



Cisco Catalyst 8500 and 8500L Series Edge Platforms Software Configuration Guide

First Published: 2020-08-20

Last Modified: 2023-04-10

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



CONTENTS

CHAPTER 1

Preface 1

Objectives 1

Document Revision History 1

Communications, Services, and Additional Information 1

CHAPTER 2

Read Me First 3

CHAPTER 3

Overview 5

CHAPTER 4

Software Packaging and Architecture 7

Software Packaging on the Cisco Catalyst 8500 Series Edge Platforms 7

Cisco Catalyst 8500 Series Edge Platforms Software Overview 7

Consolidated Packages 7

Important Information About Consolidated Packages 7

Individual Software SubPackages Within a Consolidated Package 8

Important Notes About Individual SubPackages 8

Provisioning Files 9

Important Notes About Provisioning Files 9

ROMmon Image 9

File to Upgrade Field Programmable Hardware Devices 10

Processes Overview 10

IOS as a Process 10

Dual IOS Processes 10

File Systems on the Cisco Catalyst 8500 Series Edge Platforms 11

Autogenerated File Directories and Files 11

Important Notes About Autogenerated Directories 12

CHAPTER 5**Managing the SD-Routing Device Using Cisco SD-WAN Manager 13****Information About Using Cisco SD-WAN Manager to Monitor the SD-Routing Devices 13****Benefits of Managing the SD-Routing Devices Using Cisco SD-WAN Manager 14****Prerequisites 14****Limitations 15****Supported WAN Edge Devices 15****Onboarding the SD-Routing Devices 17****Onboarding the SD-Routing Devices Using Automated Workflow 17****Configuring the Plug and Play Connect Portal 18****Configuring the Cisco SD-WAN Manager Using Quick Connect Workflow 18****Bringing Up the SD-Routing Device 19****Onboarding the SD-Routing Devices Using Bootstrap 19****Onboarding the Devices Manually 21****Onboarding the Device by Activating the Chassis Using the Token 24****Onboarding the Multi-Tenancy SD-Routing Devices 25****Onboarding the Multi-Tenancy SD-Routing Devices Using Automated Workflow 25****Onboarding the Multi-Tenancy SD-Routing Devices Manually 26****Onboarding the Device to Cisco SD-WAN Manager Using One Touch Provisioning 28****Unprovisioning the Feature 29****Software Image Management 29****Software Upgrade Using CLI 29****Add Software Images to the Repository 30****Software Upgrade Using Cisco SD-WAN Manager 30****Delete a Software Image 32****View Log of Software Upgrade Activities 32****Monitoring the Device Using Cisco SD-WAN Manager 32****Monitoring the Device Using SSH 32****Pinging the Device 33****Tracing the Route 33****Alarms and Events 33****Monitoring the Alarms and Events 34****Admin-Tech Files 34****Requesting the Admin-tech File Using Cisco SD-WAN Manager 34**

Requesting the Admin-tech File Using CLI	35
Monitoring the Real Time Data	35
Configuration Examples	35
Example: Enabling Control Connection on Cisco SD-WAN Manager	36
Example: Verifying the Enable Control Connection	36
Example: Installing the Root Certificate	36
Example: Verifying the Root Certificate Installation	36
Troubleshooting	37
Feature Information for Managing SD-Routing Devices Using vManage	38

CHAPTER 6

Deploy IOS-XE and SDWAN 39

Overview	39
Restrictions	39
Autonomous or Controller Mode	39
Switch Between Controller and Autonomous Modes	39
PnP Discovery Process	40

CHAPTER 7

Using Cisco IOS XE Software 41

Accessing the CLI Using a Router Console	41
Accessing the CLI Using a Directly-Connected Console	41
Connecting to the Console Port	41
Using the Console Interface	42
Accessing the CLI from a Remote Console Using Telnet	43
Preparing to Connect to the Router Console Using Telnet	43
Using Telnet to Access a Console Interface	44
Using Keyboard Shortcuts	45
Using the History Buffer to Recall Commands	46
Understanding the Command Mode	46
Getting Help	47
Finding Command Options	48
Using the no and default Forms of Commands	51
Saving Configuration Changes	51
Managing Configuration Files	51
Dynamic Allocation of Cores	53

Filtering the Output of the show and more Commands	53
Disabling Front-Panel USB Ports	54
Configuration Examples for Disabling of Front-Panel USB Ports	55
Verifying Disabling of Front Panel USB Ports	55
Powering Off a Router	55
Finding Support Information for Platforms and Cisco Software Images	55
Using the Cisco Feature Navigator	56
Using the Software Advisor	56
Using the Software Release Notes	56

CHAPTER 8
Bay Configuration 57

Bay Configuration C8500-12X4QC	57
Bay Configuration Examples	59
Examples	59
Breakout Support	63
Understand Breakout Support	63
Breakout Support	64
Sample Commands to Configure Breakout Support	65
Bay Configuration C8500-12X	65
Bay Configuration C8500-20X6C	65

CHAPTER 9
Licenses and Licensing Models 67

Feature Information for Available Licenses and Licensing Models	67
Available Licenses	69
Cisco DNA License	69
Guidelines for Using a Cisco DNA License	70
Ordering Considerations for a Cisco DNA License	71
High Security License	71
Guidelines for Using an HSECK9 License	72
Ordering Considerations for an HSECK9 License	73
Cisco CUBE License	73
Cisco Unified CME License	74
Cisco Unified SRST License	74
Throughput	74

Throughput as a Numeric Value	76
Throughput and System Hardware Throttling Specifications in the Autonomous Mode	77
Throughput and System Hardware Throttling Specifications in the SD-WAN Controller Mode	81
Throughput as a Tier	82
Numeric vs. Tier-Based Throughput Configuration	85
How to Configure Available Licenses and Throughput	88
Configuring a Boot Level License	88
Installing SLAC for an HSECK9 License	91
Configuring a Numeric Throughput	92
Configuring a Tier-Based Throughput	95
Converting From a Numeric Throughput Value to a Tier	99
Upgrading from a Release Supporting Numeric Throughput to a Release Supporting Tiers	102
Downgrading from a Release Supporting Tiers to a Release Supporting Only Numeric Throughput	103
Available Licensing Models	103

CHAPTER 10

Consolidated Package Management 105

Running the Cisco Catalyst 8500 Series Edge Platforms: An Overview	105
Running the Cisco Catalyst 8500 Series Edge Platforms Using a Consolidated Package: An Overview	105
Running the Cisco Catalyst 8500 Series Edge Platforms: A Summary	106
Software File Management Using Command Sets	106
The request platform Command Set	106
The copy Command	107
Managing and Configuring the Router to Run Using Consolidated Packages	107
Quick Start Software Upgrade	107
Managing and Configuring a Router to Run Using a Consolidated Package	108
Managing and Configuring a Consolidated Package Using the copy Command	108
Managing and Configuring a Consolidated Package Using the request platform software package install Command	108
Installing the Software Using install Commands	109
Restrictions for Installing the Software Using install Commands	110
Information About Installing the Software Using install Commands	110
Install Mode Process Flow	110
Booting the Platform in Install Mode	116

One-Step Installation or Converting from Bundle Mode to Install Mode	116
Three-Step Installation	117
Upgrading in Install Mode	119
Downgrading in Install Mode	119
Terminating a Software Installation	119
Configuration Examples for Installing the Software Using install Commands	120
Troubleshooting Software Installation Using install Commands	132

CHAPTER 11 **Software Upgrade Processes** 133

CHAPTER 12	Factory Reset	135
	Feature Information for Factory Reset	135
	Information About Factory Reset	135
	Software and Hardware Support for Factory Reset	137
	Prerequisites for Performing Factory Reset	137
	Restrictions for Performing a Factory Reset	138
	When to Perform Factory Reset	138
	How to Perform a Factory Reset	138
	What Happens after a Factory Reset	139

CHAPTER 13	High Availability Overview	141
	Finding Feature Information in This Module	141
	Contents	142
	Software Redundancy on the Cisco 8500 Series Catalyst Edge Platform	142
	Software Redundancy Overview	142
	Configuring two Cisco IOS processes	142
	Example	143
	Stateful Switchover	143
	SSO-Aware Protocol and Applications	144
	IPsec Failover	144
	Bidirectional Forwarding Detection	144

CHAPTER 14	Using the Management Ethernet Interface	145
	Finding Feature Information in This Module	145

Contents	145
Gigabit Ethernet Management Interface Overview	145
Gigabit Ethernet Port Numbering	146
IP Address Handling in ROMmon and the Management Ethernet Port	146
Gigabit Ethernet Management Interface VRF	146
Common Ethernet Management Tasks	147
Viewing the VRF Configuration	147
Viewing Detailed VRF Information for the Management Ethernet VRF	147
Setting a Default Route in the Management Ethernet Interface VRF	147
Setting the Management Ethernet IP Address	148
Telnetting over the Management Ethernet Interface	148
Pinging over the Management Ethernet Interface	148
Copy Using TFTP or FTP	148
NTP Server	149
SYSLOG Server	149
SNMP-Related Services	149
Domain Name Assignment	149
DNS service	149
RADIUS or TACACS+ Server	150
VTY lines with ACL	150

CHAPTER 15

Configuring Bridge Domain Interfaces	151
Restrictions for Bridge Domain Interfaces	151
Information About Bridge Domain Interface	152
Ethernet Virtual Circuit Overview	152
Bridge Domain Interface Encapsulation	152
Assigning a MAC Address	153
Support for IP Protocols	153
Support for IP Forwarding	153
Packet Forwarding	154
Layer 2 to Layer 3	154
Layer 3 to Layer 2	154
Link States of a Bridge Domain and a Bridge Domain Interface	154
BDI Initial State	154

BDI Link State	155
Bridge Domain Interface Statistics	155
Creating or Deleting a Bridge Domain Interface	155
Bridge Domain Interface Scalability	156
Bridge-Domain Virtual IP Interface	156
How to Configure a Bridge Domain Interface	156
Example	158
Displaying and Verifying Bridge Domain Interface Configuration	158
Configuring Bridge-Domain Virtual IP Interface	160
Associating VIF Interface with a Bridge Domain	160
Verifying Bridge-Domain Virtual IP Interface	160
Example Configuration Bridge-Domain Virtual IP Interface	160

CHAPTER 16
Packet Trace 163

Information About Packet Trace	163
Usage Guidelines for Configuring Packet Trace	164
Configuring Packet Trace	164
Configuring Packet Tracer with UDF Offset	166
Displaying Packet-Trace Information	169
Removing Packet-Trace Data	170
Configuration Examples for Packet Trace	170
Example: Configuring Packet Trace	170
Example: Using Packet Trace	172
Additional References	177
Feature Information for Packet Trace	178

CHAPTER 17
EVPN VPWS over SR-TE Preferred Path 181

Feature Information for EVPN VPWS over SR-TE Preferred Path	181
Restrictions for EVPN VPWS over SR-TE Preferred Path	181
Information About EVPN VPWS over SR-TE Preferred Path	182
How to Configure EVPN VPWS over SR-TE Preferred Path	182
Configuring EVPN VPWS over SR-TE Preferred Path	182
Configuring EVPN VPWS over SR-TE Preferred Path with Fallback Disable	183
Removing Fallback Disable from EVPN VPWS over SR-TE Preferred Path	183

Disabling EVPN VPWS over SR-TE Preferred Path Configuration	183
Verifying EVPN VPWS over SR-TE Preferred Path	183

CHAPTER 18
Configuring SFP+ 185

CHAPTER 19
Cisco Thousand Eyes Enterprise Agent Application Hosting 187

Cisco ThousandEyes Enterprise Agent Application Hosting	187
Feature Information for Cisco ThousandEyes Enterprise Agent Application Hosting	188
Supported Platforms and System Requirements	188
Workflow to Install and Run the Cisco ThousandEyes Application	189
Workflow to Host the Cisco ThousandEyes Application	189
Downloading and Copying the Image to the Device	191
Connecting the Cisco ThousandEyes Agent with the Controller	193
Modifying the Agent Parameters	193
Uninstalling the Application	193
Troubleshooting the Cisco ThousandEyes Application	194



CHAPTER 1

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services.

- [Objectives, on page 1](#)
- [Document Revision History, on page 1](#)
- [Communications, Services, and Additional Information, on page 1](#)

Objectives

This document provides an overview of software functionality that is specific to the Cisco Catalyst 8500 Series Edge (includes Cisco Catalyst 8500 platform and Cisco Catalyst 8500L Series platform). It is not intended as a comprehensive guide to all of the software features that can be run using the Cisco Catalyst 8500 Series Edge Platforms, but only the software aspects that are specific to this platform.

For information on general software features that are also available on the Cisco Catalyst 8500 Series Edge Platforms, see the Cisco IOS XE technology guide for that specific software feature.

Document Revision History

The Document Revision History records technical changes to this document. The table shows the Cisco IOS XE software release number and document revision number for the change, the date of the change, and a brief summary of the change.

Release No.	Date	Change Summary
IOS XE 17.4	March 17, 2021	Included information on Cisco Catalyst 8500L Series platform.
IOS XE 17.3.2	October 22, 2020	First release of the book.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).

- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

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



CHAPTER 2

Read Me First

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

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



CHAPTER 3

Overview

Cisco 8500 Series Catalyst Edge Platform significantly increases services performance, router throughput, and router scale at lower costs.

This document covers configuration details for the following models:

- Catalyst 8500 Platforms (C8500-12X4QC, C8500-12X and C8500-20X6C)
- Catalyst 8500L Platform (C8500L-8S4X)

Features	C8500-12X4QC	C8500-12X	C8500L-8S4X	C8500-20X6C
Support for In-Service Software Upgrade (ISSU)	Not supported	Not supported	Not supported	Not supported
Data plane processing	QFP 3.0	QFP 3.0	Software-based	QFP 3.0
Support for Unified Threat Defense(UTD)	Not supported	Not supported	Support exists	Not Supported
Support for Fast Reroute(FRR)	Not supported	Not supported	Not supported	Support exists



CHAPTER 4

Software Packaging and Architecture

The Cisco Catalyst 8500 Series Edge Platform (includes Cisco Catalyst 8500 platform and Cisco Catalyst 8500L Series platform) introduces a new software packaging model and architecture.

This chapter discusses this new packaging and architecture and contains the following sections:

- [Software Packaging on the Cisco Catalyst 8500 Series Edge Platforms, on page 7](#)
- [Processes Overview, on page 10](#)

Software Packaging on the Cisco Catalyst 8500 Series Edge Platforms

This section covers the following topics:

Cisco Catalyst 8500 Series Edge Platforms Software Overview

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Consolidated Packages

A consolidated package is a single image composed of individual software subpackage files. A single consolidated package file is a bootable file, and the Cisco Catalyst 8500 Series Edge Platforms can be run using the consolidated package.

Each consolidated package also contains a provisioning file. A provisioning file is used for booting in cases where the individual subpackages are extracted from the consolidated package, or optional subpackages are used to run the router. For additional information on the advantages and disadvantages of running a complete consolidated package, see the *Running the Cisco Catalyst 8500 Series Edge Platforms: An Overview*.

Important Information About Consolidated Packages

The important information about consolidated packages include:

- For each version of a consolidated package, the RPBase, RPControl, and ESPBase subpackages are identical among consolidated packages.

- For each version of consolidated package, the RPIOS subpackage is always different among consolidated packages.
- A consolidated package file is a bootable file. If the router is configured to run using the complete consolidated package, boot the router using the consolidated package file. If the router is configured to run using individual subpackages, boot the router using the provisioning file. For additional information on the advantages and disadvantages of running a complete consolidated package, see the *Running the Cisco Catalyst 8500 Series Edge Platforms: An Overview* section .
- If you need to install optional subpackages, then you must boot the router using the individual subpackage provisioning file method.

Individual Software SubPackages Within a Consolidated Package

This section provides an overview of the Cisco Catalyst 8500 Series Edge Platforms subpackages and the purpose of each individual subpackage. Every consolidated package will have all of these individual subpackages. To see additional information about each individual subpackages in a particular Cisco IOS XE release, see *Cisco IOS XE Release Notes* for that release.

