMMARY STEPS

1. **license smart renew {auth | id}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	license smart renew {auth id} Example: Router# license smart renew auth	Renews your token ID or authorization with Cisco smart licensing.

Deregistering Your Router from CSSM

When a router is taken off the inventory, shipped elsewhere for redeployment, or returned to Cisco for replacement, you can deregister that router.

Before you begin

Ensure that a Layer 3 connection to CSSM is available to successfully deregister the device.

SUMMARY STEPS

1. **license smart deregister**

DETAILED STEPS

	Command or Action	Purpose
Step 1	license smart deregister Example: Router# license smart deregister	Cancels the registration of the router and sends the router into evaluation mode. All smart licensing entitlements and certificates on the corresponding platform are removed. The product instance of the router stored on CSSM is also removed.

Verifying the Smart Licensing Configuration

Use the following **show** commands to verify the default Smart Licensing configuration. If any issue is detected, take corrective action before making further configurations.

SUMMARY STEPS

1. show license status
2. show license all
3. show license status
4. show license udi
5. show license summary
6. show license platform summary
7. show license platform detail
8. show call-home smart-licensing statistics

DETAILED STEPS

	Command or Action	Purpose
Step 1	show license status Example: Router# show license status	Displays the compliance status of Smart Licensing. Following are the possible status: <ul style="list-style-type: none"> • Waiting—Indicates that the initial state after your device has made a license entitlement request. The device establishes communication with Cisco and successfully registers itself with the Cisco license manager. • Authorized—Indicates that your device is able to communicate with the Cisco license manager, and is authorized to initiate requests for license entitlements. • Out-Of-Compliance—Indicates that one or more of your licenses are out-of-compliance. Buy more licenses, or renew the existing licenses. • Eval Period—Indicates that Smart Licensing is consuming the evaluation period. Register the device with the Cisco Licensing manager, else your license expires.

	Command or Action	Purpose
		<p>Note Repetitive 'Smart Licensing evaluation expired' warning messages are displayed on the console every hour, but there is no functionality impact on the device. To stop these repetitive messages, register the device again with new a registration token.</p> <ul style="list-style-type: none"> • Disabled—Indicates that Smart Licensing is disabled. • Invalid—Indicates that Cisco does not recognize the entitlement tag as the tag is not in the database.
Step 2	show license all Example: Router# show license all	Displays all entitlements in use. The output also displays the associated licensing certificates, compliance status, Unique Device Identifier (UDI), and other details.
Step 3	show license status Example: Router# show license status	Displays the status of all entitlements in use.
Step 4	show license udi Example: Router# show license udi	Displays the Unique Device Identifier (UDI) information.
Step 5	show license summary Example: Router# show license summary	Displays a summary of all entitlements in use.
Step 6	show license platform summary Example: Router# show license platform summary	Displays the registration status and provides detailed information about the essential, advanced, and tracking license consumption in generic or vortex license model.
Step 7	show license platform detail Example: Router# show license platform detail	Displays detailed information about: <ul style="list-style-type: none"> • Licenses that can be consumed on a platform in both, generic and vortex models • The active model, whether generic or vortex model • The current count and the next consumption count of a license
Step 8	show call-home smart-licensing statistics Example: Router# show call-home smart-licensing statistics	Displays statistics of the communication between the Smart Licensing manager and the Cisco back-end using Smart Call Home. <p>Note If the communication fails or drops, check your call home configuration for any errors.</p>

Smart Licensing Configuration Examples

Example: Viewing the Call Home Profile

To display the **http Call Home profile** or the **On-Prem Call Home profile**, use the **show call-home profile all** command.

```
Router# show call-home profile all
Tue Aug 18 23:52:16.590 UTC
```

```
Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Other address(es): default
```

Periodic configuration info message is scheduled every 17 day of the month at 13:15

Periodic inventory info message is scheduled every 17 day of the month at 13:0

Alert-group	Severity
-----	-----
inventory	normal

Syslog-Pattern	Severity
-----	-----
.*	critical

```
Router# show call-home profile all
```

```
Wed Aug 19 01:55:14.974 UTC
```

```
Profile Name: CiscoTAC-1
Profile status: ACTIVE
Profile mode: Full Reporting
Reporting Data: Smart Call Home, Smart Licensing
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: http
HTTP address(es): http://10.30.110.38/Transportgateway/services/DeviceRequestHandler
Other address(es): default
```

Periodic configuration info message is scheduled every 17 day of the month at 13:15

