General Administration Guide on Cisco ASR 9000 Series Routers, Cisco IOS XR Releases

First Published: 2024-01-01

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.

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

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

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

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

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

CHAPTER 1

About General Administration Documentation

Welcome to the remodeled *General Administration on Cisco ASR 9000 Series Routers* for all Cisco IOS XR releases.

Release-agnostic Document

This remodeled content experience helps you navigate or search the content of interest with ease. To enhance your experience of our product knowledge base, we have restructured the previous release-specific *System Management Configuration Guide for Cisco ASR 9000 Series Routers* to *General Administration on Cisco ASR 9000 Series Routers, Cisco IOS XR Releases*. This document serves as your comprehensive compilation of information related to the general administration of your router right after you setup your router.

To ensure continued relevance, we will regularly update this document to align with the latest features and releases.

Where to begin

To initiate exploring General Administration, we recommend you to review the Feature, Release, and Platform Matrix for General Administration. This resource offers valuable insights into features supported not only on the ASR 9000 Series Routers but across other IOS XR routing products, facilitating a comprehensive understanding and navigation across our documents.

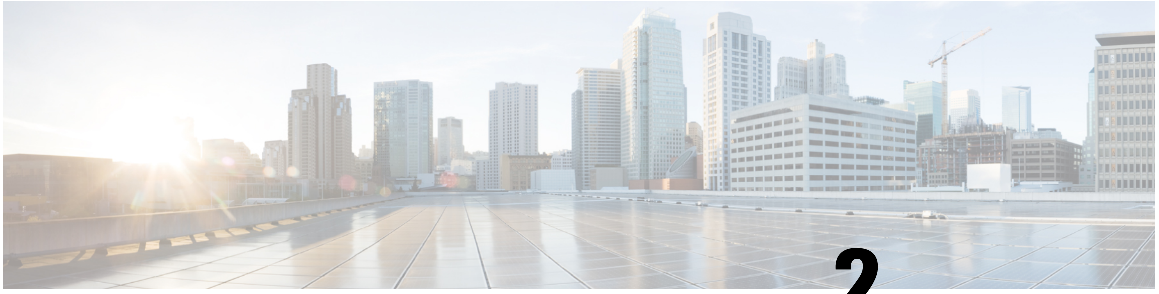
Releases Supported

The document is relevant for the following releases:

- IOS XR Release 7.11.1
- IOS XR Release 7.10.1
- IOS XR Release 7.9.2
- IOS XR Release 7.9.1
- IOS XR Release 7.8.2
- IOS XR Release 7.8.1
- IOS XR Release 7.7.2
- IOS XR Release 7.7.1

- IOS XR Release 7.5.3
- IOS XR Release 7.5.2
- IOS XR Release 7.5.1
- IOS XR Release 7.4.2
- IOS XR Release 7.4.1
- IOS XR Release 7.3.4
- IOS XR Release 7.3.3
- IOS XR Release 7.3.2
- IOS XR Release 7.3.1
- IOS XR Release 6.9.2
- IOS XR Release 6.9.1
- IOS XR Release 6.8.2
- IOS XR Release 6.8.1

Cisco IOS XR Releases prior to those listed here have reached the End of Extended Software Maintenance Date. To access the notification, please visit the End-of-Life and End-of-Sale Notices page.



CHAPTER 2

Features Introduced in Cisco IOS XR Products and Releases

This table summarizes the features enhanced and introduced for General Administration.

- Feature, Release, and Platform Matrix for General Administration, on page 3

Feature, Release, and Platform Matrix for General Administration

Use this ready reckoner to locate features you're interested in and map their availability across platforms and releases.

Table 1: Feature, Release, and Platform Matrix

Feature Name	ASR 9000 Series Routers	Other XR Routing Platforms
Increasing Commit LImit	ASR 9000, R24.2.1	Cisco 8000, R24.2.1 NCS 5500, R24.2.1
Auto-Save and Copy Router Configuration Using Public Key Authentication	ASR 9000, R7.10.1	Cisco 8000, R7.10.1 NCS 5500, R7.10.1
Support for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) options in the Copy command	ASR 9000, R7.9.1	Cisco 8000, R7.9.1 NCS 5500, R7.9.1
Auto-Save with Secure File-Transfer and Additional Configurable Parameters	ASR 9000, R7.9.1	Cisco 8000, R7.9.1 NCS 5500, R7.9.1

CHAPTER 3

Scale Profiles and Feature Profiles

Scale profiles in routers optimize performance by allowing customization for different network demands, such as high Layer 2 scale or a large number of Layer 3 routes. Feature profiles determine available software features, with the default profile supporting all features except PBB and the Layer 2 profile including PBB support but lacking IPv6, RPF, or Netflow.

TCAM is a critical resource in Cisco routers, and router profiles determine how this resource is allocated to optimize the router's performance for specific tasks. By selecting the appropriate profile, network administrators can ensure that the router operates efficiently and meets the specific needs of their network.

TCAM, scale profiles, and feature profiles optimize router performance, scalability, and security in diverse networking environments.

Scale Profiles

Scale profiles help you tune your router that is running Cisco IOS XR software. Profiles help you run the router more efficiently based on your requirements.

Market segment types or network architectures can place different scale demands on the router. Therefore, it’s important to configure the **scale profile** so that your router works efficiently.

These are some requirements when setting a scale profile:

- Use of the router as a Layer 2 transport device requires high Layer 2 scale numbers.
- Use of the router primarily as a Layer 3 device that provides Layer 3 virtual private network (VPN) services requires a high number of Layer 3 routes.

Scale Profile Types

There are three scale profiles available on your router:

Default Scale Profile

The default scale profile supports deployments that require large Layer 2 MAC tables (up to 512,000 entries) and a relatively small number of Layer 3 routes (less than 512,000).

Layer 3 Scale Profile

The Layer 3 Scale Profile supports deployments that require smaller Layer 2 MAC tables (less than 128,000 entries) and relatively higher Layer 3 routes (up to 1 million).

Layer 3 XL Scale Profile

The Layer 3 XL Scale Profile supports deployments that require minimal Layer 2 functionality and a large number of Layer 3 routes (up to 1.3 million).

Note that the support for up to 1.3 million routes is split into IPv4 scaled support and IPv4/IPv6 scaled support. You can configure up to 1.3 million IPv4 routes, or up to 1 million IPv4 routes with 128,000 IPv6 routes.

Restrictions with Layer 3 XL Scale Profile

- Video monitoring isn’t supported with the Layer 3 XL scale profile.

Configure Scale Profile

Recommendations and Guidelines

- We recommend that you configure scale profiles in the administration configuration mode and remove any L3 scale profiles committed via the global configuration mode.
- Scale profile settings in the administration configuration override scale profile settings in the global configuration.
- If the scale profile is set only in the global configuration, the setting takes effect.
- Once you configure the scale profile, you must use the **reload location all** command to reload the device, or the line cards to enable the profile.
- You can increase the memory available for BGP if you configure Layer 3 XL profile on the router.
- Configuring the layer 3 XL profile reduces the memory available for other processes.
- To activate the new profile, you must manually reboot the system.

Set Scale Profile

The tasks in this module describes how to set the scale profile on your router.

Step 1 To set the scale profile on the router, use the **hw-module profile scale** command in the Administration Configuration mode.

Example:

This example shows how to configure Layer 3 profile on the router.

```
Router# admin
Router(admin)# configure
Router(admin-config)# hw-module profile scalel xl
Router(admin-config)# commit
```

You can configure the Layer 3 XL profile on the router for BGP using the **scale l3xl** keyword to increase the memory.

Step 2 Reload the line cards to enable the profile

```
Router# reload location all
```

Step 3 To verify that the configured scale profile is enabled, use the **show hw-module profile scale** command which displays the active scale profile. If the active scale profile is different from what was configured, then the line cards were not reloaded as required.

```
Router# show hw-module profile scale
```

You can verify the memory for BGP and the other processes using the following commands before and after the configuration:

- **show processes memory detail**
- **show bgp process performance-statistics**: This command is available only from Cisco IOS XR Release 6.1.x onwards.

Feature Profiles

To allow sufficient computation capabilities within the router, the available features within the Cisco IOS XR software image are bundled. A feature profile determines which bundle of features is available for you to use.

Feature Profile Types

Default Profile

Supports all Cisco IOS XR software features except for IEEE 802.1ah provider backbone bridge (PBB).

Layer 2 Profile

Layer 2 Profile supports all Cisco IOS XR software features including IEEE 802.1ah PBB.

Restrictions with Layer 2 Profile

- Doesn’t support IPv6, reverse-path forwarding (RPF) or Netflow.
- This feature profile is supported only on 1st Generation ASR 9000 Series Line Cards- Ethernet Line Cards, and 4th Generation ASR 9000 Series Line Cards - High Density Ethernet Line Cards. Therefore, this limitation is applicable only on those line cards; not on 2nd generation line cards and 3rd generation line cards.

Configure Feature Profile

Prerequisites and Recommendations

- Before deploying your router you should determine that the feature profile is consistent with the features that you need to use. If it is not, use this task to configure a different profile.
- If the feature profile that you have configured on your router does not support a feature that you have configured, warning messages are displayed on the console, and the feature does not work.
- A configured feature profile takes effect only after you reload all the line cards on the router.

Set Feature Profile

The tasks in this module describes how to set the feature profile on your router.

Step 1 To set the feature profile on your router, use the **hw-module profile feature** command in the Administration Configuration mode.