Table 1: Individual SubPackages

SubPackage	Purpose
RPBase	Provides the operating system software for the Route Processor.
RPControl	Controls the control plane processes that interface between the IOS process and the rest of the platform.
RPAccess	Exports processing of restricted components, such as Secure Socket Layer (SSL), Secure Shell (SSH), and other security features.
RPIOS	Provides the Cisco IOS kernel, which is where IOS features are stored and run. Each consolidated package has a different RPIOS.
ESPBase	Provides the ESP operating system and control processes, and the ESP software.

Important Notes About Individual SubPackages

The important information about individual subpackage include:

- Individual subpackages cannot be downloaded from Cisco.com individually. To get these individual subpackages, users must download a consolidated package and then extract the individual subpackages from the consolidated package using the command-line interface.
- If the router is being run using individual subpackages instead of being run using a complete consolidated package, the router must be booted using a provisioning file. A provisioning file is included in all consolidated packages and is extracted from the image along with the individual subpackages whenever individual subpackages are extracted.

Provisioning Files



Note You must use the provisioning files to manage the boot process if you need to install optional subpackages.

Provisioning files manage the boot process when the Cisco Catalyst 8500 Series Edge Platforms is configured to run using individual subpackages or optional subpackages (such as the package for the Cisco WebEx Node Cisco Catalyst 8500 Series Edge Platforms Series). When individual subpackages are being used to run the Cisco Catalyst 8500 Series Edge Platforms, the router has to be configured to boot the provisioning file. The provisioning file manages the bootup of each individual subpackage and the Cisco Catalyst 8500 Series Edge Platform assumes normal operation.

Provisioning files are extracted automatically when individual subpackage files are extracted from a consolidated package.

Provisioning files are not necessary for running the router using the complete consolidated package; if you want to run the router using the complete consolidated package, simply boot the router using the consolidated package file.

Important Notes About Provisioning Files

The important information about provisioning files include:

- Each consolidated package contains two provisioning files. One of the provisioning files is always named “packages.conf”, while the other provisioning file will have a name based on the consolidated package naming structure. In any consolidated package, both provisioning files perform the exact same function.
- In most cases, the “packages.conf” provisioning file should be used to boot the router. Configuring the router to boot using this file is generally easier because the router can be configured to boot using “packages.conf”, so no changes have to be made to the boot statement when Cisco IOS XE is upgraded (the **boot system file-system:packages.conf** configuration command can remain unmodified before and after an upgrade).
- The provisioning file and individual subpackage files must be kept in the same directory. The provisioning file does not work properly if the individual subpackage files are in other directories.
- The provisioning filename can be renamed; the individual subpackage filenames cannot be renamed.
- After placing the provisioning file and the individual subpackage files in a directory and booting the router, it is highly advisable not to rename, delete, or alter any of these files. Renaming, deleting, or altering the files can lead to unpredictable router problems and behaviors.

ROMmon Image

An independent ROMmon image is released periodically separate from consolidated packages or any other software releases.

See the documentation that accompanies the ROMmon image for information on each ROMmon image. For additional information on ROMmon, see the *Cisco Catalyst 8500 Series Edge Platforms Maintain and Operate Guide*.

File to Upgrade Field Programmable Hardware Devices

Starting in Cisco IOS XE Release 3.1.0S, a hardware programmable package file used to upgrade field programmable hardware devices is released as needed. A package file is provided for the field programmable device to customers in cases where a field upgrade is required. If the Cisco Catalyst 8500 Series Edge Platforms contains an incompatible version of the hardware programmable firmware, then that firmware may need to be upgraded.

Generally an upgrade is only necessary in cases where a system message indicates one of the field programmable devices on the Cisco Catalyst 8500 Series Edge Platforms needs an upgrade or a Cisco technical support representative suggests an upgrade.

For more information on upgrading field programmable hardware devices, see the *Upgrading Field Programmable Hardware Devices for Cisco Catalyst 8500 Series Edge Platforms* document.

Processes Overview

Cisco IOS XE has numerous components that run entirely as separate processes on the Cisco Catalyst 8500 Series Edge Platforms. This modular architecture increases network resiliency by distributing operating responsibility among separate processes rather than relying on Cisco IOS software for all operations.

IOS as a Process

In almost all previous Cisco router platforms, an overwhelming majority of the internal software processes are run using Cisco IOS memory.

The Cisco Catalyst 8500 Series Edge Platforms introduce a distributed software architecture that moves many operating system responsibilities out of the IOS process. In this architecture, IOS, which previously was responsible for almost all of the internal software processes, now runs as one of many Linux processes while allowing other Linux processes to share responsibility for running the router. This architecture allows for better allocation of memory so the router can run more efficiently.

Dual IOS Processes

The Cisco Catalyst 8500 Series Edge Platforms introduces a dual IOS process model that allows for increased high availability at all times.

Using SSO, a second IOS process can be enabled on a Cisco Catalyst 8500 Series Edge Router. On Cisco Catalyst 8500 Series Edge Platforms configured with dual Route Processors, the second IOS process runs on the standby Route Processor.

The state of these dual IOS processes can be checked by entering the **show platform** command.

The advantages of a second IOS process includes:

- Increased fault tolerance—In the event of an active IOS failure, the second IOS process immediately becomes the active IOS process with little to no service disruption.

File Systems on the Cisco Catalyst 8500 Series Edge Platforms

The following table provides a list of file systems that can be seen on the Cisco Catalyst 8500 Series Edge Platforms.

Table 2: File Systems

File System	Description
bootflash:	The boot flash memory file system on the active RP.
cns:	The Cisco Networking Services file directory.
harddisk:	The hard disk file system on the active RP.
nvrn:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl:	The file system for Onboard Failure Logging files.
system:	The system memory file system, which includes the running configuration.
tar:	The archive file system.
tmpsys:	The temporary system files file system.
usb[0-1]:	The Universal Serial Bus (USB) flash drive file systems on the active RP.

If you run into a file system not listed in the above table, enter the **?** help option or see the **copy** command reference for additional information on that file system.

Autogenerated File Directories and Files

This section discusses the autogenerated files and directories that might appear on your Cisco Catalyst 8500 Series Edge Platforms, and how the files in these directories can be managed.

The following table provides a list and descriptions of autogenerated files on the Cisco Catalyst 8500 Series Edge Platforms.

Table 3: Autogenerated Files

File or Directory	Description
crashinfo files	A crashinfo file may appear in the bootflash: or harddisk: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes, but the files are not part of router operations and can be erased without impacting the functioning of the router.
core directory	The storage area for core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.

File or Directory	Description
lost+found directory	This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.
tracelogs directory	The storage area for trace files. Trace files are useful for troubleshooting. Trace files, however, are not part of router operations and can be erased without impacting the router's performance.

Important Notes About Autogenerated Directories

The important information about autogenerated directories include:

- Any autogenerated file on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by customer support. Altering autogenerating files on the bootflash: can have unpredictable consequences for system performance.
- Crashinfo, core, and trace files can be deleted, but the core and tracelog directories that are automatically part of the harddisk: file system should not be deleted.



CHAPTER 5

Managing the SD-Routing Device Using Cisco SD-WAN Manager

This chapter includes information about managing and monitoring the SD-Routing devices using Cisco SD-WAN Manager. It contains the following sections:

- [Information About Using Cisco SD-WAN Manager to Monitor the SD-Routing Devices, on page 13](#)
- [Supported WAN Edge Devices, on page 15](#)
- [Onboarding the SD-Routing Devices , on page 17](#)
- [Software Image Management, on page 29](#)
- [Monitoring the Device Using Cisco SD-WAN Manager, on page 32](#)
- [Alarms and Events, on page 33](#)
- [Admin-Tech Files, on page 34](#)
- [Configuration Examples, on page 35](#)
- [Troubleshooting , on page 37](#)
- [Feature Information for Managing SD-Routing Devcies Using vManage, on page 38](#)

Information About Using Cisco SD-WAN Manager to Monitor the SD-Routing Devices

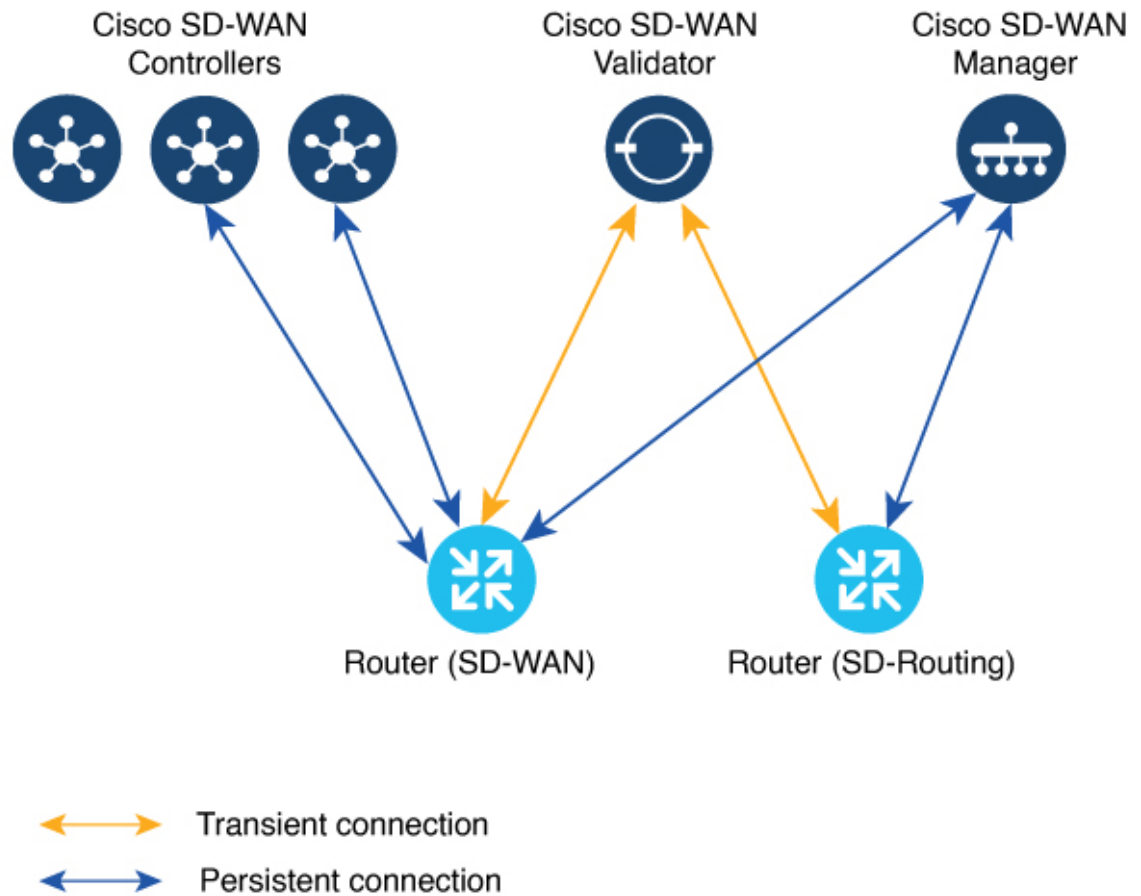
This feature allows you to perform the basic management capabilities through Cisco SD-WAN Manager on the Cisco IOS XE devices that are operating in non-SD-WAN mode. From Cisco IOS XE 17.12.1a onwards, such devices will be referred as SD-Routing devices. You can use a single Network Management System (NSM) (Cisco SD-WAN Manager) to manage and monitor all the Cisco IOS XE routers and help in simplifying solution deployments.



Note

The minimum software version required for this feature to work is Cisco IOS XE 17.12.1a and Cisco SD-WAN Release 20.12.1.

Figure 1: Managing the SD-Routing Devices



Benefits of Managing the SD-Routing Devices Using Cisco SD-WAN Manager

1. Use of a single NMS (Cisco SD-WAN Manager) for Cisco Catalyst SD-WAN and SD-Routing deployments in an Enterprise network.
2. Co-existence of Cisco SD-WAN and SD-Routing devices on the same Cisco SD-WAN Manager.

Prerequisites

The following are the prerequisites to onboard the SD-Routing devices:

- Ensure that the device run the Cisco IOS XE 17.12.1a image in install mode. For more information on the modes, see the [Modes Using Cisco CLI](#) section.
- A Cisco SD-WAN Manager instance either on-prem or hosted on a cloud.
- Connectivity from the device to the Cisco SD-WAN Manager.

- Enable netconf-yang models for enabling DMI which is required for managing from Cisco SD-WAN Manager.
- Devices operating in autonomous mode must be configured with the following basic configuration manually to establish the secure control connections with controllers (Cisco SD-WAN Validator and Cisco SD-WAN Manager):
 - System properties:
 - System-ip
 - Site-id
 - Organization-name
 - Cisco SD-WAN Validator information (IP address or FQDN Cisco SD-WAN Validator server)
 - Interface configuration:
 - Physical interface with a static or dynamic IP address and subnet mask
 - Dynamic routing or default route to provide reachability to Cisco SD-WAN Validator or Cisco SD-WAN Manager

Limitations

- Cisco SD-routing devices onboarding onto Cisco SD-WAN Manager is only supported with universalk9 images. No Payload Encryption (NPE) images are not supported.
- In Cisco IOS XE 17.12.1a release, basic monitoring is supported and additional features will be supported in the subsequent releases. For more information on supported features list, see the platform specific Release Notes.
- Cisco SD-Routing devices can only have one control connection to Cisco SD-WAN Manager from an interface with reachability to the controllers.
- Cisco SD-routing devices will not have any active connection with Cisco SD-WAN Controller.
- Dedicated management interface is not supported for the connection to the Cisco SD-WAN Manager.

Supported WAN Edge Devices

The table lists the supported WAN Edge platforms and onboarding options.

Table 4: Supported WAN Edge Platforms and Onboarding Options

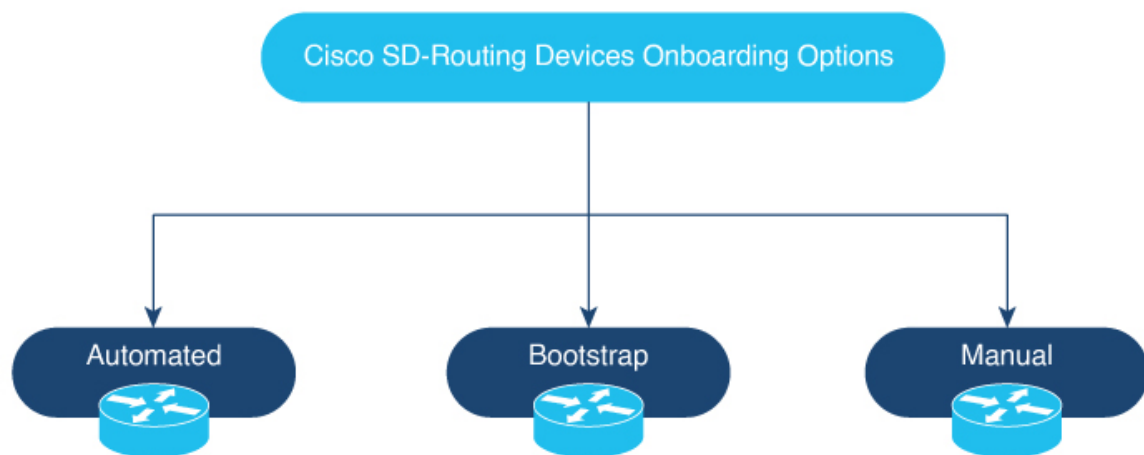
Platforms	Automated	Bootstrap	Manual
Cisco ASR 1000 Series Aggregation Services Routers			
ASR1001-HX	Yes	Yes	Yes
ASR1002-HX	Yes	Yes	Yes

Platforms	Automated	Bootstrap	Manual
Cisco 4400 Series Integrated Services Routers			
Cisco 4431 ISR	Yes	Yes	Yes
Cisco 4451 ISR	Yes	Yes	Yes
Cisco 4461 ISR	Yes	Yes	Yes
Cisco 4300 Series Integrated Services Routers			
Cisco 4321 ISR	Yes	Yes	Yes
Cisco 4331 ISR	Yes	Yes	Yes
Cisco 4351 ISR	Yes	Yes	Yes
Cisco 4200 Series Integrated Services Routers			
Cisco 4221 ISR	Yes	Yes	Yes
Cisco 100 Series Integrated Services Routers			
Cisco 1000 ISR	Yes	Yes	Yes
Cisco Catalyst 8000V Series Edge Platforms			
Cisco Catalyst 8000V	Not applicable Note Automated onboarding is applicable only for the hardware device.	Yes	Yes
Cisco Catalyst 8200 Series Edge Platforms			
C8200-1N-4T	Yes	Yes	Yes
C8200L-1N-4T	Yes	Yes	Yes
Cisco Catalyst 8300 Series Edge Platforms			
C8300-1N1S-4T2X 6T	Yes	Yes	Yes
C8300-2N2S-4T2X 6T	Yes	Yes	Yes
Cisco Catalyst 8500 Series Edge Platforms			
C8500-12X4QC	Yes	Yes	Yes
C8500-12X	Yes	Yes	Yes
C8500L-8S4X	Yes	Yes	Yes

Platforms	Automated	Bootstrap	Manual
C8500-20X6C	Yes	Yes	Yes

Onboarding the SD-Routing Devices

This section explains the workflows to onboard the SD-Routing devices:



- Onboarding the SD-Routing Devices
 - Automated Onboarding: Uses the Dynamic Host Configuration Protocol (DHCP and Cisco Plug and Play (PNP)) to automatically onboard the device to Cisco SD-WAN Manager.
 - Bootstrap Onboarding: Uses the bootstrap file either on the bootflash or on a USB and configures the device with the minimum configuration to reach the Cisco SD-WAN Manager.
 - Manual Onboarding: Configures the device manually using IOS-XE commands to onboard the device to Cisco SD-WAN Manager.