Periodic inventory info message is scheduled every 17 day of the month at 13:0

Alert-group	Severity
-----	-----
inventory	normal

Syslog-Pattern	Severity
-----	-----
.*	critical

Example: Viewing License Information Before Registration

To display the license entitlements, use the **show license all** command:

Example: Viewing License Information Before Registration

```

Router# show license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 23 hours, 36 minutes, 0 seconds

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
=====

(ESS-100G-RTU-1):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED

(NCS-5501-TRK):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED

Product Information
=====
UDI: PID:NCS-5501,SN:FOC2137R1SL

Agent Version
=====
Smart Agent for Licensing: 4.9.6_rel/41

Reservation Info
=====
License reservation: DISABLED

To display the license usage information, use the show license usage command:

Router# show license usage

License Authorization:
  Status: EVAL MODE

```


Evaluation Period Remaining: 83 days, 23 hours, 34 minutes, 34 seconds

```
(ESS-100G-RTU-1):
Description:
Count: 1
Version: 1.0
Status: EVAL MODE
Export status: NOT RESTRICTED
```

```
(NCS-5501-TRK):
Description:
Count: 1
Version: 1.0
Status: EVAL MODE
Export status: NOT RESTRICTED
```

To display all the license summaries, use the **show license summary** command:

```
Router# show license summary
Smart Licensing is ENABLED
```

```
Registration:
Status: UNREGISTERED
Export-Controlled Functionality: NOT ALLOWED
```

```
License Authorization:
Status: EVAL MODE
Evaluation Period Remaining: 83 days, 23 hours, 33 minutes, 52 seconds
```

```
License Usage:
License                               Entitlement tag                Count Status
-----
                               (ESS-100G-RTU-1)                1 EVAL MODE
                               (NCS-5501-TRK)                  1 EVAL MODE
```

To display the license status information, use the **show license status** command:

```
Router# show license status
```

Smart Licensing is ENABLED

```
Utility:
Status: DISABLED
```

```
Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED
```

```
Transport:
Type: Callhome
```

```
Registration:
Status: UNREGISTERED
Export-Controlled Functionality: NOT ALLOWED
```

```
License Authorization:
Status: EVAL MODE
Evaluation Period Remaining: 83 days, 23 hours, 32 minutes, 57 seconds
```

```
Export Authorization Key:
Features Authorized
```

Example: Registering the Router

To register a device, use the **license smart register idtoken** command:

```
Router# license smart register idtoken
Tl4UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0Ab1RMbz0%3D%0A
```

Example: Viewing License Information After Registration

To display the license entitlements, use the **show license all** command

```
Router# show license all
Smart Licensing Status
=====

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Forty-Two uLtd.
  Virtual Account: IOSXR
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Aug 18 2020 23:51:46 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Feb 14 2021 23:51:46 UTC
  Registration Expires: Aug 18 2021 23:46:43 UTC

License Authorization:
  Status: OUT OF COMPLIANCE on Aug 18 2020 23:51:57 UTC
  Last Communication Attempt: SUCCEEDED on Aug 18 2020 23:51:57 UTC
  Next Communication Attempt: Aug 19 2020 11:51:57 UTC
  Communication Deadline: Nov 16 2020 23:46:56 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
=====

Core and Aggregation Essentials SW Right-to-Use v1.0 per 100G (ESS-100G-RTU-1):
  Description: Core and Aggregation Essentials SW Right-to-Use v1.0 per 100G
  Count: 1
  Version: 1.0
  Status: OUT OF COMPLIANCE
  Export status: NOT RESTRICTED

5501 Base Hardware Tracking PID (NCS-5501-TRK):
  Description: 5501 Base Hardware Tracking PID
  Count: 1
  Version: 1.0
  Status: OUT OF COMPLIANCE
```

```

Export status: NOT RESTRICTED

Product Information
=====
UDI: PID:NCS-5501,SN:FOC2137R1SL

Agent Version
=====
Smart Agent for Licensing: 4.9.6_rel/41

Reservation Info
=====
License reservation: DISABLED

```

To display the license usage information, use the **show license usage** command:

```

Router# show license usage
License Authorization:
  Status: OUT OF COMPLIANCE on Aug 18 2020 23:51:57 UTC

Core and Aggregation Essentials SW Right-to-Use v1.0 per 100G (ESS-100G-RTU-1):
  Description: Core and Aggregation Essentials SW Right-to-Use v1.0 per 100G
  Count: 1
  Version: 1.0
  Status: OUT OF COMPLIANCE
  Export status: NOT RESTRICTED

5501 Base Hardware Tracking PID (NCS-5501-TRK):
  Description: 5501 Base Hardware Tracking PID
  Count: 1
  Version: 1.0
  Status: OUT OF COMPLIANCE
  Export status: NOT RESTRICTED