Example:

```
Router# admin
Router(admin)# configure
Router(admin-config)# hw-module profile feature l2
Router(admin-config)# commit
```

Step 2 You must reload the router or line cards to enable the profile.

```
Router# reload location all
```

Step 3 To verify that the configured feature profile is enabled, use the **show hw-module profile feature** command which displays the active feature profile. If the active feature profile is different than what was configured, the line cards or router were not reloaded as required.

Relationship Between Scale and Feature Profiles

While there are no restrictions on your choice of scale and feature profiles in relation to one another, we suggest using them together, as outlined here.

Table 2: Relationship Between Scale and Feature Profiles

	Default Feature Profile	**Layer 2 Feature Profile**
Default Scale Profile	Up to 512 K Layer 3 Cisco Express Forwarding (CEF) scale	Provider backbone bridge
Layer 2 Scale Profile	Up to 1.0 M Layer 3 CEF scale Less than 128 K MAC entries	Not Recommended
Layer 3 XL Scale Profile	Up to 1.3 M Layer 3 CEF scale	Not Recommended

Other pairs are not recommended. Note that the Layer 3 XL scale profile does not support video monitoring.

Verify Scale Profile or Feature Profile Configurations

To verify the configured scale profile or feature profile, you may perform the following steps:

Step 1 If you see warning messages in the console indicating that the active feature profile does not match the configured profile, you must reload the affected line card so that the configured profile matches the active profile.

Example:

```
Router# Nov 5 02:50:42.732 : prm_server[236]: Configured 'hw-module profile feature l2' does not
match active 'hw-module profile feature default'.
You must reload this line card in order to activate the configured profile on this card or you must
 change the configured profile.
```

Step 2 If you see warning messages in the console indicating that some features do not match the feature profile, you should either change the feature profile configuration, or remove the non-supported features.

Example:

```
Router# Nov 5 02:50:42.732 : prm_server[236]: Active 'hw-module profile feature l2' does not support
 IPv6, RPF, or Netflow features. Please remove allunsupported feature configurations.
```

TCAM Profile

The TCAM (Ternary Content Addressable Memory) profile is a configuration setting that determines how TCAM resources are allocated for various functions such as routing, access control lists (ACLs), and Quality of Service (QoS) policies. These profiles help optimize the router's performance by prioritizing TCAM usage based on the specific needs of the network. Administrators can select or customize TCAM profiles to ensure efficient handling of critical operations, thereby enhancing the overall efficiency and reliability of the network. Proper TCAM profile management is essential for maintaining high performance in large-scale and complex network environments.

Recarve iTCAM Profile

Both A99-12X100GE and A9K-4X100GE line cards have an internal TCAM of 5MB. You can recarve internal TCAM partition at a Global Configuration level to increase entries on the L2 table and V6 table. Recarving of the TCAM partition helps in the optimal and efficient utilisation of the available memory.

Table 3: Recarving iTCAM profile

Supported on	Default Limit (to-default)	Recarving Limit (to-profile-se1)
L2 table	1K entries	4K entries
V4 table	24K entries	15K entries
V6 table	1.75K entries	3.25K entries

Restrictions for iTCAM Profile

- This configuration is supported only on A99-12X100GE and A9K-4X100GE line cards.
- For 32-bit IOS-XR, perform this configuration in the Admin Configuration mode.
- For 64-bit IOS-XR perform this configuration in the Global Configuration mode.
- Unless you reload the line cards after the configuration of iTCAM profile on the linecards, the configuration does not take effect.

Configure iTCAM Profile

Recarves the internal TCAM partitions for service edge and sets the L2 scale to 4K entries in the L2 table and V6 scale to 3.5K entries in the V6 table by adjusting 24K V4 entries in the V4 table.

Step 1 Enter the global configuration mode to configure the iTCAM profile for the line cards as **to-profile-se1**.

Example:

```
Router# configure
Router(config)#
```

Step 2 Recarve TCAM partition of line cards and change the entries to accommodate more L2 or V6 entries in the L2 table and V6 table. Reload the A99-12X100GE and A9K-4X100GE line cards in the chassis.

Example:

```
Router(config)# hw-module profile itcam to-profile-se1 location 0/0/CPU0
In order to activate this new internal tcam partition profile, you must manually reload the line
card.
Router(config)# commit
```

Note If you configure the iTCAM profile as **to-default**, it enables default TCAM entries present in the linecards.

Step 3 Verify the increase in the number of L2 and V6 entries in the L2 and V6 tables respectively for line cards on an interface, using the **show prm server tcam summary all all detail all location** *location* command.

Example:

```
Router# show prm server tcam summary all all detail np3 location 0/0/CPU0


                Node: 0/0/CPU0:
----------------------------------------------------------------

TCAM summary for NP3:

  TCAM Logical Table: TCAM_LT_L2 (1)
    Partition ID: 0, valid entries: 2, free entries: 22
    Partition ID: 1, valid entries: 0, free entries: 24
    Partition ID: 2, valid entries: 0, free entries: 24
    Partition ID: 3, valid entries: 0, free entries: 2012
    Partition ID: 4, valid entries: 2, free entries: 2010
  TCAM Logical Table: TCAM_LT_ODS2 (2), max entries: 15360, num free: 15237
    Application ID: NP_APP_ID_IFIB (0).
      VMR ID:    1, used entries:   45, allocated entries:  123
      Total vmr_ids per app id: 1, Total used entries per app id: 45 Total allocated entries: 123
    Application ID: NP_APP_ID_QOS (1)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_ACL (2)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_AFMON (3)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_LI (4)
      VMR ID:    2, used entries:    0, allocated entries:    0
      Total vmr_ids per app id: 1, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_PBR (5)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
  TCAM Logical Table: TCAM_LT_ODS8 (3), max entries: 3328, num free: 3295
    Application ID: NP_APP_ID_IFIB (0).
      VMR ID:    1, used entries:   33, allocated entries:   33
      Total vmr_ids per app id: 1, Total used entries per app id: 33 Total allocated entries: 33
    Application ID: NP_APP_ID_QOS (1)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_ACL (2)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_PBR (5)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
    Application ID: NP_APP_ID_EDPL (6)
      Total vmr_ids per app id: 0, Total used entries per app id: 0 Total allocated entries: 0
```

In the output, you can see that the L2 entries have increased to 4K in the L2 table, V4 entries have reduced to 1.5K in the V4 table, and V6 entries have increased to 3.5K in the V6 table.

L2 TCAM Profile

Table 4: Feature History Table

Feature Name	Release Information	Feature Description
Higher Single-Tagged VLAN Subinterface Capacity with Layer 2 TCAM Profile on Cisco ASR 9000 Series 5th Generation High-Density Multi-Rate Line Cards	Release 24.2.1	This feature allows you to configure the L2 TCAM profile that facilitates higher scale capacity for single-tagged VLAN subinterfaces on the Cisco ASR 9000 Series 5th generation high-density multi-rate line cards. With this configuration, the feature supports up to 40,000 Single-tagged Layer 2 VLAN subinterfaces. **CLI:** This feature introduces the **hw-module profile itcam lightspeed l2tcam** command.

The **hw-module profile itcam lightspeed l2tcam profile1-dot1q** profile supports up to 40,000 single-tagged Layer 2 VLAN subinterfaces.

To revert to the default configuration that supports up to 40,000 double-tagged (Q-in-Q) Layer 2 VLAN subinterfaces, use the **no** form of the **hw-module profile itcam lightspeed l2tcam profile1-dot1q** command.

How to configure the L2 TCAM Profile

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 **hw-module profile itcam lightspeed l2tcam profile1-dot1q location** *location*

Example:

```
RP/0/RSP0/CPU0:router(config)# hw-module profile itcam lightspeed l2tcam profile1-dot1q location
0/2/CPU0

In order to activate this internal tcam partition configuration, you must manually reload the line
card.
This command must be used with caution and only when recommended by Cisco.
```

Specifies the l2tcam profile for the router.

- **profile1-dot1q**—Enables the configuration that supports 40,000 single-tagged Layer2 VLAN sub-interfaces in the specified location.

  Important The **profile-dot1q** profile supports 40,000 single-tagged Layer 2 VLAN sub-interfaces and 16,000 double-tagged Layer 2 VLAN sub-interfaces.

- **location** *node-id*—Specifies a configured location.

Important You must reload the line card for this configuration to take effect.

Use the **no** form of the **profile-dot1q** profile to revert to the default configuration that supports up to 40,000 double-tagged (Q-in-Q) Layer 2 VLAN sub-interfaces and 16,000 single-tagged Layer 2 VLAN sub-interfaces.

Step 3 Use the **commit** or **end** command.

commit —Saves the configuration changes and remains within the configuration session.

end —Prompts user to take one of these actions:

- **Yes** — Saves configuration changes and exits the configuration session.
- **No** — Exits the configuration session without committing the configuration changes.
- **Cancel** — Remains in the configuration mode, without committing the configuration changes.

Step 4 **show running-config**

Example:

```
RP/0/RSP0/CPU0:router#show running-config | i l2tcam
hw-module profile itcam lightspeed l2tcam profile1-dot1q location 0/2/CPU0
```

Displays the configured l2tcam profile.

Step 5 **reload location** *node-id*

Example:

```
RP/0/RSP0/CPU0:router# reload location 0/2/CPU0
```

Reloads the specified location on the line cards in the chassis.

CHAPTER 4

XML Manageability

XML Manageability in Cisco IOS XR Software enables XML agent services for parsing, generating, and validating XML documents. It supports programmatically working with XML, allows custom functions for XML tags, and validates document types using DTD. The XML API provides a programmable interface for router configuration and monitoring, accessible via TCP, SSL, or VRF instances. Configuration involves enabling XML agents, specifying request method (TCP or SSL), setting iteration size and idle timeout, configuring processing capabilities, and enabling VRF for communication.