To onboard the SD-Routing devices, the prerequisites are:

- System IP

For manual Onboarding, the prerequisites are:

- Site ID
- Organization-name
- Cisco SD-WAN Validator information (IP address or FQDN Cisco SD-WAN Validator server)
- Interface for connection to Cisco SD-WAN Manager (Physical, Sub-interface, and Loopback)

Onboarding the SD-Routing Devices Using Automated Workflow

To onboard the SD-routing devices using the automated workflow, perform these steps:

- Configure the Plug and Play Connect Portal
- Configure the Cisco SD-WAN Manager using quick connect workflow
- Bring up the device in Day0 mode

Configuring the Plug and Play Connect Portal

To configure the PnP Connect portal, perform these steps:

Before you begin

Ensure that you can access to the PnP Connect portal and an active Smart Account and Virtual Account using your Cisco User ID. You have to also use a CCO ID that is associated as the Smart Account or Virtual Account admin of the account, on PnP Connect portal.



Note You can enable the PnP Connect Sync only after you enter the Smart Account credentials in the Cisco SD-WAN Manager Settings page.

-
- Step 1** Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.
- Step 2** Create a Controller Profile and upload the **root-ca** if it is for an Enterprise network.
- Note** If the overlay network is **Cisco PKI**, you do not have to upload any certificate.
- Step 3** Enter the Controller Profile with controller type as VBond and click **Next**.
- Step 4** Enter the required parameters in the **Add Controller Profile** and click **Next**.
- Step 5** Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.
-

Configuring the Cisco SD-WAN Manager Using Quick Connect Workflow

To configure the Cisco SD-WAN Manager using Quick Connect workflow, perform these steps:

-
- Step 1** From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.
- Step 2** Click **Get Started**.
- Step 3** Click **Next**.
- Step 4** If you have not uploaded the provisioning file (*.csv* or *.viptela*) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload** or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.
- Note** The *.csv* file is applicable only for hardware devices. The *.viptela* file is applicable for both hardware and software devices.

- Step 5** Click **Sync Smart Account** if you have not synernized it already. You should now see your device listed in the table of the devices.
Click Sync Smart Account,
- Step 6** Click **Next**.
- Step 7** In the Add and Review Device Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.
- Step 8** Click **Next**.
- Step 9** Add any option Tag and click **Next**.
- Step 10** To verify the device that is added , choose **Configuration> Devices** and click enable **Device Model** in Table Settings.
- Step 11** A list of routers in the network is displayed, showing detailed information about each router. To verify that the devices are added, select **Configuration > Certificates**.

Bringing Up the SD-Routing Device

To bring up the SD-Routing device, perform these steps:

- Step 1** Bring up the device in Day-0 state. If the device is not in Day-0 state, use either **controller-mode reset** or **writer erase** with **reload** option to bring it to Day-0 state.
- Step 2** Ensure that the device gets the IP address over DHCP on one of the interfaces other than the Gigabit Ethernet0 interface. Also, ensure that the device is reachable to devicehelper.cisco.com and the Cisco SD-WAN Validator.
- Note** Dedicated management interface is not supported for the connection to the Cisco SD-WAN Manager.
- Step 3** The device control connection comes up on Cisco SD-WAN Manager.
- Step 4** Verify the control connection status on the Edge device using the **show sd-routing connections summary** command:

Example:

Router#**show sd-routing connections summary**

PEER PEER TYPE IP	PEER PEER PROT	PEER SYSTEM IP	SITE ID PORT	PEER PUB PRIVATE STATE	PEER UP PRIVATE UPTIME	PEER PRIV PORT	PEER PUBLIC PUBLIC
Cisco SD-WAN Manager	dtls	172.16.255.22	200	10.0.12.22	12446 up	12:05:29:3	

- Step 5** Verify the control connection status on Cisco SD-WAN Manager.

Onboarding the SD-Routing Devices Using Bootstrap

To onboard the SD-Routing device using the bootstrap, perform these steps:

- Step 1** From the Cisco SD-WAN Manager menu, go to **Workflows > Quick Connect**.

Step 2 Click **Get Started**.

Step 3 Click **Next**.

Step 4 If you have not uploaded the provisioning file (.csv or .viptela) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload** or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.

Note The .csv file is applicable only for hardware devices. The .viptela file is applicable for both hardware and software devices.

Step 5 Select the device that you want to onboard and click **Next**.

Step 6 In the Add and Review Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.

Step 7 To verify the device that is added, choose **Configuration> Devices** and click enable **Device Model** in Table Settings.

Step 8 Ensure that the device is in valid state from **Configuration > Certificate** page.

Step 9 From the Cisco SD-WAN Manager menu, choose **Configuration> Devices**.

Step 10 For the Cisco SD-Routing software devices (Cisco c8000V), perform these steps to generated the bootstrap and onboard the device:

Note For hardware devices, follow the instructions in Step 11.

- a) Click ... at the right pane of the window and choose **Generate Bootstrap Configuration**.
- b) Choose Cloud-init option and enter a name for the WAN Interface Name and click **OK**.

Note Ensure that the DHCP is enabled on the selected interface and is reachable to Cisco SD-WAN Validator and Cisco SD-WAN Manager. Also, for the software device, use only Gigabit Ethernet1 interface as the VPN0 interface.

- c) Click **Download** to download the image on the device.

Example:

Sample image: ciscosdwan_cloud_init.cfg

Sample image with Certificate : ciscosdwan_cloud_init_with_ent_cert.cfg

- d) For cloud-based controllers, the downloaded bootstrap file can be added as a user data field when you deploy the device. It will bring up the controller in SD-Routing mode and establish the connection with Cisco SD-WAN Validator and Cisco SD-WAN Manager.

Step 11 For hardware devices, perform these steps to generate the bootstrap and onboard the device:

- a) From the Cisco SD-WAN Manager menu on the device page, click **Export Bootstrap Configuration**.
- b) Select the check box for SD-Routing. In the **Export Bootstrap Configuration** dialog box, enter the **WAN Interface name**.

Note The management interface name may vary among Cisco IOS XE device models. Specify the interface name based on the model you wish to onboard and which can reach the Cisco SD-WAN Validator and Cisco SD-WAN Controller.

- c) Click **Generate Generic Configuration** to download the generic .cfg bootstrap applicable for the hardware devices. Unzip the file and rename it as *ciscosdawn.cfg*.

Note Ensure that the DHCP is enabled on the selected interfaces and is reachable to Cisco SD-WAN Validator and Cisco SD-WAN Manager.

The bootstrap file will contain the organization name, Cisco SD-WAN validator IP, and root-ca certificates. For the enterprise network, it will have the enterprise root-ca- certificates.

- d) Copy the bootstrap file to the device bootflash as *ciscosdwan.cfg*.
- e) Execute the **sd-routing bootstrap load bootflash:ciscosdwan.cfg** command.

Example:

```
Router# sd-routing bootstrap load bootflash:ciscosdwan.cfg
Located the file. Beginning to extract the data
Extraction summary
-Organization name - "aniltb2"
-Interface - GigabitEthernet0/0/0
-vbond - 99.99.1.51
Successfully extracted root-cert info

Do you want to proceed and apply extracted
parameters to enable sd-routing feature?? (yes/[no]): yes
Successfully configured bootstrap extracted parameters
Router#
*May 10 08:56:11.159: %SYS-5-CONFIG_P: Configured programmatically by process Exec from console as console
*May 10 09:05:11.751: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully from
201.201.201.1:41902 for netconf over ssh. External groups
```

- f) Verify the control connection using these **show sd-routing system status**, **show sd-routing system status**, and **show sd-routing local-properties summary** commands.

Onboarding the Devices Manually

To onboard the SD-Routing devices manually, perform these steps:

- Step 1** From the Cisco SD-WAN Manager menu, go to **Workflows > Quick Connect**.
- Step 2** Click **Get Started**.
- Step 3** Click **Next**.
- Step 4** If you have not uploaded the provisioning file (*.csv* or *.viptela*) from PnP to Cisco SD-WAN Manager, you can use either **.csv upload** or **.viptela upload** or **Sync Smart Account** option to add the device to Cisco SD-WAN Manager. If the device is already added to Cisco SD-WAN Manager, select the **skip for now** option.

Note The *.csv* file is applicable only for hardware devices. The *.viptela* file is applicable for both hardware and software devices.
- Step 5** Select the device that you want to onboard and click **Next**.
- Step 6** In the Add and Review Configuration dialog box, enter the Site-ID, System-IP, Hostname, and click **Apply**.
- Step 7** To verify device that is added, choose **Configuration > Devices** and click enable **Device Model** in Table Settings.
- Step 8** A list of routers in the network is displayed with detailed information about each router. To verify that the devices are added, select **Configuration > Certificates**.

- Step 9** Preform one of the following steps based on the device that you want to onboard manually:
- For the hardware device, enter the initial day-0 configurations using the IOS command after a system boot up.
 - For the Cisco SD-Routing software devices, deploy the Cisco c8000v in Amazon Web Services (AWS) or Azure without the bootstrap.

- Step 10** Configure the minimum parameters to enable the control connection on Cisco SD-WAN Manager.

Example:

```
netconf-yang

sd-routing
  no ipv6-strict-control
  organization-name "%Your Org. Name%"
  site-id %id%
  system-ip %system ip%
  vbond name %vbond name or vbond ip%
  vbond port 12346
  wan-interface %uplink interface%

ip route 0.0.0.0 0.0.0.0 %next hop ip%

interface %uplink interface%
  ip address %dhcp or static%
  no shutdown
```

- Step 11** Configure the required parameter to enable the SD-Routing mode:
- Ensure that the interface is configured with a static IP address or through DHCP. Also, the interface must be in **no shut** state.
 - Configure either Validator IP or Validator Name.
 - Configure the System-IP, Site-ID, Organization-Name and WAN-Interface.

- Step 12** Verify that the feature is enabled by checking the status of the vdaemon.

Example:

```
Router# show platform software yang-management process state
Confd Status: Started
```

Process	Status	State
nesd	Running	Active
syncfd	Running	Active
ncsshd	Running	Not Applicable
dmiauthd	Running	Active
nginx	Running	Not Applicable
ndbmand	Running	Active
pubd	Running	Active

```
Router#show platform software process list r0 name vdaemon
```

```
Name: vdaemon
  Process id      : 29075
  Parent process id: 29070
  Group id       : 29075
  Status        : S
  Session id    : 8829
  User time     : 263002
  Kernel time   : 347183
  Priority      : 20
  Virtual bytes : 405110784
  Resident pages: 12195
  Resident limit: 18446744073709551615
```

Minor page faults: 716496

Major page faults: 9130

Step 13 If the overlay network is for an enterprise, install the root certificates using the **request platform software sd-routing root-cert-chain install bootflash:cacert.pem** command. If the Cisco SD-WAN Manager is configured with Enterprise Certificates instead of **Cisco PKI**, you must install the root certificate on the device.

Step 14 Perform one of the following steps based on the device:

- a) For Cisco 8000v device, copy the root certificate from the CA to Cisco 8000v.
- b) Cisco devices are loaded with PKI and symantec root-certificates by default. If you need to install the enterprise root-certificate, install the certificate using the **request platform software sd-routing root-cert-chain install <path-to-root-cert>** command.

Example:

```
Device# request platform software sd-routing root-cert-chain install bootflash:ctrl_mng/cacert.pem
```

Step 15 Install the client enterprise certificates.

Note By default, the certificates will be loaded on the hardware devices. This step is only applicable for manually onboarding the software devices.

Step 16 Generate a Certificate Signed Request (CSR) for the device using the **request platform software sd-routing csr upload <bootflash:ctrl_mng/test>** command. You can specify any name for the folder that is created within the *bootflash:ctrl_mng/* directory.

Step 17 Copy the generated CSR file to the directory where you have the Enterprise CA. You can sign the certificate using the root key and root CA certificate and generate the pem certificate file.

Step 18 Copy the generated *certificate.pem* file to the device and use the **request platform software sd-routing certificate install <path-to-certificate-file>** command to install the certificate in the device.

Step 19 Verify the installation status of the certificates.

Example:

```
SJC_Primary# show sd-routing local-properties summary
.....
certificate-status           Installed
certificate-validity         Valid
certificate-not-valid-before Apr 25 00:55:28 2023 GMT
certificate-not-valid-after  Apr 24 00:55:28 2024 GMT
.....
dns-name                    Validator
site-id                     100
tls-port                    0
system-ip                   172.16.255.11
chassis-num/unique-id       C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                  12345707
```

Step 20 Onboard the device on Cisco SD-WAN Manager. When you install the client certificate, ensure that you add the following in Cisco SD-WAN Manager .

- a) Get the Chassis number and Serial number. To get the Chassis number and Serial number, use the **show sd-routing local-properties** or **show sd-routing certificate serial** command.

```
Router# show sd-routing local-properties summary
chassis-num/unique-id       C8K-aa079ca1-c141-4ac6-9b76-05864005f94e
serial-num                  12345707
```

- b) Upload the chassis-id using the **request vedge add chassis-num** <Chassis id> **org-name** <Org Name> **serial-num** <Serial number from c8kv> command on all the controllers.

Or

- c) Create a *.viptela* file using the chassis number and serial number and upload the file to Cisco SD-WAN Manager and send to controllers.

Step 21 Verify the control connection status on Cisco SD-WAN Manager.

Example:

Router#**show sd-routing connections summary**

PEER	PEER	PEER		SITE	PEER		PRIV	
PEER					PUB			
TYPE	PROT	SYSTEM IP		ID	PRIVATE IP		PORT	PUBLIC
IP				PORT	STATE	UPTIME		
vmanage	dtls	172.16.255.22		200	10.0.12.22		12446	
10.0.12.22					12446 up	12:05:29:3		

Onboarding the Device by Activating the Chassis Using the Token

To activate the chassis number, perform these steps:



Note This method is supported only on Cisco SD-WAN software devices (Cisco c8000v).

Step 1 Add the device to Cisco SD-WAN Manager using PnP Smart Sync method.

Step 2 Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.

Step 3 Create a controller profile and upload the **root-ca** if it is for an Enterprise network.