```

To display all the license summaries, use the **show license summary** command:

```

Router# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Forty-Two uLtd.
  Virtual Account: IOSXR
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: Feb 14 2021 23:51:46 UTC

License Authorization:
  Status: OUT OF COMPLIANCE
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 19 2020 11:51:56 UTC

License Usage:

```

License	Entitlement tag	Count	Status
Core and Aggregation...	(ESS-100G-RTU-1)	1	OUT OF COMPLIANCE
5501 Base Hardware T...	(NCS-5501-TRK)	1	OUT OF COMPLIANCE

To display the license status information, use the **show license status** command:

```

Router# show license status

Smart Licensing is ENABLED

```

Example: Viewing License Information After Registration

```
Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Forty-Two uLtd.
  Virtual Account: IOSXR
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Aug 18 2020 23:51:46 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Feb 14 2021 23:51:45 UTC
  Registration Expires: Aug 18 2021 23:46:42 UTC

License Authorization:
  Status: OUT OF COMPLIANCE on Aug 18 2020 23:51:57 UTC
  Last Communication Attempt: SUCCEEDED on Aug 18 2020 23:51:57 UTC
  Next Communication Attempt: Aug 19 2020 11:51:56 UTC
  Communication Deadline: Nov 16 2020 23:46:55 UTC

Export Authorization Key:
  Features Authorized:
    <none>
```



CHAPTER 12

Configuring Zero Touch Provisioning

Zero Touch Provisioning (ZTP) works as a Third Party App (TPA) in Route-Switch Processor (RSP) and Route Processor (RP). ZTP was designed to perform two different operations:

- Download and apply an initial configuration.
- Download and execute a shell script.

If the downloaded file content starts with **!! IOS XR** it is considered as a configuration file, and ZTP performs **apply_config** action on the configuration file.

If the downloaded file content starts with **#!/bin/bash**, **#!/bin/sh** or **#!/usr/bin/python** it is considered as a script file, and ZTP executes the script.

ZTP works as following:

1. XR scripts that run on boot, invoke DHCP request.
2. DHCP server returns either a user script or configuration file.
3. Download the user script or configuration file.
4. Execute the downloaded user script or apply the downloaded configuration.

Prior to Cisco IOS XR Release 6.3.1, ZTP was executed within the default network namespace and could not access the data interfaces directly. Starting with Cisco IOS XR Release 6.3.1, ZTP is executed inside the global Virtual Routing and Forwarding (VRF) network namespace with full access to all the data interfaces.

When ZTP process encounters any error, or when ZTP quits or terminates, it revert to the initial configuration that exists before starting of ZTP process.



Note

- When initiated, ZTP checks if the system start-up configuration is applied. If startup configuration is not applied, ZTP waits for 10 minutes before proceeding.
- To boot an image through ZTP, configure the ROMMON reboot mode option to 3.