XML Manageability Overview

You can enable Extensible Markup Language (XML) agent services on the routers running Cisco IOS XR Software. The XML Parser Infrastructure provides parsing and generation of XML documents with Document Object Model (DOM), Simple 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.

The Cisco IOS XR XML API provides a programmable interface to the router by external management applications. This interface provides a mechanism for router configuration and monitoring using 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.

Configure XML Manageability

To configure XML manageability, you must configure an XML SSL agent to communicate through VRFs.

Step 1 Enable the XML requests over a dedicated TCP connection or a Secure Socket Layer (SSL) for the dedicated XML agent, using the **xml agent** command. You can also configure the *iteration on size*, *session timeout*, and *throttle memory*.

Example:

```
Router:# config
Router(config):# xml agent ssl
Router(config-xml-agent)# iteration on size 500
Router(config-xml-agent)# session timeout 5
Router(config-xml-agent)# throttle memory 300
Router(config-xml-agent)# commit
```

Similarly, you can use the **xml agent tcp** command to enable the XML requests over a dedicated TCP connection."

Step 2 In this example, we've configured the XML agent to receive and send messages via VRF1 and VRF2.

Example:

```
Router# config
Router(config)# xml agent
Router(config-xml-agent)# vrf VRF1
Router(config-xml-agent)# vrf VRF2
Router(config-xml-agent)# commit
```

CHAPTER 5

Physical and Virtual Terminals

You can access and manage the configuration and settings of a router using Physical and Virtual Terminals.

Physical terminals on routers are the physical ports or interfaces that provide connectivity for devices. Ethernet Ports, Serial Ports, Console Ports and USB ports are few examples of physical terminal. 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.

Virtual terminals or **vty** lines are virtual lines that allow connecting to the device using telnet or Secure Shell (SSH). These virtual terminals can be accessed remotely over a network. The Cisco IOS XR software assigns a **vty** identifier to **vtys** according to the order in which the **vty** connection has been established.

Physical Terminals

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.

Virtual Terminals

Virtual terminal lines are used to allow remote access to the router. The virtual terminal or **vty** lines are virtual lines that allow connecting to the device using telnet or Secure Shell (SSH).

Physical location is not applicable for virtual terminals. 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.

vty Pools Supported by Default

The Cisco IOS XR software supports the following vty pools by default:

Default vty Pools

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.

User-defined vty Pool

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.

Guidelines for vty Pools

- 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.
- You can resize the default vty pool by increasing the range of vtys that compose the default vty pool.
- The vty range from 5 through 99 can reference a user-defined vty pool.
- 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.
- 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

Line Templates

Configuration templates allow you to create a name that represents a group of configuration commands. Likewise, line templates represent a set of attributes that can be applied to multiple terminal lines. It greatly reduces the time and simplifies the process of configuring multiple terminal lines.

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

Line Templates Types

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 Template

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

Line Template Guidelines

- 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 Global Configuration mode to enter line template configuration mode for the console template.
- Modify the template for virtual lines by configuring a user-defined template with the **line** *template-name* command, configuring the terminal attributes for the user-defined template from line template configuration, and applying the template to a range of virtual terminal lines using the **vty pool** command.
- The default EXEC timeout for the default line template is 10 minutes.
- The default width for the default line template is 80 characters.
- The default length for the default line template is 24 lines.
- Attributes not defined in the console template, or any virtual template, are taken from the default template.
- The default session-limit for line template is applicable to Telnet sessions only. It is not applicable for SSH sessions.

Configure Physical and Virtual Terminals

To modify the terminal attributes for the console and default line templates, follow these steps in Global configuration mode

You can use the console or default options while configuring the line templates

Modify Console Line Template

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

Step 1 **Example:**

```
Router# configure
Router(config)# line console
Router(config-line)# exec-timeout 0 0
Router(config-line)# escape-character 0x5a
Router(config-line)# session-limit 10
Router(config-line)# disconnect-character 0x59
Router(config-line)# session-timeout 100
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# commit
```

Step 2 To verify that the terminal attributes for the console line template have been applied to the console, use the **show line** command:

Example:

```
Router# show line console location 0/0/CPU0
```

Modify Default Template

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

Example:

```
Router# configure
Router(config)# line default
Router(config-line)# exec-timeout 0 0
Router(config-line)# width 512
Router(config-line)# length 512
Router(config-line)# commit
```

Create or Modify vty Pools

The two primary steps in working with templates are creating templates and applying templates.

Before you begin

Before creating or modifying the vty pools, enable the telnet server using the **telnet server** command in Global Configuration mode. See *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers* and *IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers* for more information.

Step 1 Configure number of allowable telnet servers, upto a maximum of 100 telnet servers.

Example:

```
Router# configure
Router#(config) telnet ipv4 server max-servers 10
Router#(config) line template 1
Router#(config-line) exit
Router#(config) vty-pool default 0 5 line-template default
Router#(config) commit
```

Step 2 **Example:**

Monitor Terminals and Terminal Sessions

The optional tasks in this module describes how to monitor terminals and terminal sessions on your router.

Step 1 Display the terminal parameters of terminal lines.

Example:

```
Router# show line
```

Step 2 Display the terminal attribute settings for the current terminal line

Example:

```
Router# show terminal
```

Step 3 Displays information about the active lines on the router.

Example:

```
Router# show users
```

CHAPTER 6

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.

CDP Overview

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.

CDP runs on all media that support the 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.

CDPv2

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 for more rapid error tracking, ultimately reducing costly downtime. The console or a logging server receives the reported error messages. These messages can cover instances of unmatching native VLAN IDs (IEEE 802.1Q) on connecting ports, and unmatching port duplex states between connecting devices.

By default, when CDP is enabled, the router sends CDPv2 packets. CDP also sends and receives CDPv1 packets if the device with which CDP is interacting doesn't process CDPv2 packets.

MIB: CISCO-CDP-MIB

The CDP MIB facilitates these benefits:

- Permit network management applications to learn the device type.
- Enable network management applications to ascertain the SNMP agent address of neighboring devices.
- Send SNMP queries to these devices.

TLV Definitions for CDPv2 Advertisements

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

Table 5: Definitions of TLV

TLV	Definition
Device-IDTLV	Identifies the device name in the form of a character string.
AddressTLV	Contains a list of network addresses of both receiving and sending devices.
Port-IDTLV	Identifies the port on which the CDP packet is sent.
CapabilitiesTLV	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.
PlatformTLV	Describes the hardware platform name of the device, for example, Cisco 4500.
VTPManagement 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.
NativeVLAN 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/HalfDuplex TLV	Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.

Enable CDP

Perform the following steps to enable CDP.

Step 1 Check if CDP is installed on your router by using **show install active summary.show install active summary.**CDP is an optional package.

```
Router#show install active summary
Label : 7.3.1.28I
Active Packages: 1
asr9k-xr-7.3.1.28I version=7.3.1.28I [Boot image]
```

Step 2 Enable CDP on a router using the **cdp** command. You must first enable CDP globally on the router and then enable CDP on a per-interface basis.

```
Router#configure
Router(config)#cdp
Router(config)#int TenGigE 0/5/0/11/1
Router(config-if)#cdp
Router (config-if)#commit
```

Step 3 Modify the default attributes of CDP such as default version, hold-time setting, and timer settings.

```
Router#configure
Router(config)#cdp advertise v1
Router(config)#cdp holdtime 30
Router(config)#cdp timer 20
Router(config)#commit
```

Monitor CDP

Monitoring CDP is crucial for network administrators to maintain an accurate network topology, ensure device inventory accuracy, troubleshoot network connectivity issues, enhance network security, and optimize network performance. You can monitor CDP with the following tasks:

View Neighbours Discovered Through CDP

You can display information about a specific neighboring device or all neighboring devices discovered using **show cdp entry** command.

In this example, the optional entry argument is used to display entry information related to a specific CDP neighbor.

```
Router#show cdp entry asr9k-rtr1
-------------------------
Device ID: asr9k-rtr1
SysName : asr9k-rtr1
Entry address(es):
IPv4 address: 192.0.2.1
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: 192.0.2.1
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: 192.0.2.1
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
```

Learn Interface Enabled with CDP

You can display information about the interface on which CDP is enabled using the **show cdp interface** command.

In this example, CDP information related to Packet over SONET/SDH (POS) interface 0/5/0/11/1 is displayed.

```
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
```

Display Information About Neighbours Using CDP

You can display detailed information about neighboring devices discovered using CDP.

Step 1 In the following example, you can see the detailed information displayed about neighboring devices using CDP.

```
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
```

Step 2 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.

```
Router#show cdp neighbors TenGigE 0/5/0/11/1 detail
Device ID: asr9k-rtr1 SysName : asr9k-rtr1 Entry address(es):

IPv4 address: 192.0.2.1

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
```

Display Traffic Gathered Between Devices

You can display information about the traffic gathered between devices using CDP by using the **show cdp traffic** command.

Step 1 In the following example, you can see the information displayed about the traffic gathered between devices using CDP.

```
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: 1

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

Step 2 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.