Step 4 Enter the controller type as vBond and click **Next**.

Step 5 Enter the required parameters in the **Add Controller Profile** and click **Next**.

Step 6 Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Step 7 From the Cisco SD-WAN Manager menu, select **Administration** > **Settings**.

Step 8 Go to **Smart Account Credentials** and click **Edit**.

Step 9 Enter the **Username** and **Password** and click **Save**.

Step 10 You can import the device list from PnP Connect Portal using these methods:

- a) Go to **Configuration** > **Devices** and click **Sync Smart account**.

Or

- a) Upload the *.viptela* that is downloaded from PnP Connect. Go to **Controller profiles** and click **Download the Provisioning file**.

b) From the Cisco SD-WAN Manager menu, choose **Configuration > Devices > Upload WAN Edge List**.

Step 11 The device will be in autonomous mode with startup config. The device will not be in Day0 mode.

Step 12 Apply the minimum configuration on the device.

Example:

```
netconf-yang
!
sd-routing
  no ipv6-strict-control
  organization-name "vIptela Inc Regression"
  site-id 500
  system-ip 172.16.255.15
  vbond ip 10.0.12.26
  vbond port 12346
  wan-interface GigabitEthernet2
!
ip route 0.0.0.0 0.0.0.0 10.0.5.13
!
ip interface GigabitEthernet2
  ip address 10.0.5.11 255.255.255.0
  no shutdown
!
```

Step 13 From the Cisco SD-WAN Manager menu, choose **Configuration > Certificates** and get the UUID and One Time Password (OTP) of the device you want to onboard.

Step 14 To override the chassis number that is generated by the software device, use the **request platform soft sd-routing activate chassis <newly uploaded chassis id> token <token generated by Cisco SD-WAN Manager>** command.

Step 15 If the overlay network is for an enterprise, install the enterprise-root certificates using the request platform **software sd-routing root-cert-chain install bootflash:cacert.pem** command. If the overlay network is **Cisco PKI**, you do not have to install the root certificate.

Note You do not have to generate a Certificate Signing Request (CSR) and sign it. The CSR will be generated while executing the step 14.

Step 16 Verify the control connection status on the Edge device using these commands:

Example:

```
show sd-routing local-properties summary
show sd-routing local-properties wan ipv4
show sd-routing connections summary
show sd-routing connections history
```

Onboarding the Multi-Tenancy SD-Routing Devices

This section explains the workflows to onboard the Multi-Tenancy SD-Routing devices:

- Automated Onboarding
- Manual Onboarding

Onboarding the Multi-Tenancy SD-Routing Devices Using Automated Workflow

To onboard the a multi-tenancy SD-Routing device, perform these steps:

-
- Step 1** Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.
- Create a virtual account.
 - Create a controller profile and upload the root-ca if it is for an Enterprise network.
 - Enter the controller type as vBond and click **Next**.
 - Enter the required parameters in the **Add Controller Profile** and click **Next**.
 - Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.
- Or
- Step 2** From the Cisco SD-WAN Manager menu, go to **Workflows** > **Quick Connect**.
- Step 3** Click **Get Started**.
- Step 4** Click **Next**.
- Step 5** If you have not uploaded the .csv file to Cisco SD-WAN Manager, you can use one of the upload options to upload the file. Select **skip for now** option if you have uploaded the file.
- Step 6** Click **Sync Smart account** or **.csv upload** or **.viptela upload**. You should now see your device listed in the table of devices.
- Step 7** For Software device, generate bootstrap file as explained in previous section and add it as c8000v user config file.
- Note** For Multi-tenant setup, the System-IP must be configured only through quick connect workflow. You should not configure the system-IP using the CLI option.
- Step 8** Based on the device type, perform one of these steps:
- For the software device, deploy the Cisco c8000v in Azure or AWS and enter the bootstrap file either as custom data or user data input.
 - For hardware device, bring up the device in Day-0 state. If the device is not in Day-0 state, use either **controller-mode reset** or **writer erase** with **reload** option to bring it to Day-0 state.
- Step 9** The device comes up with the Cisco SD-WAN Manager.
- Step 10** To verify the status of the device, use the **show sd-routing connection summary status** and **show sd-routing local-properties summary** commands.
-

Onboarding the Multi-Tenancy SD-Routing Devices Manually

To onboard the Multi-Tenancy SD-Routing device manually, perform these steps:

-
- Step 1** Deploy the Cisco Catalyst 8000v in Azure or AWS in autonomous mode.
- Go to software.cisco.com > **Network Plug and Play** > **Manage Devices** and ensure that you have access to Smart Account and Virtual Account.
 - Create a virtual account.
 - Create a controller profile and upload the root-ca if it is for an Enterprise network.
 - Enter the controller type as vBond and click **Next**.
 - Enter the required parameters in the **Add Controller Profile** and click **Next**.

- f) Add the device to PnP Connect. When you add the device, in the Device Mode field, select **AUTONOMOUS** for device in SD-Routing mode from the drop-down list.

Step 2 Configure the minimum parameters to enable Netconf-Yang:

Example:

```
config terminal
  netconf-yang
end
```

Step 3 Check the status of the Netconf-Yang using the **show platform software yang-management process state** command.

Step 4 Configure the required parameter to enable the Cisco SD-Routing mode:

- Ensure that the interface is configured either with static IP address or through DHCP. Also, the interface must be in **no shut** state.
- Configure either Cisco SD-WAN Validator IP or Cisco SD-WAN Validator name.
- Configure the Cisco SD-WAN Validator, Site-ID, Organization-Name and WAN-Interface.

Note For Multi-tenant setup, the System-IP must be configured only through quick connect workflow. You must not configure the System-IP using the CLI option. Also, you do not have to configure the SP Organization Name for SD-Routing devices in Multi-tenant deployment. The organization name refers to tenant's organization name for Multi-tenant deployment. It is visible only under the **show sd-routing local-properties summary** command after the device is onboarded.

Step 5 Verify that the feature is enabled by checking the status of the vdaemon.

Example:

```
Router#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id        : 29075
  Status          : S
  Session id      : 8829
  User time       : 263002
  Kernel time     : 347183
  Priority         : 20
  Virtual bytes   : 405110784
  Resident pages  : 12195
  Resident limit  : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

Step 6 Verify the SD-Routing configurations in the Edge device. Also, get the chassis number for signing and upload to Cisco SD-WAN Manager WAN Edge List.

Step 7 To verify the status of the device, use this **show sd-routing local-properties summary** command.

Step 8 Copy the root-ca-chain.crt certificate from Cisco SD-WAN Manager into SD-Routing device.

Note This step is required only if you are using Enterprise certificate method. You can skip this step if you are using **Cisco PKI** method.

Step 9 Install the *root-ca-chain.crt* in SD-Routing device.

Step 10 Upload the provision file (*.Viptela*) from PnP to Cisco SD-WAN Manager WAN Edge List and send to controllers.

Step 11 Create a *.viptela* file using the chassis number, serial number and sign it. Upload the file to Cisco SD-WAN Manager and send to controllers.

- Step 12** Get the Token from Cisco SD-WAN Manager. To onboard the device by establishing the control connection with Cisco SD-WAN Validator and Cisco SD-WAN Manager, use the **request platform software sd-routing activate chassis-number <chassis-num> token <token>** command.
- Step 13** To verify the status of the device, use the **show sd-routing connection summary status** and **show sd-routing local-properties summary** commands.

Onboarding the Device to Cisco SD-WAN Manager Using One Touch Provisioning

To perform the one touch provisioning for a device, follow these steps:

Before you begin

When you configure a device by using the one touch provisioning, ensure that the process meets these requirements:

- Device must be in autonomous mode. You should stop the PnP discovery and device must have either a start up configuration or any configuration. The device should not be in Day-0 state.
- Device must be configured to reach Cisco SD-WAN Validator and Cisco SD-WAN over the WAN interface.

Device must have the minimum required configuration for SD-Routing feature to communicate with controllers.

Also, onboarding the device to Cisco SD-WAN Manager using One Touch Provisioning method eliminates these steps to add the device:

- Adding WAN Edge device to Cisco SD-WAN Manager by using **.csv** or **.viptela** or **sync smart account**.
- Cisco device must be configured in SD-routing mode. You have to use the Manual or Bootstrap method to configure the device without adding the device to Cisco SD-WAN Manager.

- Step 1** From the Cisco SD-WAN Manager menu, choose **Administration > Settings** and enable One Touch Provisioning.
- Step 2** Check if **One Touch Provisioning** is **Enabled**. If **Enabled**, go to Step 5.
- Step 3** If **One Touch Provisioning** is **Disabled**, click **Edit**.
- Step 4** For the **Enable Claim WAN Edges** setting, choose **Enabled** and click **Save**.
- Step 5** Go to **Configuration > Devices > Unclaimed Devices**.
- Choose the device you wish to claim and click **Claim Device(s)**.
 - The device is removed from **Unclaimed Devices List** and listed on **WAN Edge List**.
- Step 6** To verify the status of the device, use these **show sd-routing system status** , and **show sd-routing local-properties summary** commands.

Unprovisioning the Feature

To unprovision the feature, perform these steps:

Step 1 Remove the SD-Routing feature configuration from the device.

Example:

Note This option will delete all the certificates. You have to reinstall all the certificates.

Example:

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no sd-routing
Warning! Disabling this feature will result in deleting client certificates. Please backup the
certificates and use the CLIs to reinstall them on enabling this feature again.
Do you want to continue? (y/n)[n]: y
```

Step 2 Invalidate the device. For instructions, see the step 4 from the [Onboarding the Devices Manually, on page 21](#) section.

Step 3 To delete the device:

- a) From the Cisco SD-WAN Manager menu, choose **Configuration> Devices**.
- b) Click **WAN Edge List** and choose the device that you want to delete.
- c) Click **Delete WAN Edge**.
- d) Read the message and click **Yes**.

Software Image Management

This section explains the process to upgrade the software image. Cisco SD-WAN Manager supports uploading a prepackaged Cisco virtual machine image, *tar.gz*, or an image in *qcow2* format. It is mandatory to upload a scaffold file if you choose a *qcow2* image file. Similarly, you can now select either an image package file or a *qcow2* image file with a scaffold file when configuring a Virtual Network Function (VNF) during service chain creation. Cisco SD-WAN Manager communicates with NETCONF that uses a simple Remote Procedure Call to retrieve operational data when an autonomous mode device is onboarded in Cisco SD-WAN Manager. (NETCONF) is a standard transport protocol that communicates with network devices. NETCONF provides mechanisms to edit configuration data. Cisco SD-WAN Manager upgrade workflow for the SD-Routing device is similar to the Controller mode Workflows.



Note The minimum software version required for this feature to work is Cisco IOS XE 17.12.1a.

Software Upgrade Using CLI

To upgrade the software, perform these steps:

Before you begin

- Disk Space Check: Checks for available bootflash space for downloading and expanding image.
- Image repository Check: Checks for remote server reachability.
- Auto Boot Enable: Checks if auto boot is enabled on the device.

-
- Step 1** Download the Cisco IOS XE Release 17.12 image from the software page <https://software.cisco.com>.
- Step 2** Upload the image to the device.
- Step 3** Install the new software using the **install add file <bootflash:/file name> activate commit** command and activate.

Example:

```
Device# install add file <bootflash:/c8000v-universalk9.17.12.01.0.166070.SSA.bin activate commit
```

The device reloads when the activation is complete.

Note This is an interactive command and it prompts to review and accept it. This command fails if there is any unsaved configuration in the device. You will have to execute the **write memory** command and reinstall the software.

- Step 4** Verify the upgrade using the **install commit** command.
-

Add Software Images to the Repository

Before you can upgrade the software on an SD-Routing device or Cisco SD-WAN Manager to a new software version, you need to add the software image to the Cisco SD-WAN Manager software repository. For more information on uploading the Cisco Catalyst 8000v Edge software to Cisco SD-WAN Controller using Cisco SD-WAN Manager and Remote server, see the [Manage Software Repository](#) section of the *Cisco SD-WAN Monitor and Maintain Configuration Guide*.

Software Upgrade Using Cisco SD-WAN Manager

To upgrade the software image on a device, perform these steps:

Before you begin

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see [Downgrade a Cisco vEdge Device to an Older Software Image](#) in the Cisco SD-WAN Getting Started Guide.
- If you want to perform a Cisco SD-WAN Manager cluster upgrade see, [Upgrade Cisco vManage Cluster](#)
- Auto Boot Enable: Checks if auto boot is enabled on device.

-
- Step 1** From the Cisco SD-WAN Manager menu, choose **Maintenance > Software Upgrade**.
- Step 2** Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.

Step 3 In the table of devices, select the devices to upgrade by selecting the check box on the far left.

Note While upgrading Cisco SD-WAN Manager clusters, select all the nodes of the cluster in the table.

Step 4 Click **Upgrade**.

Step 5 In the **Software Upgrade** slide-in pane, do as follows:

- a) Choose the server from which the device should download the image: **vManage**, **Remote Server**, or **Remote Server – vManage**.

- Note**
- If you chose **Remote Server**, ensure that the device can reach the remote server.
 - When downloading an image from a remote server manually, ensure that only the following valid characters are used:
 - User ID: a-z, 0-9, ., _ , -
 - Password: a-z, A-Z, 0-9, _ , *, ., +, =, %, -
 - URL Name or Path: a-z, A-Z, 0-9, _ , *, ., +, =, %, -, :, /, @, ?, ~

- b) For **SD-WAN Manager**, choose the image version from the **Version** drop-down list.
- c) For **Remote Server – SD-WAN Manager**, choose the **vManage OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.
- d) Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

Note The **Activate and Reboot** option is not available while upgrading Cisco SD-WAN Manager software. You must activate the image after the upgrade task is completed and reboot Cisco SD-WAN Manager.

- e) Click **Upgrade**

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

Step 6 Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.

Step 7 From the Cisco SD-WAN Manager menu, choose **Maintenance > Software Upgrade** and view the devices.

Step 8 Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.

Step 9 In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

- Note**
- If the control connection to Cisco SD-WAN Manager does not come up within the configured time limit, Cisco SD-WAN Manager automatically reverts the device to the previously running software image.
 - If you upgrade the Cisco VEdge software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco VEdge software.

Delete a Software Image

To delete a software image from a SD-Routing device:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance > Software Upgrade**.
2. Click **WAN Edge, Controller, or Cisco SD-WAN Manager**.
3. Choose one or more devices from which you want to delete a software image.
4. Click the **Delete Available Software**.
The **Delete Available Software** dialog box opens.
5. Choose the software version to delete.
6. Click **Delete**.

View Log of Software Upgrade Activities

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon.
Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.
2. Click the **Arrow** icon to see details of a task. Cisco SD-WAN Manager opens a status window displaying the status of the task and details of the device on which the task was performed.

Monitoring the Device Using Cisco SD-WAN Manager

The **Monitor** window provides a single-page, real-time user interface that facilitates a consolidated view of all the monitoring components and services of a Cisco SD-Routing devices. You can establish the connection and monitor the device using the following options:

- SSH Terminal
- Ping
- Traceroute

Also, you can collect the system status information in a compressed *.tar* file. Cisco SD-WAN Manager can retrieve and download a *.tar* file from the device. After retrieving the file, you can delete the copy of the file on the device to free up the disk space.

When you enable the SD-Routing mode, this feature is enabled on the device and Cisco SD-WAN Manager by default.

Monitoring the Device Using SSH

To establish the connection and monitor the device using the SSH option, perform these steps:

-
- Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**.