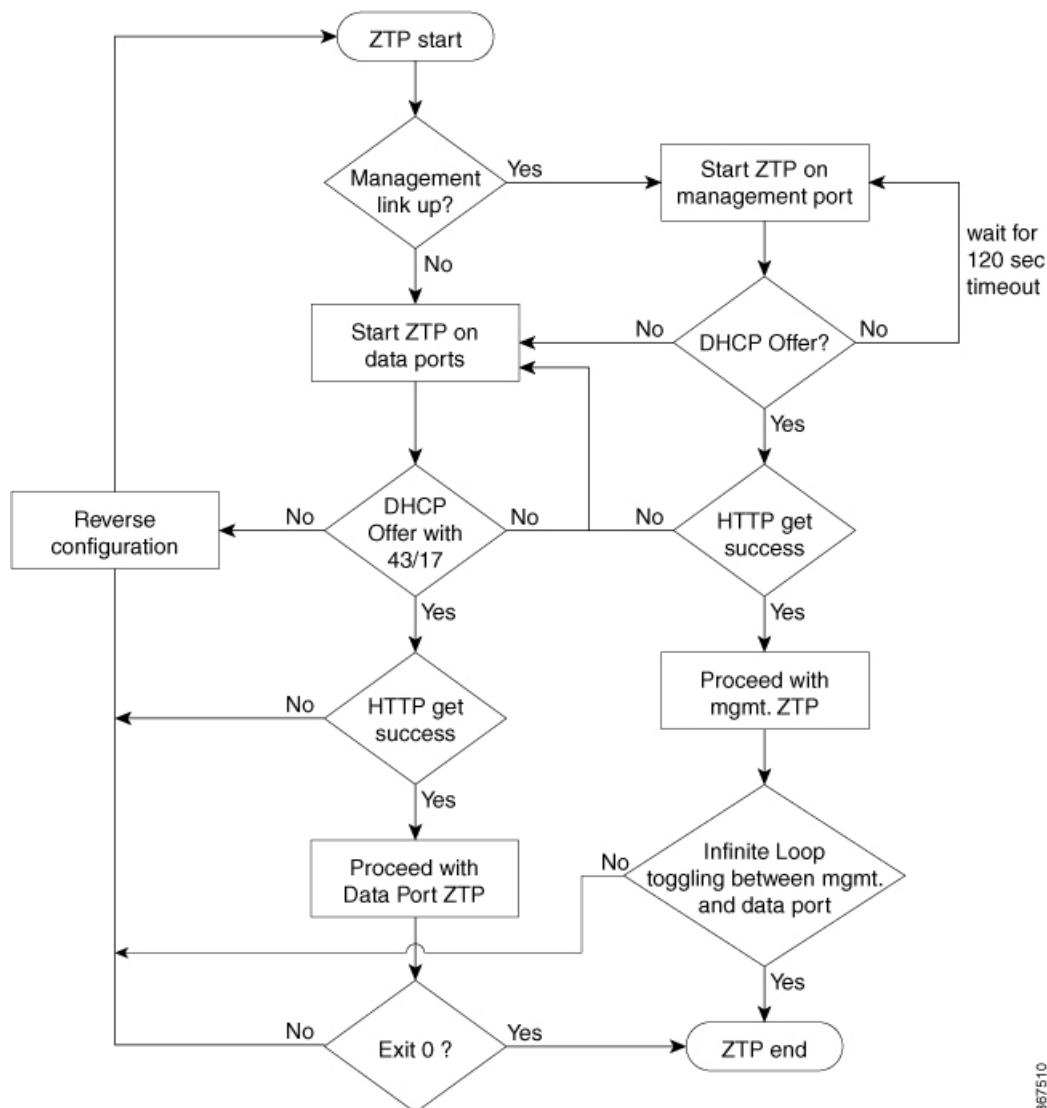
ZTP Switches between Management and Data Port

From Cisco IOS XR Release 6.5.1, during the fresh boot of a router, auto ZTP process is initiated from the management port and switches to data port. The following events cause the ZTP process to switch between management and data port:

- When ZTP does not find an active interface.
- When ZTP does not receive DHCP response and time elapsed since dhclient started is greater than 128 seconds.
- When ZTP encounters an error.

The below flow diagram illustrates the ZTP process.

Figure 7: ZTP Process Flow Sequence



367510

**Note**

- During fresh boot or manual invocation, ZTP enables IPv6 on all data port interfaces in the dataport mode.
- The auto breakout mode is not supported.
- Starting from Cisco IOS XR Release 6.5.1, auto data port is supported.

- [Manual ZTP Invocation](#) , on page 191
- [ZTP Bootscript](#), on page 192
- [ZTP Utilities](#), on page 193
- [Examples](#), on page 194

Manual ZTP Invocation

Manual Zero Touch Provisioning (ZTP) can be invoked manually via CLI commands. This manual way helps you to provision the router in stages. Ideal for testing out ZTP configuration without a reboot. If you would like to invoke a ZTP on an interfaces(data ports or management port), you don't have to bring up and configure the interface first. You can execute the **ztp initiate** command, even if the interface is down, ZTP script will bring it up and invoke dhclient. So ZTP could run over all interfaces no matter it is up or down.

Use the **ztp initiate**, **ztp breakout**, **ztp terminate**, and **ztp clean** commands to force ZTP to run over more interfaces.

- **ztp initiate**— Invokes a new ZTP DHCP session. Logs can be found in **/disk0:/ztp/ztp.log**.
- **ztp terminate**—Terminates any ZTP session in progress.
- **ztp breakout**—Will perform 4x10 breakout detection.
- **ztp clean**—Removes only the ZTP state files.