```
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
```

CHAPTER 7

Disk Mirroring

Note We recommend using the disk mirroring feature only on routers with route processors (RPs) or route switch processors (RSPs) that use hard disk drive (HDD); not on the ones with RPs or RSPs that use solid-state drive (SSD).

The Route Switch Processor (RSP) card has a primary storage device that is used to store installation packages and configuration files. This primary storage device is referred to as the primary boot device and is essential for booting the RSP and its normal operation.

Disk mirroring replicates the critical data on the primary boot device onto another storage device on the same RSP, henceforth referred to as the secondary device. If the primary boot device fails, applications continue to be serviced transparently by the secondary device, hence avoiding a switchover to the standby RSP. The failed primary storage device can be replaced or repaired without disruption of service.

Disk mirroring should only mirror critical data on the primary boot device onto a secondary storage device. Disk Mirroring shouldn't mirror any noncritical data such as logging data.

Partitioning Disk Devices

To separate critical data from noncritical data, the disk devices need to be partitioned.

- disk0 is partitioned to disk0: and disk0a:
- disk1is partitioned to disk1: and disk1a:

Disk0: and disk1: are used for critical data whereas, disk0a: and disk1a: are used to store logging data and other noncritical data.

Disk Partition Size

Before you can configure disk mirroring on the RSP, you must have partitioned the secondary storage device. The sizes of disk partitions are related to the total disk size, and are provided in the following table.

Table 6: Size of Disk Partitions in Relation to Size of Disk

Size of Disk	Primary Partition Percentage	Secondary Partition Percentage
Less than 900 MB	Partitioning not supported	Partitioning not supported
900 MB to 1.5 GB	80%	20%
1.5 GB to 3 GB	60%	40%
More than 3 GB	50%	50%

Note The primary partition on the secondary storage device must be large enough to contain all data on the primary boot device. This can be an issue if the primary boot device hasn't yet been partitioned. For example, in the situation where both the primary boot device and the secondary storage device are 1 GB in size. The primary boot device contains 950 MB of data, and the secondary storage device is already partitioned to 800 MB in the primary partition and 200 MB in the secondary partition. In such cases, the 950 MB of data from the primary boot device doesn't fit on the secondary storage device because of the partition. Such a configuration is rejected and an error is displayed. Replace the secondary storage device with a higher capacity device.

Configure Disk Mirroring

Step 1 Before enabling disk mirroring, the following conditions must be met:

- 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 a user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- The secondary storage device specified for the mirroring must be installed in the same node as the primary boot device. The supported storage devices are disk0: and disk1:
- The secondary storage device must be the same size or larger than the designated primary storage device.
- The secondary storage device must be partitioned.

If you don't partition the primary boot device, the following occurs:

- The contents of the primary device are replicated to the secondary device.
- Control of the mirroring server switches to the secondary storage device.
- The primary device is partitioned.

- Data is replicated back to the primary boot device.

Note Although compactflash: can be used as the secondary device on a Performance Route Processor (PRP–2), there’s an issue with the ROM Monitor not being able to boot the minimum boot image (MBI) from the secondary device if the device isn’t disk0: or disk1:. In such a situation, you would need to go into ROMMON mode and boot the PRP-2 manually using the MBI on the compactflash:.

Step 2 Partition the secondary storage device into two partitions. If the device is already partitioned, then you do not need to perform the following configuration:

```
Router#format disk1: partition
```

Step 3 Remove any noncritical data from the primary boot device. The primary boot device should contain installation packages and configuration files only. Log files can be copied to the *a* partition of the secondary device, for example disk1a:

Step 4 Enable disk mirroring of the primary device to the secondary device using the **mirror** command.

```
Router#configure
Router(config)#mirror location 0/rsp0/cpu0 disk0:disk1:
```

After disk mirroring is configured, if there’s a fault on the primary boot drive or it can’t be accessed for any reason, then control is automatically transferred to the secondary storage device.

Step 5 Verify disk mirroring is enabled for an RSP node or all locations using the **show mirror location all** command. This command also provides the status of the synchronization between the primary and secondary devices.

```
Router(admin)#show mirror location all

Mirror Information for 0/RSP0/CPU0.
========================================================
 Mirroring Enabled
   Configured Primary:         disk0:
   Configured Secondary:       disk1:

 Current Mirroring State:      Redundant
   Current Physical Primary:   disk0:
   Current Physical Secondary: disk1:

 Mirroring Logical Device:     disk0:
 Mirroring Logical Device2:    disk1:

 Physical Device     State       Flags
--------------------------------------------------------
  disk0:           Available     Enabled
  disk1:           Available     Enabled
  compactflash:    Available
  (null)           Available
  disk0a:          Available
  disk1a:          Available
  compactflasha:   Not Present
  harddisk:        Available

Mirroring Rommon Variable
 BOOT_DEV_SEQ_CONF = disk0:;disk1:
 BOOT_DEV_SEQ_OPER = disk0:;disk1:
 MIRROR_ENABLE = Y
```

Step 6 Verify that disk synchronization is enabled for disk mirroring using the **mirror verify** command.

```
Router#mirror verify

Mirror Verify Information for 0/0/CPU0.
```

```
=======================================================
  Primary device and secondary device are fully synchronized.
```

Replace the Secondary Mirroring Device

The secondary disk mirroring device is typically replaced in any of the following scenarios:

- The disk fails or becomes unreliable.
- Upgrading to a larger or faster disk or expanding storage capacity.
- During a hardware refresh cycle to ensure compatibility and leverage newer technology.
- As part of a maintenance strategy or scheduled replacement.
- When configuration changes require aligning with new requirements.

Step 1 Verify the mirroring state. In the output, the *current mirroring state* must be *redundant.*

```
Router#show mirror
```

Step 2 Pause the Mirroring using the **mirror pause** command.

```
Router#mirror pause
```

Step 3 Verify that mirroring has paused using the **show mirror** command. In the output, the *current mirroring State* should be *paused.*

```
Router#show mirror
```

Step 4 Unmount the device using the **unmount** command.

```
Router#unmount disk1:
```

Step 5 Physically remove the device and insert a new device.

Step 6 Format the disk using the **format** command.

```
Router# format disk1: partition
```

Step 7 Verify that the device is formatted using the **show media** command. Then, resume the mirroring.

```
Router# show media
```

Step 8 Resume the mirroring using the **mirror resume** command.

```
Router# mirror resume
```

Step 9 Verify that the mirroring has restarted using the **show mirror** command. In the output, the *current mirroring state* should be *syncing*. It can take 15–30 minutes for the mirroring process to complete. The exact time depends on the number of packages or files on the boot device. When the mirroring is complete, the *current mirroring state* should be *redundant*.

```
Router# show mirror
```

Replace the Primary Mirroring Device

The secondary disk mirroring device is typically replaced in any of the following scenarios:

- The disk fails or becomes unreliable.
- Upgrading to a larger or faster disk or expanding storage capacity.
- During a hardware refresh cycle to ensure compatibility and leverage newer technology.
- As part of a maintenance strategy or scheduled replacement.
- When configuration changes require aligning with new requirements.

Step 1 Verify the mirroring state using the **show mirror** command. In the output, the *current mirroring state* must be *redundant*.

```
Router#show mirror
```

Step 2 Pause the mirroring using the **mirror pause** command.

```
Router#mirror pause
```

Step 3 Verify that mirroring has paused using the **show mirror** command. In the output, the *current mirroring State* should be *paused.*

```
Router#show mirror
```

Step 4 Unmount the device using the **unmount** command.

```
Router#unmount disk1:
```

Step 5 Physically remove the device and insert a new device.

Step 6 Format the disk using the **format** command.

```
Router#format disk1: partition
```

Step 7 Verify that the device is formatted using the **show media** command. Then, resume the mirroring.

```
Router#show media
```

Step 8 Resume the mirroring using the **mirror resume** command.

```
Router#mirror resume
```

Step 9 Verify that the mirroring has restarted using the **show mirror** command. In the output, the *current mirroring state* should be *syncing*. It can take 15–30 minutes for the mirroring process to complete. The exact time depends on the number of packages or files on the boot device. When the mirroring is complete, the *current mirroring state* should be *redundant*.