- Step 2** Choose a device from the list of devices that is displayed.
- Step 3** For a single device, click . . . for the desired device and choose **SSH Terminal**.
(Or)
- Step 4** From the Cisco SD-WAN Manager menu, choose **tools > SSH Terminal**.
- Step 5** Enter the password twice (same as SD-Routing) in the terminal to establish the connection with the device.
- Step 6** From the terminal, execute the **show commands** to monitor the device.
-

Pinging the Device

To ping the device, perform these steps:

- Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**.
- Step 2** Choose a device from the list of devices that is displayed.
- Step 3** For a single device, click . . . for the desired device and choose **Ping**.
- Step 4** From the **Monitor** page, enter the destination IP address.
- Step 5** Click **Ping**.
- The results of the ping will be printed in the window below.
-

Tracing the Route

To establish the connection and monitor the device using the trace routing option, perform these steps:

- Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**.
- Step 2** Choose a device from the list of devices that is displayed.
- Step 3** For a single device, click . . . for the desired device and choose **Trace Route**.
- Step 4** From the **Trace Route** page, enter the destination IP address.
- Step 5** Click the **Start** button to trace the route.
-

Alarms and Events

When an even occurs on an individual device in the overlay network, the device reports it by sending a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager then filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.

Use the Alarms screen to display detailed information about alarms generated by SD-Routing devices in the overlay network.

Monitoring the Alarms and Events

You can view alarms from the Cisco SD-WAN Manager dashboard by clicking the **Bell** icon at the top-left corner. The alarms are grouped into Active or Cleared. By default, alarms are displayed for the last 24 hours. Alternatively, follow these steps to view alarms from the **Alarms** screen in Cisco SD-WAN Manager.

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor > Devices > Logs**.

Step 2 From the Cisco SD-WAN Manager menu, choose **Monitor > Alarms**.

The alarms are displayed in graphical and tabular formats.

Step 3 To view more details for a specific alarm, click ... for the desired alarm, and then click **Alarm Details**.

The **Alarm Details** window opens and displays the probable cause of the alarm, impacted entities, and other details.

Admin-Tech Files

You can view the generated admin-tech files whenever the admin-tech files are available on a device.

You can view the list of generated admin-tech files and then decide which files to copy from your SD-Routing device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.

Requesting the Admin-tech File Using Cisco SD-WAN Manager

An Admin-tech file is a collection of system status information used for troubleshooting a given issue. To request a Admin-tech file, perform these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Tools > Operational Commands**.

Step 2 For a single device, click ... for the desired device and choose **Generate Admin Tech**.

Step 3 In the **Generate admin-tech File** window, limit the contents of the Admin-tech tar file if desired:

- a) The **Include Logs** check box is checked by default. Uncheck this check box to omit any log files from the compressed tar file.
- b) Check the **Include Cores** check box to include any core files.

Note The core files are stored in the *bootflash:/core* or *harddisk:/core* directory on the local device.

- c) Check the **Include Tech** check box to include any files related to device processes (daemons), memory details and operations.

Step 4 Click **Generate**.

Cisco SD-WAN Manager creates the Admin-tech file. The file name format is *hostname-date-time-admin-tech.tar.gz*.

Step 5 To view the generated Admin-tech file, from the Cisco SD-WAN Manager menu, choose **Tools > Operational Commands > Show Admin Tech List**.

Requesting the Admin-tech File Using CLI

To request a Admin-tech file using CLI, perform these steps:

Use the **request tech-support** command to generate the admin-tech file.

```
Device#request tech-support
21:03:46.447 UTC Thu Aug 10 2023 : Collecting 'show tech-support'...
21:04:51.880 UTC Thu Aug 10 2023 : 'show tech-support' collected successfully!
21:04:55.091 UTC Thu Aug 10 2023 : Collecting binary traces...
21:04:55.216 UTC Thu Aug 10 2023 : Binary traces collected successfully!
21:04:55.219 UTC Thu Aug 10 2023 : Collecting platform-dependent files...
21:05:43.467 UTC Thu Aug 10 2023 : Platform-dependent files collected successfully!
21:05:43.475 UTC Thu Aug 10 2023 : Generating tech-support bundle...
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle file
bootflash:core/1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz [size: 8648 KB]
21:05:56.648 UTC Thu Aug 10 2023 : Tech-support bundle generated successfully!

1HX-2017#
1HX-2017#dir bootflash:core
Directory of bootflash:/core/

1471682  -rw-                1  Aug 11 2023  04:26:51 +00:00  .callhome
45      -rw-                25429  Aug 10 2023  21:05:56 +00:00
1HX-2017_RP_0-debug_bundle_20230810-210346-UTC-info.txt
49      -rw-                8854997  Aug 10 2023  21:05:54 +00:00
1HX-2017-debug_bundle_20230810-210346-UTC.tar.gz
1471685  drwx                4096  Mar 22 2021  20:03:54 +00:00  modules

29633794048 bytes total (16795193344 bytes free)
1HX-2017#
```

Monitoring the Real Time Data

To ping the device, perform these steps:

- Step 1** From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**.
 - Step 2** Choose a device from the list of devices that is displayed.
 - Step 3** For a single device, click ... for the desired device and choose **Real Time**.
 - Step 4** Select the category of data from the **Device Options** drop-down list.
- The results will be displayed.

Configuration Examples

This section provides the configuration examples.

Example: Enabling Control Connection on Cisco SD-WAN Manager

This example shows how to enable control connection on Cisco SD-WAN Manager:

```
(config) sd-routing
(config-sd-routing) system-ip 172.16.255.15
(config-sd-routing) organization-name viptela
(config-sd-routing) vbond ip 10.0.12.26
(config-sd-routing) site-id 500
(config-sd-routing) wan-interface GigabitEthernet2
```

Example: Verifying the Enable Control Connection

Use the **show platform software yang-management process state** command to check the connection status.

```
Device#show platform software yang-management process state
ConfD Status: Started
```

Process	Status	State
nesd	Running	Active
syncfd	Running	Active
ncsshd	Running	Not Applicable
dmiauthd	Running	Active
nginx	Running	Not Applicable
ndbmand	Running	Active
pubd	Running	Active

Use the **show platform software yang-management process list r0 name vdaemon** command to check the vdaemon status.

```
Device#show platform software process list r0 name vdaemon
Name: vdaemon
  Process id       : 29075
  Parent process id: 29070
  Group id        : 29075
  Status          : S
  Session id      : 8829
  User time       : 263002
  Kernel time     : 347183
  Priority         : 20
  Virtual bytes   : 405110784
  Resident pages  : 12195
  Resident limit  : 18446744073709551615
  Minor page faults: 716496
  Major page faults: 9130
```

Example: Installing the Root Certificate

This examples shows how to install the root certificate:

```
Device# request platform software sd-routing root-cert-chain install bootflash:root-ca.crt
```

Example: Verifying the Root Certificate Installation

Use the **show sd-routing local-properties summary** command to check the root certificate installation status.


```

Device#show sd-routing local-properties summary
personality                vedge
sp-organization-name       vIPtela Inc Regression
organization-name          vIPtela Inc Regression
root-ca-chain-status       Installed
root-ca-crl-status         Not-Installed

Device#show sd-routing local-properties summary
certificate-status          Installed
certificate-validity        Valid
certificate-not-valid-before Apr 25 00:55:28 2023 GMT
certificate-not-valid-after  Apr 24 00:55:28 2024 GMT
.....
dns-name                   vbond
site-id                    100
tls-port                   0
system-ip                  172.16.255.11
chassis-num/unique-id      C8K-aa079cal-c141-4ac6-9b76-05864005f94e
serial-num                 12345707

```

Troubleshooting

This section provides commands that can be used to troubleshoot the common issues while managing and monitoring the SD-Routing devices using Cisco SD-WAN Manager:

- **Show version**



Note The operating mode is included in **show version** command.

When sd-routing feature is enabled:

```

Device#show version | include mode
Router operating mode: Autonomous (SD-Routing)
Device#

```

When sd-routing feature is not enabled:

```

Device#show version | include mode
Router operating mode: Autonomous
Device#

```

- **show platform software yang-management process state**
- **show sd-routing system status**
- **show sd-routing connections summary**
- **show platform software process list r0 name vdaemon**
- **show sd-routing local-properties summary**
- **show sd-routing local-properties wan ipv4**
- **show sd-routing local-properties vbond**
- **show sd-routing connections history**

Feature Information for Managing SD-Routing Devcies Using vManage

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for SD-Routing Devcies Using Cisco SD-WAN Manager

Feature Name	Releases	Feature Information
Managing SD-Routing Devices Using Cisco SD-WAN Manager	Cisco IOS XE Release 17.12.1a	This feature allows you to perform management operations for SD-Routing devices using Cisco SD-WAN Manager. You can use a single network manage system (Cisco SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.



CHAPTER 6

Deploy IOS-XE and SDWAN

- Overview, on page 39
- Restrictions, on page 39
- Autonomous or Controller Mode, on page 39
- Switch Between Controller and Autonomous Modes, on page 39
- PnP Discovery Process, on page 40

Overview

You can use the universalk9 image to deploy both Cisco IOS XE SD-WAN and Cisco IOS XE on Cisco IOS XE devices. This helps in seamless upgrades of both the SD-WAN and non SD-WAN features and deployments.

Restrictions

Autonomous or Controller Mode

Access the Cisco IOS XE and Cisco IOS XE SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the routers and includes the Cisco IOS XE functionality. To access Cisco IOS XE SD-WAN functionality switch to the Controller mode.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html#Cisco_Concept.dita_42020dbf-1563-484f-8824-a0b3f468e787

Switch Between Controller and Autonomous Modes

The default mode of the device is autonomous mode. Use the **controller-mode** command in Privileged EXEC mode to switch between controller and autonomous modes.

The **controller-mode enable** command switches the device to controller mode

The **controller-mode disable** command switches the device to autonomous mode

For information see [Cisco SD-WAN Getting Started Guide](#)

PnP Discovery Process

You can use the existing Plug and Play Workflow to determine the mode of the device.

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change, if required. This discovery is based on the controller profile attached to the device UID in the smart account/virtual account. The mode change results in a reboot of the device. Once reboot is complete, the device performs appropriate discovery process.

Plug and Play (PnP) deployment include the following discovery process scenarios:

Boot up Mode	Discovery Process	Mode Change
Autonomous	Plug and Play Connect Discovery or on-premise plug and play server discovery	No Mode change
Controller	Plug and Play Connect Discovery or on-premise plug and play server discovery	Mode change to autonomous mode



CHAPTER 7

Using Cisco IOS XE Software

This chapter provides information to prepare you to configure the Cisco Catalyst 8500 Series Edge Platforms:

- [Accessing the CLI Using a Router Console, on page 41](#)
- [Using Keyboard Shortcuts, on page 45](#)
- [Using the History Buffer to Recall Commands, on page 46](#)
- [Understanding the Command Mode, on page 46](#)
- [Getting Help, on page 47](#)
- [Using the no and default Forms of Commands, on page 51](#)
- [Saving Configuration Changes, on page 51](#)
- [Managing Configuration Files, on page 51](#)
- [Dynamic Allocation of Cores, on page 53](#)
- [Filtering the Output of the show and more Commands, on page 53](#)
- [Disabling Front-Panel USB Ports, on page 54](#)
- [Powering Off a Router, on page 55](#)
- [Finding Support Information for Platforms and Cisco Software Images, on page 55](#)

Accessing the CLI Using a Router Console

The following sections describe how to access the command-line interface (CLI) using a directly-connected console or by using Telnet or a modem to obtain a remote console:

Accessing the CLI Using a Directly-Connected Console

This section describes how to connect to the console port on the router and use the console interface to access the CLI.

The console port on a Cisco Catalyst 8500 Series Edge Platforms is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is located on the front panel of each Route Processor (RP).

Connecting to the Console Port

To connect to the console port, complete the following steps:

SUMMARY STEPS

1. Configure your terminal emulation software with the following settings:
2. Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or using the RJ-45-to-DB-9 DTE adapter (labeled “Terminal”).

DETAILED STEPS

-
- Step 1** Configure your terminal emulation software with the following settings:
- 9600 bits per second (bps)
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
- Step 2** Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or using the RJ-45-to-DB-9 DTE adapter (labeled “Terminal”).
-

Using the Console Interface

Every RP on a Cisco Catalyst 8500 Series Edge Platforms has a console interface. Notably, a standby RP can be accessed using the console port in addition to the active RP in a dual RP configuration.

To access the CLI using the console interface, complete the following steps:

SUMMARY STEPS

1. After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the following prompt appears:
2. Press **Return** to enter user EXEC mode. The following prompt appears:
3. From user EXEC mode, enter the **enable** command as shown in the following example:
4. At the password prompt, enter your system password. If an enable password has not been set on your system, this step may be skipped. The following example shows entry of the password enablepass:
5. When your enable password is accepted, the privileged EXEC mode prompt appears:
6. You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.
7. To exit the console session, enter the **quit** command as shown in the following example:

DETAILED STEPS

-
- Step 1** After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the following prompt appears:

Example:

```
Press RETURN to get started.
```

- Step 2** Press **Return** to enter user EXEC mode. The following prompt appears:

Example:

```
Router>
```

Step 3 From user EXEC mode, enter the **enable** command as shown in the following example:

Example:

```
Router> enable
```

Step 4 At the password prompt, enter your system password. If an enable password has not been set on your system, this step may be skipped. The following example shows entry of the password enablepass:

Example:

```
Password: enablepass
```

Step 5 When your enable password is accepted, the privileged EXEC mode prompt appears:

Example:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the console session, enter the **quit** command as shown in the following example:

Example:

```
Router# quit
```

Accessing the CLI from a Remote Console Using Telnet

This section describes how to connect to the console interface on a router using Telnet to access the CLI.

Preparing to Connect to the Router Console Using Telnet

Before you can access the router remotely using Telnet from a TCP/IP network, you need to configure the router to support virtual terminal lines (vty) using the **line vty** global configuration command. You also should configure the vty to require login and specify a password.

**Note**

To prevent disabling login on the line, be careful that you specify a password with the **password** command when you configure the **login** line configuration command. If you are using authentication, authorization, and accounting (AAA), you should configure the **login authentication** line configuration command. To prevent disabling login on the line for AAA authentication when you configure a list with the **login authentication** command, you must also configure that list using the **aaa authentication login** global configuration command. For more information about AAA services, see the *Cisco IOS XE Security Configuration Guide*, and the *Cisco IOS Security Command Reference Guide*.

In addition, before you can make a Telnet connection to the router, you must have a valid host name for the router or have an IP address configured on the router. For more information about requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, see the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Using Telnet to Access a Console Interface

To access a console interface using Telnet, complete the following steps:

SUMMARY STEPS

1. From your terminal or PC, enter one of the following commands:
2. At the password prompt, enter your login password. The following example shows entry of the password `mypass`:
3. From user EXEC mode, enter the **enable** command as shown in the following example:
4. At the password prompt, enter your system password. The following example shows entry of the password `enablepass`:
5. When the enable password is accepted, the privileged EXEC mode prompt appears:
6. You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.
7. To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

DETAILED STEPS

Step 1 From your terminal or PC, enter one of the following commands:

- **connect** *host* [*port*] [*keyword*]
- **telnet** *host* [*port*] [*keyword*]

In this syntax, *host* is the router hostname or an IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information, see the *Cisco IOS Configuration Fundamentals Command Reference Guide*.

Note If you are using an access server, then you will need to specify a valid port number such as **telnet 172.20.52.40 2004**, in addition to the hostname or IP address.

The following example shows the **telnet** command to connect to the router named `router`:

Example:

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

Step 2 At the password prompt, enter your login password. The following example shows entry of the password `mypass`:

Example:

```
User Access Verification
Password: mypass
```

Note If no password has been configured, press **Return**.

Step 3 From user EXEC mode, enter the **enable** command as shown in the following example:

Example:

```
Router> enable
```

Step 4 At the password prompt, enter your system password. The following example shows entry of the password enablepass:

Example:

```
Password: enablepass
```

Step 5 When the enable password is accepted, the privileged EXEC mode prompt appears:

Example:

```
Router#
```

Step 6 You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

Step 7 To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

Example:

```
Router# logout
```

Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

The following table lists the keyboard shortcuts for entering and editing commands.

Table 6: Keyboard Shortcuts

Keystrokes	Purpose
Ctrl-B or the Left Arrow key ¹	Move the cursor back one character
Ctrl-F or the Right Arrow key ¹	Move the cursor forward one character
Ctrl-A	Move the cursor to the beginning of the command line
Ctrl-E	Move the cursor to the end of the command line
Esc B	Move the cursor back one word
Esc F	Move the cursor forward one word

¹ The arrow keys function only on ANSI-compatible terminals such as VT100s.

Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

The following table lists the history substitution commands.

Table 7: History Substitution Commands

Command	Purpose
Ctrl-P or the Up Arrow key ²	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Ctrl-N or the Down Arrow key ¹	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.
Router# show history	While in EXEC mode, list the last several commands you have just entered.

² The arrow keys function only on ANSI-compatible terminals such as VT100s.

Understanding the Command Mode

The command modes available in the traditional Cisco IOS CLI are exactly the same as the command modes available in Cisco IOS XE.

You use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

The following table describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

Table 8: Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the logout command.
Privileged EXEC	From user EXEC mode, use the enable EXEC command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal privileged EXEC command.	Router (config) #	To return to privileged EXEC mode from global configuration mode, use the exit or end command.
Interface configuration	From global configuration mode, specify an interface using an interface command.	Router (config-if) #	To return to global configuration mode, use the exit command. To return to privileged EXEC mode, use the end command.
Diagnostic	<p>The router boots up or accesses diagnostic mode in the following scenarios:</p> <p>In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will.</p> <p>A user-configured access policy was configured using the transport-map command that directed the user into diagnostic mode. See the Chapter 4, “Console Port, Telnet, and SSH Handling” of this book for information on configuring access policies.</p> <p>The router was accessed using a Route Processor auxiliary port.</p> <p>A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered and the router was configured to go into diagnostic mode when the break signal was received.</p>	Router (diag) #	<p>If the IOS process failing is the reason for entering diagnostic mode, the IOS problem must be resolved and the router rebooted to get out of diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the router is accessed through the Route Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway.</p>
ROM monitor	From privileged EXEC mode, use the reload EXEC command. Press the Break key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the continue command.

Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the commands listed in the following table:

Table 9: Help Commands and Purpose

Command	Purpose
help	Provides a brief description of the help system in any command mode.
abbreviated-command-entry?	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<Tab>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command ?	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Finding Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS XE software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

The following table shows examples of how you can use the question mark (?) to assist you in entering commands.

Table 10: Finding Command Options

Command	Comment
Router> enable Password: <password> Router#	Enter the enable command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a “#” from the “>”; for example, Router> to Router# .
Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)# .

Command	Comment
<pre> Router(config)# interface serial ? <0-6> Serial interface number Router(config)# interface serial 4 ? / Router(config)# interface serial 4/ ? <0-3> Serial interface number Router(config)# interface serial 4/0 ? <cr> Router(config)# interface serial 4/0 Router(config-if)# </pre>	<p>Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.</p> <p>When the <cr> symbol is displayed, you can press Enter to complete the command.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)# .</p>
<pre> Router(config-if)# ? Interface configuration commands: . . . ip Interface Internet Protocol config commands keepalive Enable keepalive lan-name LAN Name command llc2 LLC2 Interface Subcommands load-interval Specify interval for load calculation for an interface locaddr-priority Assign a priority group logging Configure logging for interface loopback Configure internal loopback on an interface mac-address Manually set interface MAC address mls mls router sub/interface commands mpoa MPOA interface configuration commands mtu Set the interface Maximum Transmission Unit (MTU) netbios Use a defined NETBIOS access list or enable name-caching no Negate a command or set its defaults nrzi-encoding Enable use of NRZI encoding ntp Configure NTP . . . Router(config-if)# </pre>	<p>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</p>

Finding Command Options

Command	Comment
<pre>Router(config-if)# ip ? Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# ip</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>
<pre>Router(config-if)# ip address ? A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip address command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the negotiated keyword.</p> <p>A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 ? A.B.C.D IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	<p>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ? secondary Make this IP address a secondary address <cr> Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you can enter the secondary keyword, or you can press Enter.</p> <p>A <cr> is displayed; you can press Enter to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, Enter is pressed to complete the command.</p>

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the command **default command-name**, you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function of the **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

This task saves the configuration to NVRAM.

Managing Configuration Files

On the Cisco Catalyst 8500 Series Edge Platforms, the startup configuration file is stored in the nvram: file system and the running-configuration files are stored in the system: file system. This configuration file storage setup is not unique to the Cisco Catalyst 8500 Series Edge Platforms and is used on several Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router's other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

The **copy** command can be used to backup startup configuration files. The following examples show the startup configuration file in NVRAM being backed up:

Example 1: Copying a Startup Configuration File to Bootflash

```

Router# dir bootflash:
Directory of bootflash:/
 11 drwx 16384 Sep 18 2020 15:16:35 +00:00 lost+found
1648321 drwx 4096 Oct 22 2020 12:08:47 +00:00 .installer
97921 drwx 4096 Sep 18 2020 15:18:00 +00:00 .rollback_timer
12 -rw- 1910 Oct 22 2020 12:09:09 +00:00 mode_event_log
1566721 drwx 4096 Sep 18 2020 15:33:23 +00:00 core
1215841 drwx 4096 Oct 22 2020 12:09:48 +00:00 .prst_sync
1289281 drwx 4096 Sep 18 2020 15:18:18 +00:00 bootlog_history
13 -rw- 133219 Oct 22 2020 12:09:34 +00:00 memleak.tcl
14 -rw- 20109 Sep 18 2020 15:18:39 +00:00 ios_core.p7b
15 -rwx 1314 Sep 18 2020 15:18:39 +00:00 trustidrootx3_ca.ca
391681 drwx 4096 Oct 6 2020 15:08:54 +00:00 .dbpersist
522241 drwx 4096 Sep 18 2020 15:32:59 +00:00 .inv
783361 drwx 49152 Oct 27 2020 08:36:44 +00:00 tracelogs
832321 drwx 4096 Sep 18 2020 15:19:17 +00:00 pnp-info
1207681 drwx 4096 Sep 18 2020 15:19:20 +00:00 onep
750721 drwx 4096 Oct 22 2020 12:09:57 +00:00 license_evlog
946561 drwx 4096 Sep 18 2020 15:19:24 +00:00 guest-share
383521 drwx 4096 Sep 18 2020 15:34:13 +00:00 pnp-tech
1583041 drwx 4096 Oct 22 2020 11:27:38 +00:00 EFI
16 -rw- 34 Oct 6 2020 13:56:03 +00:00 pnp-tech-time
17 -rw- 82790 Oct 6 2020 13:56:14 +00:00 pnp-tech-discovery-summary
18 -rw- 8425 Oct 6 2020 15:09:18 +00:00 lg_snake
19 -rw- 6858 Oct 7 2020 10:53:21 +00:00 100g_snake
20 -rw- 4705 Oct 22 2020 13:01:54 +00:00 startup-config

26975526912 bytes total (25538875392 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
3517 bytes copied in 0.647 secs (5436 bytes/sec)

```

Example 2: Copying a Startup Configuration File to USB Flash Disk

```

Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 Oct 27 2020 14:10:20 -07:00
c8000aep-universalk9.17.02.01.SPA.bin
255497216 bytes total (40190464 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
3172 bytes copied in 0.214 secs (14822 bytes/sec)
Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 Oct 27 2020 14:10:20 -07:00
c8000aep-universalk9.17.02.01.SPA.bin
15:40:45 -07:00 startup-config255497216 bytes total (40186880 bytes free)

```

Example 3: Copying a Startup Configuration File to a TFTP Server

```

Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)

```

For more detailed information on managing configuration files, see the *Managing Configuration Files* section in the *Cisco IOS XE Configuration Fundamentals Configuration Guide*

Dynamic Allocation of Cores

Dynamic core allocations on the Cisco Catalyst 8500L Series platform provide flexibility for users to leverage the CPU cores for different services and/or CEF/IPSec performances. The Cisco Catalyst 8500L Series platform are equipped with 12 CPU cores and have the flexibility to allocate cores into the service plane from the data plane. The core allocation is based on the customer configuration of the different services available on these platforms.

From Cisco IOS XE Release 17.4 onwards, you can use the **platform resource { service-plane-heavy | data-plane-heavy }** command to adjust the cores across service plane and data plane. However, you have to reboot the device for the configured profile to take effect.

```
Router(config)# platform resource { service-plane-heavy | data-plane-heavy }
```



Note By default, when a device boots up, the mode is service-plane-heavy.

The following show command output shows the CPU cores allocation for the data plane:

```
Router# show platform software cpu allocation
CPU alloc information:

Control plane cpu alloc: 0-1,12-13

Data plane cpu alloc: 2-11

Service plane cpu alloc: 0

Template used: CLI-data_plane_heavy
```



Note In the above example, the maximum data plane core allocation is 12.

The following show command output shows the CPU cores allocation for the service plane:

```
Router# show platform software cpu allocation

CPU alloc information:
Control plane cpu alloc: 0-1,12-13

Data plane cpu alloc: 6-11

Service plane cpu alloc: 2-5,14-17

Template used: CLI-service_plane_heavy
```

Filtering the Output of the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

show *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol
FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Disabling Front-Panel USB Ports

SUMMARY STEPS

1. enable
2. configure terminal
3. platform usb disable
4. end
5. write memory

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	platform usb disable Example: Device # platform usb disable	Disables USB ports. Note For re-enabling of front-panel usb ports, use the no form of command (no platform usb disable).
Step 4	end Example: Device(config-router-af) # end	Exits address family configuration mode and returns to privileged EXEC mode.
Step 5	write memory	Save to configuration.

Configuration Examples for Disabling of Front-Panel USB Ports

Example: Disabling Front-Panel USB Ports On Autonomous, Controller and vManage Mode

The following example shows the configuration of disabling front-panel USB ports on autonomous, controller and vManage mode:

```
13RU#sh run | inc usb
platform usb disable
13RU#
```

Verifying Disabling of Front Panel USB Ports

To verify the disabling of USB ports on your device, use the following show command:

show platform usb status

```
Router#show platform usb status
USB enabled
Router#
```

Powering Off a Router

Before you turn off a power supply, make certain the chassis is grounded and you perform a soft shutdown on the power supply. Not performing a soft shutdown will often not harm the router, but may cause problems in certain scenarios.

To perform a soft shutdown before powering off the router, enter the **reload** command to halt the system and then wait for ROM Monitor to execute before proceeding to the next step.

The following screenshot shows an example of this process:

```
Router# reload
Proceed with reload? [confirm]
...(Some messages are omitted here)
Initializing Hardware...
Calculating the ROMMON CRC...CRC is correct.
```

Place the power supply switch in the Off position after seeing this message.

Finding Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or the software release notes.

Using the Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Using the Software Advisor

To see if a feature is supported by a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com at <http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl>.

You must be a registered user on Cisco.com to access this tool.

Using the Software Release Notes

Cisco IOS XE software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- New feature information
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. Refer to Cisco Feature Navigator for cumulative feature information.



CHAPTER 8

Bay Configuration

- [Bay Configuration C8500-12X4QC, on page 57](#)
- [Breakout Support, on page 63](#)
- [Bay Configuration C8500-12X, on page 65](#)
- [Bay Configuration C8500-20X6C, on page 65](#)

Bay Configuration C8500-12X4QC

On C8500-12X4QC there are three built-in EPAs that are configurable.

The following table describes the port details:

Bay Number	EPA	Port Configuration	Interface numbers
Bay 0 8xSFP+	1/10G EPA	Eight 1/10G interfaces - TE0 - TE7 Disabled when 100G port in used in Bay 1	0/0/0 0/0/1 0/0/2 0/0/3 0/0/4 0/0/5 0/0/6 0/0/7 0/0/8

Bay Number	EPA	Port Configuration	Interface numbers
Bay 1 4xSFP+/1xQSFP	1/10/40/100G EPA	Four 1/10G interfaces active - TE0 - TE3 (interfaces 0/1/0 ... 0/1/3) The bay can be used in the following modes: <ul style="list-style-type: none"> • Four 1/10G interfaces • One 40G interface active • One 100G interface. This utilizes the eight 1/10G ports of Bay 0 	0/1/0 0/1/1 0/1/2 0/1/3
Bay 2 3xQSFP	40/100G EPA	Three 40G interfaces (0/1/0 to 0/1/2) One 100G interface (0/0/0) (0/0/0)	0/0/0 0/1/0 0/1/1 0/1/2



Note The speed of a 10G interface can be 1G or 10G based on the SFP transceiver plugged into to the port. Even when the speed changes the interface name is still indicated as TenGigabitEthernet.

By default, C8500-12X4QC operates Bay 1 in 10G mode and Bay 2 in 40G mode. The Bay 1 mode can be changed from 10G to 40G to 100G and vice versa. But if Bay 1 is set to 100G, all ports of Bay 0 move to *admin down* state and the ports are no longer functional.

The Bay 2 mode can be changed from 40G to 100G and vice versa. The mode change on Bay 2 does not impact traffic on Bay 1.

Use the **show platform** and **show ip interface** commands to view the bay and interface details:

Router#show platform

Chassis type: C8500-12X4QC

Slot	Type	State	Insert time (ago)
0	C8500-12X4QC	ok	1w3d
0/0	BUILTIN-8x1/10G	ok	1w3d
0/1	BUILTIN-100/40/4x10G	ok	00:04:53
0/2	BUILTIN-100G/3X40G	ok	00:08:16
R0	C8500-12X4QC	ok	1w3d
R0/0		ok, active	1w3d
R0/1		ok, standby	1w3d
F0	C8500-12X4QC	ok, active	1w3d
P0	AIR-AC-750W-R	ok	1w3d
P1	AIR-AC-750W-R	ps, fail	1w3d

```

P2          C8500-FAN-1R          ok          1w3d

Slot        CPLD Version          Firmware Version
-----
0           19020715              12.2 (20181120:104547) [user-gd_secur...
R0           19020715              12.2 (20181120:104547) [user-gd_secur...
F0           19020715              12.2 (20181120:104547) [user-gd_secur...

Router#show ip interface
Te0/0/0          unassigned        YES NVRAM    down          down
Te0/0/1          unassigned        YES NVRAM    down          down
Te0/0/2          unassigned        YES NVRAM    down          down
Te0/0/3          unassigned        YES NVRAM    down          down
Te0/0/4          unassigned        YES NVRAM    down          down
Te0/0/5          unassigned        YES NVRAM    down          down
Te0/0/6          unassigned        YES NVRAM    down          down
Te0/0/7          unassigned        YES NVRAM    down          down
Te0/1/0          unassigned        YES NVRAM    down          down
Te0/1/1          unassigned        YES NVRAM    down          down
Te0/1/2          unassigned        YES NVRAM    down          down
Te0/1/3          unassigned        YES NVRAM    down          down
Fo0/2/0          unassigned        YES unset   down          down
Fo0/2/4          unassigned        YES unset   down          down
Fo0/2/8          unassigned        YES unset   down          down
GigabitEthernet0 10.104.33.213 YES NVRAM    up            up
Router#

```

Bay Configuration Examples

The following examples show how mode can be changed on C8500-12X4QC to achieve different traffic speeds:

Examples

The following example shows how to change to 40G mode on Bay 1 of C8500-12X4QC:

```

Router(config)# hw-module subslot 0/1 mode 40G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
*Oct 29 17:58:10.020 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 17:58:10.028 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.028 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.028 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/0 moved to
default config
*Oct 29 17:58:10.028 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 1 would be lost
*Oct 29 17:58:10.035 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.036 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.036 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/1 moved to
default config
*Oct 29 17:58:10.036 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 2 would be lost

```

```
*Oct 29 17:58:10.043 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.043 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.043 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/2 moved to
default config
*Oct 29 17:58:10.043 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 3 would be lost
*Oct 29 17:58:10.050 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.050 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 17:58:10.050 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/3 moved to
default config
*Oct 29 17:58:11.050 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from 10G
to 40G! system_configured TRUE
*Oct 29 17:58:11.057 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
on subslot 0/1
*Oct 29 17:58:11.057 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 10G mode to 40G mode
*Oct 29 17:58:11.057 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 17:58:11.058 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 1 would be lost
*Oct 29 17:58:11.059 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 2 would be lost
*Oct 29 17:58:11.059 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 3 would be lost
*Oct 29 17:58:11.060 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 17:58:11.061 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
subslot 0/1
*Oct 29 17:58:16.297 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 1
*Oct 29 17:58:16.298 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum number
of XCVR = 1
```