From release 6.2.3, the log file ztp.log is saved in **/var/log** folder, and a copy of log file is available at **/disk0:/ztp/ztp.log** location using a soft link. However, executing **ztp clean** clears files saved on disk and not on **/var/log** folder where current ZTP logs are saved. In order to have a log from current ZTP run, you must manually clear the ZTP log file from **/var/log/** folder.

For more information of the commands, see the ZTP command chapter in the .

This task shows the most common use case of manual ZTP invocation: invoke 4x10 breakout discovery and ZTP.

SUMMARY STEPS

1. **ztp breakout**
2. **ztp initiate dataport**

DETAILED STEPS

	Command or Action	Purpose
Step 1	ztp breakout Example: <pre>RP/0/RP0/CPU0:router# ztp breakout</pre>	Tries the 4x10 breakout on 100 GE interfaces that supports breakout and are operationally down after no-shut. If the 10x10 breakout configure brings any 10GE interface operationally up, the breakout configuration is retained; if not, the breakout configuration is reverted.
Step 2	ztp initiate dataport Example: <pre>RP/0/RP0/CPU0:router# ztp initiate dataport Wed Apr 22 10:52:24.417 UTC Invoke ZTP? (this may change your configuration) [confirm] [y/n] :y ZTP will now run in the background. ZTP might bring up the interfaces if they are in shutdown state. Please use "show logging" or look at /disk0:/ztp/ztp.log to check progress.</pre>	Invokes DHCP sessions on all data ports that are either up or could be brought up. ZTP runs in the background.

ZTP Bootscript

If you want to hard code a script to be executed every boot, configure the following.

```
conf t
  ztp bootscript /disk0:/myscript
commit
```

The above configuration will wait for the first data-plane interface to be configured and then wait an additional minute for the management interface to be configured with an IP address, to ensure that we have connectivity in the third party namespace for applications to use. If the delay is not desired, use:

```
conf t
  ztp bootscript preip /disk0:/myscript
commit
```


Note

When the above command is first configured, you will be prompted if you wish to invoke it now. The prompt helps with testing.

This is the example content of **/disk0:/myscript**:

```
#!/bin/bash
exec &> /dev/console # send logs to console
source /pkg/bin/ztp_helper.sh

# If we want to only run one time:
xrcmd "show running" | grep -q myhostname
if [[ $? -eq 0 ]]; then
```



```

        echo Already configured
    fi

    # Set the hostname
    cat >/tmp/config <<%%
    !! XR config example
    hostname myhostname
    %%
    xrapplly /tmp/config

    #
    # Force an invoke of ZTP again. If there was a username normally it would not run. This
    # forces it.
    # Kill off ztp if it is running already and suppress errors to the console when ztp runs
    # below and
    # cleans up xrcmd that invokes it. ztp will continue to run however.
    #
    xrcmd "ztp terminate noprompt" 2>/dev/null
    xrcmd "ztp initiate noprompt" 2>/dev/null

```

ZTP Utilities

ZTP includes a set of shell utilities that can be sourced within the user script. **ztp_helper.sh** is a shell script that can be sourced by the user script. **ztp_helper.sh** provides simple utilities to access some XR functionalities. Following are the bash functions that can be invoked:

- **xrcmd**—Used to run a single XR exec command:

```
xrcmd "show running"
```

- **xrapplly**—Applies the block of configuration, specified in a file:

```

cat >/tmp/config <<%%
!! XR config example
hostname nodel-mgmt-via-xrapplly
%%
xrapplly /tmp/config

```

- **xrapplly_with_reason**—Used to apply a block of XR configuration along with a reason for logging purpose:

```

cat >/tmp/config <<%%
!! XR config example
hostname nodel-mgmt-via-xrapplly
%%
xrapplly_with_reason "this is a system upgrade" /tmp/config

```

- **xrapplly_string**—Used to apply a block of XR configuration in one line:

```
xrapplly_string "hostname foo\ninterface GigabitEthernet0/0/0/0\nip address 1.2.3.44 255.255.255.0\n"
```

- **xrapplly_string_with_reason**—Used to apply a block of XR configuration in one line along with a reason for logging purposes:

```
xrapplly_string_with_reason "system renamed again" "hostname venus\n interface TenGigE0/0/0/0\n ipv4 address 172.30.0.144/24\n"
```

- **xrreplace**—Used to apply XR configuration replace in XR namespace via a file.

```
cat rtr.cfg <<%%
!! XR config example
hostname nodel-mgmt-via-xrreplace
%%
xrreplace rtr.cfg
```