```
Router#show mirror
```

CHAPTER 8

Call Home

Cisco's Call Home feature facilitates email and http/https notifications for critical system policies. It supports different message formats for compatibility with pager services or XML-based applications, enabling paging of support engineers, emailing Network Operations Centers, and generating Technical Assistance Center cases. Call Home delivers alerts with diagnostic and environmental information, offering customizable destination profiles and formats such as short text, full text, and XML machine-readable.

Call Home Overview

Call Home provides an email and http/https-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. 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.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination is provided for sending alerts to the Cisco TAC, but you can also define your own destination profiles. When you configure Call Home to send messages, the appropriate CLI show command is executed and the command output is attached to the message. Call Home messages are delivered in the following formats:

- Short text format which provides a 1-2 line description of the fault that is suitable for pager or printed reports.

- Full text format which provides a fully formatted message with detailed information that is suitable for human reading.

- XML machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com. The XML format enables communication with the Cisco Systems Technical Assistance Center.

Destination Profiles

A destination profile includes the following information:

- One or more alert groups—The group of alerts that trigger a specific Call Home message if the alert occurs.
- One or more e-mail or http destinations—The list of recipients for the Call Home messages generated by alert groups assigned to this destination profile
- Message format—The format for the Call Home message (short text, full text, or XML)
- Message severity level—The Call Home severity level that the alert must meet before a Call Home message is sent to all e-mail and http url addresses in the destination profile. An alert isn't generated if the Call Home severity level of the alert is lower than the message severity level set for the destination profile.

You can also configure a destination profile to allow periodic inventory update messages by using the inventory alert group that sends out periodic messages daily, weekly, or monthly.

The following predefined destination profiles are supported:

- CiscoTAC-1—Supports the Cisco-TAC alert group in XML message format.

Call Home Alert Groups

An alert group is a predefined subset of alerts or events that Call Home detects and reports to one or more destinations. Alert groups allow you to select the set of alerts that you want to send to a predefined or custom destination profile. Alerts are sent to e-mail destinations in a destination profile only if that alert belongs to one of the alert groups associated with that destination profile and if the alert has a Call Home message severity at or above the message severity set in the destination profile.

The following table lists supported alert groups and the default CLI command output included in Call Home messages generated for the alert group.

Alert Group	Description	Executed Commands
Environmental	Events related to power, fan, and environment-sensing elements such as temperature alarms.	• **show environment** • **show logging** • **show inventory** • **show environment trace** • **show diag**
Inventory	Inventory status that is provided whenever a unit is cold booted, or when FRUs are inserted or removed. This alert is considered a noncritical event, and the information is used for status and entitlement.	• **admin show platform** • **admin show version** • **admin show diag** • **admin show inventory oid**

Syslog	Events generated by specific interesting syslog messages	• **admin show version** • **admin show logging** • **admin show inventory**
Configuration	User-generated request for configuration or configuration change event.	• **show version** • **show running config all** • **show inventory** • **show configuration history last 30** • **show configuration commit changes last 1**
Snapshot	This alert group can be configured for periodic notifications	By default, this alert group has no commands to be run. You can add the required commands that need to be run.

Call Home maps the syslog severity level to the corresponding Call Home severity level for syslog port group messages.

Call Home Message Levels

Call Home allows you to filter messages based on their level of urgency. You can associate each destination profile (predefined and user-defined) with a Call Home message level threshold. The Call Home message level ranges from 0 (lowest level of urgency) to 9 (highest level of urgency). Call Home messages are generated if they have a severity level equal to or greater than the Call Home message level threshold for the destination profile.

Call Home messages that are sent for syslog alert groups have the syslog severity level mapped to the Call Home message level.

Note Call Home doesn’t change the syslog message level in the message text.

The following table lists each Call Home message level keyword and the corresponding syslog level for the syslog port alert group.

Call Home Level	Keyword	syslog Level	Description
9	Catastrophic	N/A	Network-wide catastrophic failure.
8	Disaster	N/A	Significant network impact.
7	Fatal	Emergency (0)	System is unusable.
6	Critical	Alert (1)	Critical conditions that indicate that immediate attention is needed.

5	Major	Critical (2)	Major conditions.
4	Minor	Error (3)	Minor conditions.
3	Warning	Warning (4)	Warning conditions.
2	Notification	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	Normal	Information (6)	Normal event signifying return to normal state.
0	Debugging	Debug (7)	Debugging messages.

Obtaining Smart Call Home

If you have a service contract directly with us, you can register your devices for the Smart Call Home service. Smart Call Home provides fast resolution of system problems by analyzing Call Home messages sent from your devices and providing background information and recommendations. For issues that can be identified as known, particularly GOLD diagnostics failures, Automatic Service Requests are generated with the Cisco-TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time diagnostic alerts
- Analysis of Call Home messages from your device and, where appropriate, Automatic Service Request generation, routed to the appropriate TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through a downloadable Transport Gateway (TG) aggregation point. You can use a TG aggregation point in cases that require support for multiple devices or in cases where security requirements mandate that your devices may not be connected directly to the Internet.
- Web-based access to Call Home messages and recommendations, inventory, and configuration information for all Call Home devices. Provides access to associated field notices, security advisories, and end-of-life information

You need the following items to register:

- The SMARTnet contract number for your device
- Your e-mail address
- Your Cisco.com ID

For more information about Smart Call Home, see the Smart Call Home page at this URL: https://supportforums.cisco.com/community/netpro/solutions/smart_services/smartcallhome

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist you in resolving problems more quickly. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your identity remains anonymous, and no identifying information is sent.

When Call Home is configured for anonymous reporting, only, inventory, and test messages are sent to Cisco. No identifying information is sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). We maintain the privacy of all customers. For information about how we treat personal information, see the Cisco Privacy Statement.

Configure Call Home

The tasks in this module describes how to configure the sending of Call Home messages.

Step 1 Each router must include a contact e-mail address. You can optionally include other identifying information for your system installation. Here, apart from customer email-id, contract-id, customer-id, customer phone number, customer address are configured.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#contact-email-addr user1@cisco.com
Router(config-call-home)#contract-id Contract-identifier
Router(config-call-home)#customer-id Customer1
Router(config-call-home)#phone-number +405-123-4567
Router(config-call-home)#street-address "300 E. Tasman Dr. San Jose, CA 95134"
Router(config-call-home)#site-id SJ-RouterRoom1
```

If you include spaces in your entry, the entry must be quoted "".

You can use the **show call home** command to display information about the configured system contacts.

Step 2 You must have at least one activated destination profile for Call Home messages to be sent. The CiscoTAC-1 profile exists by default but is not active. The range of Call Home messages size is from 50 to 3145728 characters.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#profile my_profile
Router(config-call-home-profile)#destination address email support_me@cisco.com
Router(config-call-home-profile)#destination message-size-limit 1000
Router(config-call-home-profile)#destination preferred-msg-format xml
Router(config-call-home-profile)#destination transport-method email
Router(config-call-home-profile)#active
```

You can use the **show call-home profile** to verify that destination profile is activated.

Step 3 An alert is sent only to destination profiles that have subscribed to the Call Home alert group. Before configuring alert-group with a destination profile, use the **show call-home alert-group** command to view available alert groups.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#profile my_profile
Router(config-call-home-profile)#subscribe-to-alert-group environment severity major
Router(config-call-home-profile)#subscribe-to-alert-group inventory periodic monthly 1 10:00
Router(config-call-home-profile)#subscribe-to-alert-group syslog severity major pattern
Router(config-call-home-profile)#subscribe-to-alert-group snapshot severity major pattern
Router(config-call-home-profile)#subscribe-to-alert-group configuration severity major pattern
```

You can use the **show call-home profile** command to display information about destination profile.

Step 4 Call Home messages are sent via email. You must configure your email server before Call Home messages can be sent. You can specify upto 5 mail servers with their priroity. The mail server with the lower priority is tried first.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#sender from my_email@cisco.com
Router(config-call-home)#mail-server 198.51.100.1 priority 1
Router(config-call-home)#rate-limit 4
```

You can use the **show call-home mail-server** status to display the status of the specified mail server.

Step 5 Before enabling Call-Home, you must configure the source interface for http over IPv6. However, for http over IPv4, Call-Home works without the source interface. In the case of a dual-stack call-home configuration on the device, the IPv4 address is preferred over the IPv6 address. This may result in IPv6 resolution failure. Due to this limitation, the IPv6 device registration with the licensing server may only be done with a single mode, that is, IPv6 only configuration. Use the **http client source-interface ipv6** command to configure the source interface.

Step 6 By default the sending of Call Home messages is disabled. Perform this task to enable the sending of Call Home messages. Ensure that you've enabled destination profile for any Call Home messages before enabling the sending of Call Home messages.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#service active
```

Configure Call Home Features

Configure Smart Call Home (Single Command)

This task enables all call home basic configurations using a single command.

Configure all call home basic configurations using the **call-home reporting** command.

```
Router#configure
Router(config)#call-home reporting contact-email email@company.com
```

Configure Call Home Data Privacy

This task enables you to scrub data from the call-home message to protect the privacy of the user. The default data-privacy level is normal.

- **Normal** - scrubs all normal level commands, such as password/ username/ ip/ destination.failure.
- **High** - scrubs all normal level commands plus the IP domain name and IP address commands.
- **Hostname** - scrubbing the hostname from call-home messages may cause Smart Call Home processing failure.

Note Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.

Configure data privacy to scrub data from the call-home messages using the **data-privacy** command.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#data-privacy level high
Router(config-call-home)#commit
```

Configure Call Home Syslog Throttling

This task enables or disables the call home syslog message throttling and avoid sending repetitive call home syslog messages. By default, syslog message throttling is enabled.

Use **syslog-throttling** to enable or disable call home syslog message throttling.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#syslog-throttling
Router(config-call-home)#commit
```

Enable AAA Authorization for Call Home Messages

This task helps you enable AAA Authorization for call home messages.

Enable AAA Authorization for call home messages using the **aaa-authorization** command.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#aaa-authorization username u1
Router(config-call-home)#commit
```

Manually Send Call Home Alert Group Messages

Manually triggering Call Home alert group messages is subjected to the following guidelines:

- Only the snapshot, configuration, and inventory alert groups can be sent manually. Syslog alert groups can't be sent manually.
- When you manually trigger a snapshot, configuration, or inventory alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile's active status, subscription status, or severity setting.
- When you manually trigger a snapshot, configuration, or inventory alert group message and don't specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.

Configure manually triggering of call home alert group messages using the **call-home send** command. In the following example, snapshot , configuration, and inventory alert group messages are sent to one destination profile. You can also send call home alert group messages to all the profiles, if specified.

```
Router#call-home send alert-group snapshot profile p1
Router#call-home send alert-group configuration profile p1
Router#call-home send alert-group inventory profile p1
Router#commit
```

Manually Send Command Output Message for a Command List

Manually sending command output message for a command list is subjected to the following guidelines:

- The specified command or list of commands can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If the email option is selected using the “email” keyword and an email address is specified, the command output is sent to that address.
- If neither the email nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the “email” nor the “http” keyword is specified, the service request number is required for both long-text, and XML message formats and is provided in the subject line of the email.
- If the HTTP option is specified, the CiscoTAC-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. The user must specify either the destination email address or an SR number but they can also specify both.

Use the **call-home send** command to execute a command or a list of commands and send the command output through the HTTP or email protocol.