The following example shows how to change to 40G mode to 100G on Bay 1 of C8500-12X4QC:

```
Router(config)# hw-module subslot 0/1 mode 100G
Changing mode of subslot 0/1 to 100G will cause EPA in subslot 0/0 to go offline
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Oct 29 18:09:01.360 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 18:09:01.368 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:01.368 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
*Oct 29 18:09:01.368 IST: BUILTIN-100/40/4x10G[0/1] : FortyGigabitEthernet0/1/0 moved to
default config
*Oct 29 18:09:02.368 IST: BUILTIN-8x1/10G[0/0] : config for spa port 0 would be lost
*Oct 29 18:09:02.375 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.376 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.376 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/0 moved to default
config
*Oct 29 18:09:02.376 IST: BUILTIN-8x1/10G[0/0] : config for spa port 1 would be lost
*Oct 29 18:09:02.382 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.382 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
```



```
*Oct 29 18:09:02.382 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/1 moved to default
config
*Oct 29 18:09:02.382 IST: BUILTIN-8x1/10G[0/0] : config for spa port 2 would be lost
*Oct 29 18:09:02.389 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.389 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.389 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/2 moved to default
config
*Oct 29 18:09:02.389 IST: BUILTIN-8x1/10G[0/0] : config for spa port 3 would be lost
*Oct 29 18:09:02.395 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.395 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.395 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/3 moved to default
config
*Oct 29 18:09:02.395 IST: BUILTIN-8x1/10G[0/0] : config for spa port 4 would be lost
*Oct 29 18:09:02.402 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.402 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.402 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/4 moved to default
config
*Oct 29 18:09:02.402 IST: BUILTIN-8x1/10G[0/0] : config for spa port 5 would be lost
*Oct 29 18:09:02.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.409 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/5 moved to default
config
*Oct 29 18:09:02.409 IST: BUILTIN-8x1/10G[0/0] : config for spa port 6 would be lost
*Oct 29 18:09:02.415 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.415 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.415 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/6 moved to default
config
*Oct 29 18:09:02.415 IST: BUILTIN-8x1/10G[0/0] : config for spa port 7 would be lost
*Oct 29 18:09:02.422 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.422 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:09:02.422 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/7 moved to default
config
*Oct 29 18:09:03.423 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from 40G
to 100G! system_configured TRUE
*Oct 29 18:09:03.433 IST: BUILTIN-8x1/10G[0/0] : config for spa port 0 would be lost
*Oct 29 18:09:03.434 IST: BUILTIN-8x1/10G[0/0] : config for spa port 1 would be lost
*Oct 29 18:09:03.435 IST: BUILTIN-8x1/10G[0/0] : config for spa port 2 would be lost
*Oct 29 18:09:03.435 IST: BUILTIN-8x1/10G[0/0] : config for spa port 3 would be lost
*Oct 29 18:09:03.436 IST: BUILTIN-8x1/10G[0/0] : config for spa port 4 would be lost
*Oct 29 18:09:03.437 IST: BUILTIN-8x1/10G[0/0] : config for spa port 5 would be lost
*Oct 29 18:09:03.437 IST: BUILTIN-8x1/10G[0/0] : config for spa port 6 would be lost
*Oct 29 18:09:03.438 IST: BUILTIN-8x1/10G[0/0] : config for spa port 7 would be lost
*Oct 29 18:09:03.439 IST: BUILTIN-8x1/10G[0/0] : Old mode cleanup done!
*Oct 29 18:09:03.440 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-8x1/10G) offline in subslot
0/0
*Oct 29 18:09:03.445 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
on subslot 0/1
*Oct 29 18:09:03.445 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 40G mode to 100G mode
*Oct 29 18:09:03.445 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 18:09:03.446 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 18:09:03.446 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
subslot 0/1
```

```
*Oct 29 18:09:08.790 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 1
*Oct 29 18:09:08.792 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum number
of XCVR = 1
Router(config)#
*Oct 29 18:09:15.552 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100/40/4x10G) online in subslot
0/1
```

The following example shows how to change to 10G mode from 100G on Bay 1 of C8500-12X4QC:

```
Router(config)# hw-module subslot 0/1 mode 10G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]
*Oct 29 18:14:36.484 IST: %PLATFORM_SCC-1-AUTHENTICATION_FAIL: Chassis authentication failed

*Oct 29 18:14:38.219 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 18:14:38.227 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:14:38.227 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:14:38.227 IST: BUILTIN-100/40/4x10G[0/1] : HundredGigE0/1/0 moved to default
config
*Oct 29 18:14:39.228 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from
100G to 10G! system_configured TRUE
*Oct 29 18:14:39.230 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
on subslot 0/1
*Oct 29 18:14:39.230 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 100G mode to 10G mode
*Oct 29 18:14:39.230 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be lost
*Oct 29 18:14:39.231 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 18:14:39.232 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
subslot 0/1
*Oct 29 18:14:44.472 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 4
*Oct 29 18:14:44.475 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum number
of XCVR = 4
*Oct 29 18:15:03.336 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100/40/4x10G) online in subslot
0/1
```

The following example shows how to change to 100G mode from 100G on Bay 2 of C8500-12X4QC:

```
Router(config)# hw-module subslot 0/2 mode 100G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Oct 29 18:17:03.394 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 0 would be lost
*Oct 29 18:17:03.401 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:17:03.401 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:17:03.401 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/0 moved to
default config
*Oct 29 18:17:03.401 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 1 would be lost
*Oct 29 18:17:03.406 IST: BUILTIN-100G/3X40G[0/2] : Breakout XCVR type QSFP 4X10G AC7M (546)
is not allowed as XCVR port FortyGigabitEthernet0/2/0 is not configured in breakout
*Oct 29 18:17:03.406 IST: %IOSXE_EPA-3-XCVR_PROHIBIT: Transceiver is prohibited to come
online for interface FortyGigabitEthernet
*Oct 29 18:17:03.407 IST: BUILTIN-100G/3X40G[0/2] : XCVR prohibited on port
FortyGigabitEthernet0/2/0, epa_name=BUILTIN-100G/3=FortyGigabitEthernet0/2/0,
xcvr_speed=400000000, admin_state=UNSHUT xcvr_type=546

*Oct 29 18:17:03.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:17:03.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
```

```

console as console
*Oct 29 18:17:03.409 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/4 moved to
default config
*Oct 29 18:17:03.409 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 2 would be lost
*Oct 29 18:17:03.417 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:17:03.417 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
console as console
*Oct 29 18:17:03.417 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/8 moved to
default config
*Oct 29 18:17:03.423 IST: BUILTIN-100G/3X40G[0/2] : Breakout XCVR type QSFP 4SFP10G CU4M
(541) is not allowed as XCVR port Forhernet0/2/4 is not configured in breakout
*Oct 29 18:17:03.423 IST: %IOSXE_EPA-3-XCVR_PROHIBIT: Transceiver is prohibited to come
online for interface FortyGigabitEther
*Oct 29 18:17:03.423 IST: BUILTIN-100G/3X40G[0/2] : XCVR prohibited on port
FortyGigabitEthernet0/2/4, epa_name=BUILTIN-100G/3=FortyGigabitEthernet0/2/4,
xcvr_speed=40000000, admin_state=UNSHUT xcvr_type=541

*Oct 29 18:17:04.418 IST: BUILTIN-100G/3X40G[0/2] : Received mode change request from 40G
to 100G! system_configured TRUE
*Oct 29 18:17:04.423 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100G/3X40G) reloaded on
subslot 0/2
*Oct 29 18:17:04.423 IST: BUILTIN-100G/3X40G[0/2] : EPA moving from 40G mode to 100G mode
*Oct 29 18:17:04.423 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 0 would be lost
*Oct 29 18:17:04.424 IST: BUILTIN-100G/3X40G[0/2]: config for spa port 1 would be lost
*Oct 29 18:17:04.425 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 2 would be lost
*Oct 29 18:17:04.425 IST: BUILTIN-100G/3X40G[0/2] : Old mode cleanup done!
*Oct 29 18:17:04.426 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100G/3X40G) offline in subslot
0/2
*Oct 29 18:17:09.685 IST: BUILTIN-100G/3X40G[0/2] : Number of ports 1
*Oct 29 18:17:09.686 IST: BUILTIN-100G/3X40G[0/2] : XCVR namestring create: Maximum number
of XCVR = 1
Router(config)#
Router(config)#
*Oct 29 18:17:16.017 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100G/3X40G) online in subslot
0/2

```

Breakout Support

Understand Breakout Support

Breakout support for a port helps to split a higher density port to multiple independent and logical ports. Starting from Cisco IOS XE 17.4, breakout support is introduced in Bay 2 of C8500-12X4QC that supports breakout capable 40G native ports. The breakout support is of 4X10G and uses a 3-tuple approach.



Note Breakout support is only supported on C8500-12X4QC (not C8500-20X6C).

The following table explains the interface names when breakout is configured:

Table 11: Interface Names when Breakout is Configured

Sr. No	Interface names	Description
	Te0/2/0, Te0/2/1, Te0/2/2, Te0/2/3, Te0/2/4, Te0/2/5, Te0/2/6, Te0/2/7, Te0/2/8, Te0/2/9, Te0/2/10, Te0/2/11	All three 40 G native ports working in 10G breakout mode
	Fo0/2/0, Fo0/2/4, Te0/2/8, Te0/2/9, Te0/2/10, Te0/2/11	1st native port in 40G mode 2nd native port in 40G mode 3rd native port in 10G breakout mode
	Fo0/2/0, Te0/2/4, Te0/2/5, Te0/2/6, Te0/2/7, Fo0/2/8	1st native port in 40G mode 2nd native port 10G breakout mode 3rd native port in 40G mode
	Te0/2/0, Te0/2/1, Te0/2/2, Te0/2/3, Fo0/2/4, Fo0/2/8	1st native port in 10G breakout mode 2nd native port in 40G mode 3rd native port in 40G mode
	1st native port in 10G breakout mode 2nd native port in 40G mode 3rd native port in 40G mode	1st native port in 40G mode 2nd native port in 10G breakout mode 3rd native port in 10G breakout mode
	Te0/2/0, Te0/2/1, Te0/2/2, Te0/2/3, Te0/2/4, Te0/2/5, Te0/2/6, Te0/2/7, Fo0/2/8	1st native port in 10G breakout mode 2nd native port in 10G breakout mode 3rd native port in 40G mode
	Te0/2/0, Te0/2/1, Te0/2/2, Te0/2/3, Fo0/2/4, Te0/2/8, Te0/2/9, Te0/2/10, Te0/2/11	1st native port in 10G breakout mode 2nd native port in 40G mode 3rd native port in 10G breakout mode

Breakout Support



Note Before using the breakout capability, ensure that Bay 2 is configured in 40G mode

```
Router(config)#hw-module subslot 0/2 breakout 10G port ?  
  
all                configure all native ports in breakout mode  
native_port_0      configure native port 0 in breakout mode  
native_port_4      configure native port 4 in breakout mode  
native_port_8      configure native port 8 in breakout mode
```

Sample Commands to Configure Breakout Support

When native_port 0 and 8 are in 10G breakout and native_port 4 is running in 40G mode

```
hw-module subslot 0/2 breakout 10g port native_port_0  
hw-module subslot 0/2 breakout 10g port native_port_8
```

When all three native 40G ports have same breakout config

```
hw-module subslot 0/2 breakout 10g port all  
hw-module subslot 0/2 breakout none port all
```

When you want to remove breakout configuration from all ports

```
hw-module subslot 0/2 breakout none port all
```

Bay Configuration C8500-12X

On C8500-12X4 there is one built-in EPA that supports ports TE0 - TE11 for SFP/SFP+ transceivers.

Bay Configuration C8500-20X6C

On C8500-20X6C there are two built-in EPAs that are configurable.

Bay Number	EPA	Port Configuration	Interface numbers
Bay 0 20xSFP+	1/10G EPA	Twenty 1G interfaces Twenty 10G interfaces Twenty 1/10G interfaces	0/0/0 0/0/1 0/0/2 0/0/3 0/0/4 0/0/5 0/0/6 0/0/7 0/0/8 0/0/9 0/0/10 0/0/11 0/0/12 0/0/13 0/0/14 0/0/15 0/0/16 0/0/17 0/0/18 0/0/19
Bay 1 6xQSFP+	40/100G EPA	Six 40/100G interfaces active The bay can be used in the following modes: <ul style="list-style-type: none"> • Six 40G interfaces • Six 100G interfaces • Six 40/100G interfaces 	0/1/0 0/1/1 0/1/2 0/1/3 0/1/4 0/1/5



CHAPTER 9

Licenses and Licensing Models

This chapter provides information about the licenses that are available on Cisco Catalyst 8000 Edge Platforms Family, supported throughput options, and how to configure the available licenses and throughput. It also outlines the licensing models available on Cisco Catalyst 8000 Edge Platforms Family.



Note The information in this chapter applies predominantly to a device operating in the autonomous mode. References to the controller mode are included in certain sections for the sake of comparison and completeness. Where the information applies to controller mode, this has been called-out categorically.

For a more detailed overview on Cisco Licensing, go to <https://cisco.com/go/licensingguide>.

This chapter includes the following major sections:

- [Feature Information for Available Licenses and Licensing Models](#), on page 67
- [Available Licenses](#) , on page 69
- [Throughput](#) , on page 74
- [How to Configure Available Licenses and Throughput](#) , on page 88
- [Available Licensing Models](#), on page 103

Feature Information for Available Licenses and Licensing Models

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for Available Licenses and Licensing Models

Feature Name	Releases	Feature Information
Aggregate Throughput Throttling - Virtual Platforms	Cisco IOS XE Cupertino 17.9.1a	<p>On virtual platforms of the Cisco Catalyst 8000 Edge Platforms Family, <i>for all throughput levels</i>, when you configure a bidirectional throughput value on the device, aggregate throughput throttling is effective.</p> <p>This enhancement does not change the throttling behaviour that has always been applicable to virtual platforms: any throttling applies only to data that is transmitted (Tx). Data that is received (Rx) is unthrottled.</p> <p>See Throughput , on page 74, Throughput as a Numeric Value , on page 76, and Throughput as a Tier, on page 82.</p>
Aggregate Throughput Throttling - Physical Platforms	Cisco IOS XE Cupertino 17.8.1a	<p>On the <i>physical</i> platforms of Cisco Catalyst 8000 Edge Platforms Family, for throughput levels greater than 250 Mbps and Tier 2 and higher tiers, when you configure the bidirectional throughput value on the device, aggregate throughput throttling is effective. This means that traffic is throttled in an aggregate manner irrespective of the distribution of the traffic in the upstream and downstream direction.</p> <p>The bidirectional throughput is represented in the license PID (For example, DNA-C-500M-E-3Y and DNA-C-T2-E-3Y). The aggregate throughput is double the bidirectional throughput.</p> <p>See Throughput as a Numeric Value , on page 76 and Throughput as a Tier, on page 82.</p>
Tier-Based Licenses	Cisco IOS XE Cupertino 17.7.1a	<p>Support for tier-based throughput configuration was introduced in addition to existing bandwidth-based (numeric) throughput configuration.</p> <p>Starting with the lowest throughput level, the available tiers are Tier 0 (T0), Tier 1 (T1), Tier 2 (T2), and Tier3 (T3). Each tier represents a throughput level.</p> <p>If the license PID for a product is tier-based, the license is displayed with the tier value in the CSSM Web UI.</p> <p>For a product with a tier-based license, you can <i>configure</i> a tier-based throughput value, and you can also <i>convert</i> to a tier-based throughput value.</p>

Feature Name	Releases	Feature Information
Cisco Digital Network Architecture (DNA) licenses	Cisco IOS XE Amsterdam 17.3.2	Support for Cisco DNA licenses was introduced on Cisco Catalyst 8000 Edge Platforms Family. Cisco DNA Licenses are categorised into network-stack licenses and a DNA-stack add-on licenses.
High Security License (HSECK9)	Cisco IOS XE Amsterdam 17.3.2	Support for the HSECK9 license was introduced on Cisco Catalyst 8000 Edge Platforms Family.
Cisco Unified Border Element license (Cisco UBE license) Cisco Unified Communications Manager Express license (Cisco Unified CME license) Cisco Unified Survivable Remote Site Telephony license (Cisco Unified SRST license)	Cisco IOS XE Amsterdam 17.3.2	Support for Cisco UBE, Cisco Unified CME, Cisco Unified SRST licenses was introduced on Cisco Catalyst 8000 Edge Platforms Family

Available Licenses

This section lists all the licenses that are available on Cisco Catalyst 8000 Edge Platforms Family, usage guidelines, and ordering considerations.