- **admincmd**—Used to run an admin CLI command in XR namespace. Logs can be found in **/disk0:/ztp/ztp_admincmd.log**

```
admincmd running [show platform]

ztp-user connected from 192.0168.0.1 using console on host
sysadmin-vm:0_RP0# show platform | nomore
Tue Jan 30 23:12:30.757 UTC
Location Card Type HW State SW State Config State
-----
0/RP0 NCS-5501 OPERATIONAL OPERATIONAL NSHUT
0/FT0 NCS-1RU-FAN-FW OPERATIONAL N/A NSHUT
0/FT1 NCS-1RU-FAN-FW OPERATIONAL N/A NSHUT
0/PM0 NCS-1100W-ACFW OPERATIONAL N/A NSHUT
0/PM1 NCS-1100W-ACFW OPERATIONAL N/A NSHUT
```

- **xrapply_with_extra_auth**—Used to apply XR configuration that requires authentication, in XR namespace via a file. The **xrapply_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups.

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrapply_with_extra_auth >/tmp/config
```

- **xrreplace_with_extra_auth**—Used to apply XR configuration replace in XR namespace via a file The **xrreplace_with_extra_auth** API is used when configurations that require additional authentication to be applied such as alias, flex groups

```
cat >/tmp/config <<%%
!! XR config example
alias exec alarms show alarms brief system active
alias exec version run cat /etc/show_version.txt
%%
xrreplace_with_extra_auth >/tmp/config
```

Examples

ZTP logs its operation on the flash file system in the directory **/disk0:/ztp/**. ZTP logs all the transaction with the DHCP server and all the state transition. Prior executions of ZTP are also logged in **/disk0:/ztp/old_logs/**.

The following example displays the execution of a simple configuration script downloaded from a data interface using the command **ztp initiate interface Ten 0/0/0/0 verbose**, this script will unshut all the interfaces of the system and configure a load interval of 30 seconds on all of them.

```
#!/bin/bash
#####
# *** Be careful this is powerful and can potentially destroy your system ***
# *** !!! Use at your own risk !!! ***
#
# Script file should be saved on the backend HTTP server
#####

source ztp_helper.sh
config_file="/tmp/config.txt"
interfaces=$(xrcmd "show interfaces brief")

function activate_all_if(){
    arInt=$(echo $interfaces | grep -oE '(Te|Fo|Hu) [0-9]*/[0-9]*/[0-9]*/[0-9]*')
    for int in ${arInt[*]}; do
        echo -ne "interface $int\n no shutdown\n load-interval 30\n" >> $config_file
    done
    xrapplly_with_reason "Initial ZTP configuration" $config_file
}

### Script entry point
if [ -f $config_file ]; then
    /bin/rm -f $config_file
else
    /bin/touch $config_file
fi
activate_all_if;
exit 0
```

The following example displays the ZTP logging output:

```
Oct 11 11:05:38 172.30.0.54 ztp-script: Hello from ncs-5001-c !!!
Oct 11 11:05:40 172.30.0.54 ztp-script: current=6.1.1, desired=6.1.1
Oct 11 11:05:40 172.30.0.54 ztp-script: Version match, proceeding to configuration
Oct 11 11:05:41 172.30.0.54 ztp-script: Starting autoprovision process...
Oct 11 11:05:42 172.30.0.54 ztp-script: ### XR K9SEC INSTALL ###
Oct 11 11:05:44 172.30.0.54 ztp-script: ### Downloading complete ###
Oct 11 11:05:55 172.30.0.54 ztp-script: Waiting for k9sec package to be activated
Oct 11 11:06:01 172.30.0.54 ztp-script: ### XR K9SEC INSTALL COMPLETE ###
Oct 11 11:06:03 172.30.0.54 ztp-script: ### Installing midnight commander ###
Oct 11 11:06:04 172.30.0.54 ztp-script: ### Downloading system configuration ###
Oct 11 11:06:05 172.30.0.54 ztp-script: ### Downloading system configuration complete ###
Oct 11 11:06:06 172.30.0.54 ztp-script: ### Applying initial system configuration ###
Oct 11 11:06:11 172.30.0.54 ztp-script: !!! Checking for errors !!!
Oct 11 11:06:14 172.30.0.54 ztp-script: ### Applying system configuration complete ###
Oct 11 11:06:15 172.30.0.54 ztp-script: Autoprovision complete...
```