```
Router#call-home send “show version;show running-config;show inventory” email support@example.com
msg-format xml
```

Configure an HTTP Proxy Server for Call Home

This task enables you to configure HTTP Proxy Server for call home. You can configure HTTP Proxy Server in the range of 1 to 65535.

Configure port for the HTTP Proxy Server for call home using the **http-proxy** command.

```
Router#configure
Router(config)#call-home
Router(config)#http-proxy p1 port 100
Router(config)#commit
```

Configure Snapshot Alert Group on Call Home

This task enables you to configure snapshot alert group on Call Home.

Configure a command to the snapshot alert group using the **alert-group-configuration snapshot** command. In the following example, **show ver** command is added.

```
Router#configure
Router(config-call-home)#alert-group-configuration snapshot
Router(config-call-home-snapshot)#add-command "show ver"
Router(config-call-home-snapshot)#commit
```

Configure Anonymous Reporting on Call Home

This task enables you to configure anonymous reporting on call home. When **anonymous-reporting-only** is set, only inventory and test messages are sent.

Configure an anonymous mode profile by using the **anonymous-reporting-only** command.

```
Router#configure
Router(config)#call-home
Router(config-call-home)#profile ciscotac
Router(config-call-home-profile)#anonymous-reporting-only
Router(config-call-home-profile)#commit
```

Configure Call Home to use VRF

This task enables you to configure call home for the specified VRF. VRF works only for the http transport method. It does not work for the email transport method.

Configure call home to for the specified vrf by using the **vrf** command.

```
Router#configure
Router(config)#call-home
Router(config)#vrf v1
Router(config)#commit
```

Configure Call Home to use Source Interface

This task enables you to configure call home to use source interface. Source-interface supports email and HTTP messages.

Configure call-home to use source interface using the **source-interface** command.

```
Router#configure
Router(config)#call-home
Router(config)#source-interface tengige 192.0.2.1
Router(config)#commit
```

CHAPTER 9

File System

This module describes additional enhancement to file system commands. File System commands are instructions that can be used to manage and manipulate files and directories within a file system.

Secure File Transfer

Table 7: Feature History Table

Feature Name	Release Information	Feature Description
Secure File Transfer	Release 7.9.1	Now, you can securely transfer router files to an archive server. It's made possible because the copy command now supports SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol using the underlying SSH protocol implementation. Secure transfer of files from the router maintains the integrity, confidentiality, and availability of network configurations. This feature modifies the **copy** command.

You can duplicate files or data in the router from one location to another using the **copy** command. This functionality helps to create a copy of a file, folder, or data set and place it in a specific destination. You can use the copy functionality to back up files, move data between directories, create duplicates of the files for editing or distribution without modifying the original content. It also allows you to retain the original data while making a duplicate that you can further manipulate independently.

Starting with Cisco IOS XR Release 7.9.1, we've enhanced the functionality of the copy command to support secure file transfer from the router. Secure file transfer protects data during transit using the SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) when sharing files within or across networks. The

SFTP and SCP functionalities in the copy feature use the SSH protocol implementation in the router to secure transfer the files to a remote server.

You can use the following options in the **copy** command for secure file transfer:

- **sftp:** You can transfer the files to a remote location using the **SFTP** file transfer protocol. SFTP is a secure file transfer protocol for transferring large files.
- **scp:** You can transfer the files to a remote location using the **SCP** file transfer protocol. SCP is a secure copy protocol to transfer files between servers.

Starting Cisco IOS XR Software Release 7.10.1, you can use public-key authentication while copying the running configuration. To know more about using public-key authentication with **copy** refer the *Auto-Save and Copy Router Configuration Using Public Key Authentication* in Configuration Management Commands chapter in General Administration Guide.

Prerequisites:

Enable the SSH Server in the router as follows:

```
Router# config
Router(config)# ssh server v2
Router(config)# ssh server vrf default
Router(config)# ssh server netconf vrf default
Router(config)# commit
```

Copy Files Using SCP

Step 1 Copy the running configuration file from the router to a remote server using SCP using the **copy** command.

```
Router# copy running-config scp://root:testpassword@192.0.4.2//var/opt/run_conf_scp.txt

Destination file name (control-c to cancel): [/var/opt/run_conf_scp.txt]?

.
215 lines built in 1 second
[OK]Connecting to 192.0.4.2...22
Password:

  Transferred 3271 Bytes
  3271 bytes copied in 0 sec (0)bytes/sec
```

Step 2 Verify if the copied files are available in the SCP server using the **ls** utility.

```
[root@scp_server ~]# ls -ltr /var/opt/run_conf_scp.txt
-rw-r--r-- 1 root root 3271 Mar 21 18:07 /var/opt/run_conf_scp.txt
```

Copy files Using SFTP

Step 1 Copy the running configuration file from the router to a remote server using SFTP using the **copy** command.

```
Router#copy running-config sftp://root:testpassword@192.0.2.1//var/opt/run_conf_sftp.txt
```

```
Destination file name (control-c to cancel): [/var/opt/run_conf_sftp.txt]?

.
215 lines built in 1 second
[OK]Connecting to 192.0.2.1...22
Password:
sftp> put /tmp/tmpsymlink/nvgen-34606-_proc_34606_fd_75 /var/opt/run_conf_sftp.txt


/tmp/tmpsymlink/nvgen-34606-_proc_34606_fd_75

  Transferred 3271 Bytes
  3271 bytes copied in 0 sec (3271000)bytes/sec
sftp> exit
```

Step 2 Verify if the copied files are available in the SFTP server using the **ls** utility

```
[root@sftp_server ~]# ls -ltr /var/opt/run_conf_sftp.txt
-rw-r--r-- 1 root root 3271 Mar 21 18:07 /var/opt/run_conf_sftp.txt
```

Increasing Commit Limit

Table 8: Feature History Table

Feature Name	Release Information	Feature Description
Increasing Commit Limit	Release 24.2.1	The maximum number of commits is increased in the router that allows you to configure complex topology changes without interruptions caused by the default blocking of commit changes during rebase or ASCII backup operations. You can prevent the commit operation from getting blocked by using the **cfs check** command, which increases the commit (pacount) count from 20 to 40, and the commit file diff size (configuration data) from 2 MB to 4 MB, and by using the **clear configuration ascii inconsistency** command, which performs an ASCII backup after 55 minutes. The feature modifies the following commands: • **cfs check** • **clear configuration ascii inconsistency**

The Cisco IOS XR Routers use a two-stage configuration model. The first stage is target configuration, where you build the configurations using the necessary commands in the command line interface. The second stage is the commit, where the configuration made in the target stage is added to the router configuration using the **commit** command. After each commit, the router generates a file for the newly configured changes and adds it to its running configuration, making it an integral part of the running configuration.

Note This target configuration doesn’t impact the router's running configuration.

The Cisco IOS XR routers perform rebase and ASCII backup operations to maintain the real time configuration in the backup copy. The rebase and ASCII backup operations block you from committing configurations to the router.

Note Starting with Release 24.3.1, the rebase operation no longer blocks the commit operation.

This allows you to configure complex topology changes without being interrupted by the default blocking of commit changes during the rebase operation. For more information, see the section Concurrent Configuration Rebase during Commit, on page 50.

In rebase, the router automatically saves your changes to the backup binary configuration file after 20 commits, or 2 MB of configuration data. The router blocks the commit while saving the configuration to the backup file. The router takes a few seconds to complete the rebase operation, during which, if you terminate the CLI session, the router loses the target configurations in the blocked commit.

In ASCII backup, the router automatically saves a copy of its running configuration in the ASCII format. This backup process takes place if there has been a commit to the router configuration and when the ASCII backup timer completes a 55-minute window after the previous backup event. However, if there was no commit when the ASCII backup timer completes 55 minutes, the counter is reset without any backup. During the ASCII backup, the router blocks the configuration commits.

Starting with Release 24.2.1, we have made the following enhancements:

- You can use the **cfs check** command to increase the rebase limits in the router from 20 to 40 commits and the configuration data from 2 MB to 4 MB. When configuring the router, you can check the current commit count and configuration data size using the **show cfgmgr commitdb** command. If the commit count is 20 or higher, or the configuration data size is 2 MB or above, the router initiates a rebase within 10 seconds. By using the **cfs check** command to increase the commit count to 40 and the configuration data to 4 MB, you can commit without delay.

- You can use the **clear configuration ascii inconsistency** command to perform an ASCII backup and reset the ASCII backup timer to zero. Once the backup is complete, the router will automatically initiate the next periodic ASCII backup operation only after 55 minutes from the time the **clear configuration ascii inconsistency** command is executed.

Guidelines and Restrictions for Increasing the Commit Limit

- The **clear configuration ascii inconsistency** command initiates an ASCII backup and resets the ASCII backup timer count to zero. Following this, the router will automatically initiate the next periodic ASCII backup operation only after 55 minutes from the time **clear configuration ascii inconsistency** command is executed. For example, if you execute a commit operation after executing a **clear configuration ascii**

inconsistency command, the router will perform an ASCII backup operation 55 minutes after the**clear configuration ascii inconsistency** command was executed, and merge the new commit into ASCII backup. Hence, before the next 55 minutes, you must execute the **clear configuration ascii inconsistency** command again to reset the ASCII backup timer to zero.

- When the router enters standby mode or reloads, the ASCII timer does not reset to zero, and the router performs an ASCII backup operation 55 minutes after the first commit operation before the standby mode or reload.
- Cisco does not recommend executing **clear configuration inconsistency** and **clear configuration ascii inconsistency** commands regularly after each commit, as it causes hard disk wear and tear. You should execute these commands only before a commit or sequence of commits that must be done within a specific timeframe and without being delayed by rebase and ASCII backup operations. As these commands perform disk input and output operations in the background, frequent execution of these commands causes frequent access to the hard disk, which increases the wear and tear on the hard disk.

Increasing the Rebase Limits

You can increase the rebase limits as follows:

1. Use the **cfs check** command to increase the commit count to 40 and the configuration data to 4 MB.

```
Router# cfs check
Creating any missing directories in Configuration File system...OK
Initializing Configuration Version Manager...OK
Syncing commit database with running configuration...OK
```

2. Verify if the **cfs check** command is executed using the **show configuration history** command.

```
Router# show configuration history last 5
Sno.  Event      Info                           Time Stamp
~~~~  ~~~~~      ~~~~                           ~~~~~~~~~~
1     cfs check  completed                      Wed Jan 10 11:42:21 2024
2     commit     id 1000000001                  Wed Jan 10 11:39:26 2024
3     startup    configuration applied          Wed Jan 10 11:39:02 2024
```

Perform ASCII Backup and Rest ASCII Backup Timer

You can perform ASCII backup and rest ASCII backup timer as follows:

1. Use the **clear configuration ascii inconsistency** command to perform ASCII backup at that instance and reset the ASCII backup timer count to zero.

```
Router# clear configuration ascii inconsistency
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! It is recommended to run this command only when all nodes in router      !!!!
!!!! are in IOS-XR RUN state. To determine node state, run following command: !!!!
!!!! 'show platform'.                                                         !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Proceed with the command ?[confirm] y
 Ascii configuration backup is in progress...
Configuration ascii backup complete
```

2. Verify if the **clear configuration ascii inconsistency** command is executed using the **show configuration history** command.

```
Router# show configuration history last 5
Sno.  Event      Info                           Time Stam
```

```
~~~~   ~~~~~      ~~~~                           ~~~~~~~~~~
1      backup     Periodic ASCII backup          Wed Jan 10 11:48:20 2024
2      cfs check  completed                      Wed Jan 10 11:42:21 2024
3      commit     id 1000000001                  Wed Jan 10 11:39:26 2024
4      startup    configuration applied          Wed Jan 10 11:39:02 2024
```

Concurrent Configuration Rebase during Commit

Table 9: Feature History Table

Feature Name	Release Information	Feature Description
Concurrent Configuration Rebase during Commit	Release 24.3.1	The router performs the commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation. This removes the need to use the **cfs check** command to increase the commit count and the commit file diff size.

Cisco IOS XR routers use a two-stage configuration model. In the first stage, configurations are built using necessary commands in the command line interface, and in the second stage, the configurations are committed to the router.

During rebase and ASCII backup operations, the router blocks configuration commits. However, the "Concurrent Configuration Rebase during Commit" feature allows the router to perform commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation.

The Cisco IOS XR routers perform rebase and ASCII backup operations to maintain the real time configuration in the backup copy.

Before Release 24.3.1,

- The rebase and ASCII backup operations block you from committing configurations to the router.
- You can increase the maximum number of commits and reset the ASCII backup timer to allow the router to configure complex topology changes without interruptions caused by the default blocking of commit changes during rebase or ASCII backup operations. For more information, see the section Increasing Commit Limit, on page 47.

From Release 24.3.1,

- The router performs the commit and rebase operations simultaneously, ensuring that the commit operation remains unblocked during the rebase operation. This removes the need to use the **cfs check** command to increase the commit count and the commit file diff size.
- However, the ASCII backup operations still block the commit operation. You can reset the ASCII backup timer using the clear configuration ascii inconsistency command. This allows the router to perform an ASCII backup after 55 minutes and perform commit operations without being blocked by ASCII backup operations. For more information on ASCII backup, see the section Increasing Commit Limit, on page 47.

CHAPTER 10

Configuration Management

This module describes the enhancements done to Configuration Management Commands. Configuration management commands are specific instructions used within configuration management tools to automate the setup, modification, and maintenance of system and software configurations.

Auto-Save Configuration

Table 10: Feature History Table

Feature Name	Release Information	Feature Description
Auto-Save with Secure File-Transfer and Additional Configurable Parameters	Release 7.9.1	Apart from automatically backing up the running configuration after every commit, you can also do the following with Auto-Save: • Save running configurations to remote systems using Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). • Configure wait-time between two subsequent auto-saves. • Append time-stamp to the file name of the saved configuration. • Save the encrypted password. • Specify the maximum number of files that you can auto-save. The feature introduces these changes: CLI: Modified the **configuration commit auto-save**command Yang Data Model: • New XPaths for Cisco-IOS-XR-config-autosave-cfg • New XPaths for Cisco-IOS-XR-um-config-commit-cfg

You can configure the router to automatically take the backup of the running configuration by using **configuration commit auto-save** command. This auto-save feature saves the configuration to the specified location on the router after every **commit** is made. These auto-save files are stored in the form of Linux files.

Starting Cisco IOS XR Software Release 7.9.1, the auto-save feature is enhanced to provide a set of functionalities. This feature adds the following functionailites:

- You can save the running configuration backup files to remote location using **scp** and **sftp** file transfer protocols. SCP is a secure copy protocol to transfer files between servers. Whereas SFTP is a secure file transfer protocol for transfering large files.

- You can can save encrypted passwords for the remote and non-remote URLs.
- You can mention maximum number of files that can be saved automatically. Once the maximum number of auto-saved file is reached, the newer auto-save files starts replacing the older auto-save files. The default value of **maximum** is 1. You can save upto 4294967295 files.
- You can append timestamp to the auto-saved configuration file name. The **timestamp** uses the time and timezone configured on the router. The saved file displays timestamp in <day> <month> <date> <hours> <minutes> <seconds> <milliseconds> format. Here is an example of auto-saved file with time-stamp - *: test_123.autosave.1.ts.Tue_Jan_31_15-15-51_805_IST*
- You can specify how long to wait before next auto-save happens in terms of days, months or hours after the commit is made. The default value of **wait-time** is zero.

You can also configure options such as **password**, **timestamp**, **maximum**, and **wait-time** with the **configuration commit auto-save** command. The location to save the file-name must be specified in <protocol>://<user>@<host>:<port>/<url-path>/<file-name> format. When filename is accessed through VRF, you can specify filename in **filename** <protocol>://<user>@<host>:<port>;<vrf name>/<url-path>/<file-name> format.

Restriction for Auto-Save Configuration

The auto-save configuration is only available on the local paths, scp, and sftp paths.

Configure Auto-Save

Step 1 Use the **configuration commit auto-save** command to auto-save the configuration.

```
Router#configure
Router(config)#configuration commit auto-save
Router(config-cfg-autosave)#commit
```

Step 2 You can also use options such as **password**, **timestamp**, **maximum**, and **wait-time** with the **configuration commit auto-save** command.

```
Router(config-cfg-autosave)#configuration commit auto-save filename
sftp://user1@server1://test-folder/test_123
Router(config-cfg-autosave)#password clear encryption-default cisco
Router(config-cfg-autosave)#timestamp
Router(config-cfg-autosave)#maximum 10
Router(config-cfg-autosave)#wait-time days 0 hours 0 minutes 0 seconds 5
Router(config-cfg-autosave)#commit
```

Step 3 If you're using public-key authentication, you don't need to mention **password.**

Auto-Save and Copy Router Configuration Using Public Key Authentication

Table 11: Feature History Table

Feature Name	Release Information	Feature Description
Auto-Save and Copy Router Configuration Using Public Key Authentication	Release 7.10.1	You can now experience passwordless authentication while automatically saving running configurations and securely copying them on the router. The feature uses public key-based authentication, a secure logging method using a secure shell (SSH), which provides increased data security. This feature offers automatic authentication and single sign-on benefits, which also aids in a secure automation process. This feature modifies **configuration commit auto-save** and **copy** command to support password-less authentication.

From Cisco IOS XR Software Release 7.10.1, you don't need to remember and enter the **password** as you can use public key-based authentication while doing the following:

- Automatically saving your running configuration
- Copying the configuration from a source (such as a network server) to a destination (such as a flash disk)

Password is automatically verified when you have enabled SSH connection using public key-based authentication. Using public key-based authentication avoids several problems such as password disclosure and password leakage.

Public key is mathematically related to private key. The private key is secret, whereas the public key is available on the servers. You can copy the public key to the SSH server from the SSH client. Then, when you try to secure the running configuration, the SSH server tries to authenticate by generating a challenge using the public key. Only the private key can answer this challenge. As the keys are related, log-in is successful.

Use Public-Key Authentication with Auto-Save and Copy Commands

Step 1 Ensure you have enabled public key-based authentication of SSH clients, using the following steps:

- Generate RSA key pair on the router configured as the SSH client. Use the **cyrpto key generate authentication-ssh rsa** command to generate the RSA key pair.

- Use the **show crypto key mypubkey authentication-ssh rsa** command to view the details of the RSA key. The key value starts with *ssh-rsa* in this output.
- Copy the RSA public key from the SSH client to the SSH server.
    - You can do this either by logging in to the remote SSH server with your established user credentials, or have a system administrator on the remote system add the key on the SSH server.
    - If the SSH server is a Cisco IOS XR router, then you can use the **crypto key import authentication rsa** command on the router prompt of the server to import the key from the SSH client. You will then be prompted to enter the public key.
    - If the SSH server is a Linux server, then you must add the public key to the `~/.ssh/authorized_keys` file of the respective user account in that server. This file contains a list of all authorized public keys on that server.

For more detailed information on how to enable SSH connection using public-key based authentication, see *Public Key Based Authentication of SSH Clients* in System Security Configuration Guide.

Step 2 When you are using public key authentication for auto-save, you don't need to mention **password**.

```
Router(config-cfg-autosave)#configuration commit auto-save filename
sftp://user1@server1://test-folder/test_123
Router(config-cfg-autosave)#timestamp
Router(config-cfg-autosave)#maximum 10
Router(config-cfg-autosave)#wait-time days 0 hours 0 minutes 0 seconds 5
Router(config-cfg-autosave)#commit
```

Step 3 While you’re using public-key authentication for copying running configuration from the router to a remote server, you don't need to mention **password** in the command.

```
Router#copy running-config scp://root@192.0.4.2//var/opt/run_conf_scp.txt
Router#copy running-config sftpp://root@192.0.4.2//var/opt/run_conf_sftp.txt
```

CHAPTER 11

General Administration Commands

The Cisco Command Reference Guide serves as a comprehensive resource, offering a catalog of command-line interface (CLI) commands for configuring and verifying General Administration tasks.

Reference to Command Reference Guide

The Cisco Command Reference Guide serves as a comprehensive resource, offering a catalog of command-line interface (CLI) commands for configuring and verifying General Administration tasks.

To view the list of supported commands, see *General Administartion Command Reference for ASR 9000 Series Routers*.

CHAPTER 12

YANG Data Models for General Administration

Learn how to configure and retrieve the operational status of the YANG data models for General Administration on ASR 9000 Series Routers.

To get started with using these data models, see:

List of YANG Data Models for General Administration

Here is a list of YANG data models that you can use to configure and manage General Administration on the router:

Table 12: General Administration YANG Data Models

Cisco XR Native Data Model	Unified Data Model	OpenConfig Data Model
Cisco-IOS-XR-man-xml-ttyagent-cfg		
Cisco-IOS-XR-man-xml-ttyagent-oper	Cisco-IOS-XR-um-xml-agent-cfg	
Cisco-IOS-XR-manageability-object-tracking-cfg	Cisco-IOS-XR-um-vrf-cfg	
Cisco-IOS-XR-manageability-perfmgmt-cfg		
Cisco-IOS-XR-tty-show-line-oper	Cisco-IOS-XR-um-line-cfg	openconfig-system-terminal
Cisco-IOS-XR-tty-show-terminal-oper	Cisco-IOS-XR-um-line-exec-timeout-cfg	
Cisco-IOS-XR-tty-vty-cfg	Cisco-IOS-XR-um-line-general-cfg	
Cisco-IOS-XR-terminal-device-cfg	Cisco-IOS-XR-um-line-timestamp-cfg	
Cisco-IOS-XR-terminal-device-oper	Cisco-IOS-XR-um-terminal-device-cfg	
Cisco-IOS-XR-tty-show-terminal-oper	Cisco-IOS-XR-um-vty-pool-cfg	

Cisco XR Native Data Model	Unified Data Model	OpenConfig Data Model
Cisco-IOS-XR-tty-management-datatypes		
Cisco-IOS-XR-tty-management-cfg		
Cisco-IOS-XR-tty-management-oper		
Cisco-IOS-XR-tty-vty-cfg		
Cisco-IOS-XR-cdp-oper		
Cisco-IOS-XR-cdp-cfg		
Cisco-IOS-XR-mirror-cfg	Cisco-IOS-XR-um-mirror-cfg	
Cisco-IOS-XR-mirror-oper		
Cisco-IOS-XR-call-home-cfg	Cisco-IOS-XR-um-call-home-cfg	
Cisco-IOS-XR-config-autosave-cfg	Cisco-IOS-XR-um-config-commit-cfg	

You can access the data models using one of these following options:

Access Data Models From Router

To access data models directly from the router, you can follow these steps:

Step 1 Enter the global configuration mode.

Example:

```
Router#configure
```

Step 2 Configure the NETCONF network management protocol to remotely configure and manage the router using YANG data models.

Example:

```
Router(config)#netconf-yang agent ssh
```

Step 3 Commit the configuration.

Example:

```
Router(config)#commit
```

Step 4 Establish a NETCONF session with the device and retrieve the capabilities information.

Example:

```
Router#show netconf-yang capabilities
Tue Sep 19 22:03:26.305 UTC
[Netconf capabilities]

   D: Has deviations

 Capability                                                              | Revision |D
```

```
----------------------------------------------------------------------------------+----------+-
urn:ietf:params:netconf:base:1.1                                                  | -        |
urn:ietf:params:netconf:capability:candidate:1.0                                  | -        |
urn:ietf:params:netconf:capability:confirmed-commit:1.1                           | -        |
urn:ietf:params:netconf:capability:interleave:1.0                                 | -        |
urn:ietf:params:netconf:capability:notification:1.0                               | -        |
urn:ietf:params:netconf:capability:rollback-on-error:1.0                          | -        |
urn:ietf:params:netconf:capability:validate:1.1                                   | -        |
http://cisco.com/ns/yang/Cisco-IOS-XR-8000-fib-platform-cfg                       |2019-04-05|
http://cisco.com/ns/yang/Cisco-IOS-XR-8000-lpts-oper                              |2022-05-05|
http://cisco.com/ns/yang/Cisco-IOS-XR-8000-platforms-npu-resources-oper           |2020-10-07|
http://cisco.com/ns/yang/Cisco-IOS-XR-8000-qos-oper                               |2021-06-28|
http://cisco.com/ns/yang/Cisco-IOS-XR-Ethernet-SPAN-act                           |2021-03-22|
http://cisco.com/ns/yang/Cisco-IOS-XR-Ethernet-SPAN-cfg                           |2022-07-13|
http://cisco.com/ns/yang/Cisco-IOS-XR-Ethernet-SPAN-datatypes                     |2021-10-06|
http://cisco.com/ns/yang/Cisco-IOS-XR-Ethernet-SPAN-oper                          |2022-09-05|
http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-aaacore-cfg                             |2019-04-05|
http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-ldapd-cfg                               |2022-06-22|
http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-ldapd-oper                              |2022-05-20|
http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-lib-cfg                                 |2020-10-22|
http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-lib-datatypes
----------------------------------   Truncated for brevity  --------------------------------------
```

By examining the capabilities, you can view the available data models for the software version installed on the router.

Access Data Models From Cisco Feature Navigator

To access data models from Cisco Feature Navigator, you can follow these steps:

Step 1 Go to Cisco Feature Navigator.

Step 2 If you have a Cisco.com account, click on the **Login** button and enter your credentials. If you don't have an account, you can click **Continue as Guest**.

You will be directed to the Cisco Feature Navigator main page.

Step 3 Click **YANG Data Models**.

Step 4 Select the **Product** and **Cisco IOS XR Release** based on your requirement.

The data models are listed based on type—Cisco XR native models, Unified models and OpenConfig models.

You can use the search field to search for specific data model of interest.

Step 5 Click the specific data model of interest to view more details.

The data model is displayed in a hierarchical tree structure making it easier to navigate and understand the relationships between different YANG modules, containers, leaves and leaf lists. You can apply filters to further narrow down the data model definitions for the selected platform and release based on status such as deprecated, obsolete and unsupported nodes.

You can also click the **Download** icon to export the data model information in Excel format.

This visual tree form helps you get insights into the nodes that you can use to automate your network.

The data models on Cisco Feature Navigator is regularly updated based on IOS XR release. If you encounter any problem or have suggestions for improvements, share your experience using Send us your feedback link.

Access Data Models From GitHub

To access the data models from GitHub repository, you can follow these steps:

Step 1 Go to the GitHub repository for data models.

On the repository page, you will find a list of folders based on IOS XR releases.

Step 2 Navigate to the release folder of interest to view the list of supported data models and their definitions. For example, if you want to access the data models for IOS XR release 7.10.1, click on the folder named `7.10.1`.

Inside the folder, you will find a list of YANG files representing different data models.

Step 3 Click on the YANG file you want to access to view its contents.

You can also click on the **Raw** button to see the raw code or use the **Download** button to download the file to your computer.

Each data model defines a complete and cohesive model, or augments an existing data model with additional XPaths. To view a comprehensive list of the data models supported in a release, navigate to the **Available-Content.md** file in the repository. The unsupported sensor paths are documented as deviations. For example, `openconfig-acl.yang` provides details about the supported sensor paths, whereas `cisco-xr-openconfig-acl-deviations.yang` shows the unsupported sensor paths for `openconfig-acl.yang` model.

Step 4 Repeat the above steps for other versions or data models of interest.

The GitHub repository for IOS XR data models is regularly updated based on release. You can also contribute to the repository by submitting pull requests, opening issues if you encounter any problems or have suggestions for improvements.

Get Started With IOS XR YANG Data Models

Here is a generic outline of the steps involved in programmatically configuring your router using YANG data models:

1. Enable network management protocol—Manage the router remotely using the protocols such as NETCONF or gRPC.

2. Install the necessary libraries and tools—Depending on the programming language you are using, you may need to install libraries or tools to programatically interact with the router. For example, if you are using Python, you might need to install the `ncclient` library.

3. Establish a session with the router—Use the programming language of your choice to establish a connection to the router using NETCONF or gRPC protocols. This involves providing connection parameters such as device IP address, username, password, and port number.

4. Retrieve the router capabilities—View the supported features and functionalities available on the router.
5. Create or modify configurations—Use YANG data models to create or modify the configuration on the router.
6. Apply the configuration—Push the updated configuration via the NETCONF or gRPC protocol to modify the router's running configuration to reflect the desired changes.
7. Validate the configuration—Verify that the changes are successfully applied. You can retrieve the running configuration or specific configuration parameters to ensure that the device is configured as intended.

For detailed instructions about using the data models, refer the *Programmability Configuration Guide*.