Cisco DNA License

A Cisco Digital Network Architecture (DNA) software license combines several feature-specific licenses.



Note A Cisco DNA license includes all feature licenses except the following: High Security (HSECK9), Cisco Unified Border Element (Cisco UBE), Cisco Unified Communications Manager Express (Cisco Unified CME), and Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST). See [Ordering Considerations for a Cisco DNA License, on page 71](#).

Cisco DNA licenses are categorized into network-stack licenses and DNA-stack add-on licenses.

Cisco DNA Licenses Available on Catalyst 8000V Edge Software, Catalyst 8200, and 8300 Series Edge Platforms:

Network-stack licenses:

- Network Essentials
- Network Advantage: includes features available with Network Essentials, and more.

- Network Premier: includes features available Network Essentials, Network Advantage, and more.

DNA-stack add-on licenses:

- Cisco DNA Essentials: add-on license available only with Network Essentials.
- Cisco DNA Advantage: add-on license available only with Network Advantage. Includes features available with DNA Essentials and more.
- Cisco DNA Premier: add-on license available only with Network Premier. Includes features available with DNA Essentials, DNA Advantage and more.

Cisco DNA Licenses Available on Catalyst 8500 Series Edge Platforms:

Network-stack licenses:

- Network Advantage
- Network Premier: includes features available Network Advantage, and more.

DNA-stack add-on licenses:

- Cisco DNA Advantage
- Cisco DNA Premier: add-on license available only with Network Premier. Includes features available with DNA Advantage and more.

Guidelines for Using a Cisco DNA License

- Guidelines that apply to all platforms in the Cisco Catalyst 8000 Edge Platforms Family:
 - A network-stack license is a perpetual or permanent license and has no expiration date.
 - A DNA-stack add-on license is a subscription or term license and is valid only until a certain date. A 3-year and 5-year option is available for all DNA-stack add-on licenses. A 7-year subscription option is available for certain DNA-stack add-on licenses.
 - If you order a Cisco DNA license when purchasing new hardware, the license is not preconfigured on the device. You must configure the boot level license and then the throughput, on the device.
 - If you configure tier-based throughput, which is supported from Cisco IOS XE Cupertino 17.7.1a, Tier 3 (T3) is not supported with the Network Essentials and DNA Essentials licenses.

This means, to configure T3 (throughput greater than or equal to 2.5 G), you must configure Network Advantage/ DNA Advantage, or Network Premier/DNA Premier as the boot level license.

This also means that if you have configured T3 as the throughput, you cannot change the boot level license to Network Essentials and DNA Essentials.

- Guidelines that apply only to Catalyst 8000V Edge Software:

On Catalyst 8000V Edge Software, when you configure a network-stack license, you must also configure the corresponding DNA-stack add-on license.
- Guidelines that apply only to Catalyst 8200, 8300, 8500 Series Edge Platforms:

- The DNA-stack add-on license that is available with each network-stack license is optional. You can configure a network-stack license without a DNA-stack add-on license, but you cannot configure DNA-stack add-on license without the corresponding network-stack license.
- If you use a DNA-stack add-on license, renew the license before term expiry to continue using it, or deactivate the DNA-stack add-on license and then reload the device to continue operating with the network-stack license capabilities.

Ordering Considerations for a Cisco DNA License

A Cisco DNA license subsumes all performance, boost, and technology package licenses (securityk9, uck9, and appxk9). This means that when you order a Cisco DNA network-stack license, or a Cisco DNA-stack add-on license, if a performance, boost, and technology package license is required or applicable, it is automatically added to the order.

The license Product ID (PID) you purchase can only be a DNA-stack add-on license PID.

The license PID also indicates the throughput you are entitled to. The throughput may be represented by a numeric value or a tier. For example:

- DNA-C-**10M**-E-3Y, is a license PID where the throughput is represented by a numeric value. The **10M** means that you are entitled to 10 Mbps bidirectional throughput.

For more information about a numeric throughput value and related concepts, see sections [Throughput](#) , on page 74 and [Throughput as a Numeric Value](#) , on page 76.

- DNA-C-**T0**-E-3Y, is a license PID where the throughput is represented by a tier value. The **T0** means that you are entitled to up to 15 Mbps bidirectional throughput.

For more information about a tier-based throughput value and related concepts, see sections [Throughput](#) , on page 74 and [Throughput as a Tier](#), on page 82.

If the throughput you order is greater than 250 Mbps, or Tier 2 or a higher tier, an HSECK9 license is *required*. See [High Security License](#) , on page 71.



Note

When you purchase a license PID with a tier-based throughput value of *T1*, an HSECK9 license is automatically provided. However, the maximum throughput on the device is still throttled to 250 Mbps *in each direction*.

High Security License

The High Security license (HSECK9 license) is an export-controlled license. An export-controlled license is restricted by U.S. export control laws.

This license is required for the use of full cryptographic functionality, that is, throughput greater than 250 Mbps (Tier 2 and higher tiers), and tunnel count over and above a certain number (the number varies depending on the platform).



Note

The term "throughput" refers to encrypted throughput on physical platforms. On virtual platforms, it refers to encrypted *and* unencrypted throughput - combined.

Without an HSECK9 license, the supported tunnel count and the supported throughput for the various models of the Cisco Catalyst 8000 Edge Platforms Family is as follows:

PID	No. Of Tunnels <i>Without</i> HSECK9 License	Supported Throughput <i>Without</i> HSECK9 License
C8500-12X	N/A	N/A
C8500-12X4QC	N/A	N/A
C8500L-8G4X	N/A	N/A
C8300-2N2S-4T2X	1000	T0, T1
C8300-2N2S-6T	1000	T0, T1
C8300-1N1S-4T2X	1000	T0, T1
C8300-1N1S-6T	1000	T0, T1
C8200-1B-4T	1000	T0, T1
C8200L-1N-4T	1000	T0, T1
C8000V	150	T0, T1



Note By using an HSECK9 license the tunnel count restriction is lifted and you can configure throughput greater than 250 Mbps. For detailed information about the available throughput options, see [Throughput and System Hardware Throttling Specifications in the Autonomous Mode, on page 77](#) and [Numeric and Tier Mapping](#).

To know if an HSECK9 license is being used on a device, enter the **show license summary** command in privileged EXEC mode. On all devices in the Cisco Catalyst 8000 Edge Platforms Family, the HSECK9 license is displayed as: Router US Export Lic. for DNA (DNA_HSEC). For example:

```
Device# show license summary
```

```
Account Information:
```

```
Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
```

```
Virtual Account: Eg-VA
```

```
License Usage:
```

License	Entitlement Tag	Count	Status
network-advantage_T2	(NWSTACK_T2_A)	1	IN USE
dna-advantage_T2	(DSTACK_T2_A)	1	IN USE
Router US Export Lic...	(DNA_HSEC)	1	IN USE

Guidelines for Using an HSECK9 License

The HSECK9 license is tied to the chassis. Therefore, one HSECK9 license is required for each chassis UDI where you want to use cryptographic functionality.

An HSECK9 license requires authorization before use. This authorization is provided by a Smart Licensing Authorization Code (SLAC), which you must install on the device. You must install a SLAC for each HSECK9 license you use. A SLAC is generated in and obtained from CSSM. How you obtain SLAC from CSSM

depends on the topology you have implemented. For more information, see [Installing SLAC for an HSECK9 License, on page 91](#).

Once SLAC is installed, enter the **show license authorization** command in privileged exec mode, to confirm. If SLAC is installed, the status field displays: SMART AUTHORIZATION INSTALLED on <timestamp>. For example:

```
Device# show license authorization
Overall status:
  Active: PID:C8300-1N1S-4T2X, SN:FDO2250A0J5
        Status: SMART AUTHORIZATION INSTALLED on Dec 03 08:24:35 2021 UTC
        Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X, SN:FDO2250A0J5
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

Ordering Considerations for an HSECK9 License

If you order your DNA licenses in the same configuration as Catalyst 8000 hardware platforms, the option to order an HSECK9 license is available or is selected, if applicable. For example, in case of Catalyst 8500 Series Edge Platforms, when you order hardware, an HSECK9 license is automatically added to the order, because throughput support *starts* at greater than 250 Mbps on these platforms. Further, the requisite SLAC for the HSECK9 license is also factory-installed on the device.

If you order your DNA licenses in a configuration that is separate from your Catalyst 8000 hardware platforms, you must order the HSECK9 license in the configuration for the Catalyst 8000 hardware platforms, if required.

If you plan to use an HSECK9 license with new hardware that you are ordering, provide your Smart Account and Virtual Account information *with* the hardware order. This enables Cisco to factory-install SLAC for the HSECK9 license on the hardware. You must still configure throughput on the device before you start using it.



Note If the HSECK9 license is ordered separately (not with the hardware order), SLAC cannot be factory-installed.

Cisco CUBE License

A Cisco Unified Border Element License (Cisco UBE license) does not require any boot level configuration before you enable it. After purchase, you can refer to the configuration guide to configure the available Cisco UBE features.

For information about the features available with a Cisco UBE license, see the *Cisco Unified Border Element Configuration Guide* for the required release at: <https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html>.

For information about supported platforms and about purchasing a Cisco UBE license, see the datasheet at: <https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-border-element/data-sheet-c78-729692.html>. You must order a Cisco UBE license separately if required. It is not automatically included with any other license.

For information about how to report usage of a Cisco UBE license, see [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#). In the context of this licensing model, a Cisco UBE license is an *unenforced* license.

Cisco Unified CME License

A Cisco Unified Communications Manager Express License (Cisco Unified CME license) does not require any boot level configuration before you enable it. After purchase, you can refer to the configuration guide to configure the available Cisco UBE features.

For information about the features available with a Cisco Unified CME license, see the [Cisco Unified Communications Manager Express System Administrator Guide](#).

For information about supported platforms and about purchasing a Cisco Unified CME license, see the datasheet at:

<https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html>.

You must order a Cisco Unified CME license separately if required. It is not automatically included with any other license.

For information about how to report usage of a Cisco Unified CME license, see [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#). In the context of this licensing model, a Cisco UBE license is an *unenforced* license.

Cisco Unified SRST License

A Cisco Unified Survivable Remote Site Telephony License (Cisco Unified SRST license) does not require any boot level configuration before you enable it. After purchase, you can refer to the configuration guide to configure the available Unified SRST features.

For information about the features available with a Cisco Unified SRST license, see the [Cisco Unified SCCP and SIP SRST System Administrator Guide \(All Versions\)](#).

For information about supported platforms and about purchasing a Cisco Unified SRST license, see the datasheet at:

<https://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html>.

You must order a Cisco Unified SRST license separately if required. It is not automatically included with any other license.

For information about how to report usage of a Unified SRST license, see [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#). In the context of this licensing model, a Unified SRST license is an *unenforced* license.

Throughput

The *throughput* tells you how much data is allowed to be transferred on the device. You can configure this value in the autonomous mode. Data is then transmitted (Tx) and received (Rx) at the configured rate.

If you don't explicitly configure a throughput, default throughput is effective.

Encrypted and Unencrypted Throughput

Encrypted throughput, also known as crypto throughput, is throughput that is protected by a cryptographic algorithm.

Unencrypted throughput on the other hand, is in plain text. Unencrypted throughput is also referred to as Cisco Express Forwarding (CEF) traffic.



Important

In case of physical platforms (Catalyst 8200, 8300, and 8500 Series Edge Platforms), all references to “throughput” in this document refer only to cryptographic throughput.

In case of virtual platforms (Catalyst 8000V Edge Software), all references to “throughput” in this document refer to both, encrypted and unencrypted throughput.

Throttled and Unthrottled Throughput

Throttled throughput refers to the enforcement of a restriction on the throughput.

Unthrottled throughput means no limit is enforced, and the device throughput is at the maximum capability of the device.

Whether throughput will be throttled or not, is determined by the throughput value you configure, and if the system’s hardware is designed to impose a throttling limit for that configured throughput level. For more information about this, see [Throughput and System Hardware Throttling Specifications in the Autonomous Mode, on page 77](#) in this document.

Depending on whether the device is a physical or a virtual one, throttling is also applied differently. On virtual platforms, if throughput is throttled, throttling applies only to Tx data and not Rx data. On physical platforms, if throughput is throttled, throttling applies to Tx and Rx data.



Note

On physical platforms (Catalyst 8200, 8300, and 8500 Series Edge Platforms), unencrypted throughput (Tx and Rx), is unthrottled by default.

Where to Find Throughput Information for a Device

The throughput you are entitled to, is a value that is represented in the License product ID (PID) when you order a Cisco DNA license. It can be a numeric throughput value, such as DNA-C-**10M**-E-3Y, or a tier-based throughput value, such as DNA-C-**T0**-E-3Y.

To display current throughput configuration on the device:

- For physical platforms enter the **show platform hardware throughput crypto** privileged EXEC command.
- For virtual platforms enter the **show platform hardware throughput level** privileged EXEC command.

Depending on whether your license PID has a numeric throughput value, or tier-based throughput value, refer to the corresponding section below for further details.

Throughput as a Numeric Value

This refers to a numeric value (10M, 15M, 250M, 1G, and so on) that is configured as throughput.

The numeric throughput value you are entitled to is in the license PID and it is bi-directional. It is the maximum throughput that is allowed *in each direction* (Tx and Rx). The aggregate throughput is the *sum* of the throughput in both directions and therefore double the bi-directional throughput.

For example, if the license PID is DNA-C-**10M**-E-3Y, 10 Mbps is the bi-directional throughput, and the throughput value you configure on the device. It means that a maximum of 10 Mbps can be transmitted and 10 Mbps can be received. The aggregate throughput available is 20 Mbps.

Starting with Cisco IOS XE Cupertino 17.8.1a, throttling behaviour has changed as follows: *Only on physical platforms, and for throughput levels greater than 250 Mbps*, when you configure a throughput value on the device, aggregate throughput throttling is effective. This means that traffic is throttled in an aggregate manner irrespective of the distribution of Tx and Rx traffic.

Starting with Cisco IOS XE Cupertino 17.9.1a, throttling behaviour has changed as follows: *On virtual platforms, for all throughput levels*, when you configure a bidirectional throughput value on the device, aggregate throughput throttling is effective. This enhancement does not change the throttling behaviour that has always been applicable to virtual platforms: any throttling applies only to Tx data. Rx data is always unthrottled.



Note If the aggregate for the throughput level you configure on a virtual platform is greater than 250 Mbps, aggregate throttling is not effective unless an HSECK9 license is available on the device (that is, SLAC is installed).

• Example: Throttling when throughput is greater than 250 Mbps

Let us suppose that you order license PID DNA-C-**500M**-A-3Y. This means that 500 Mbps is the bi-directional throughput and 1Gbps is the aggregate throughput. The release-wise configuration and behaviour is as follows:

- Until Cisco IOS XE Cupertino 17.7.x, on physical and virtual platforms: If you configure a throughput of 500 Mbps on the device, the maximum Tx throughput available is 500 Mbps and the maximum Rx throughput is 500 Mbps. (Except on virtual platforms, where Rx is not throttled.)
- From Cisco IOS XE Cupertino 17.8.1a:
 - On physical platforms, if you configure a throughput of 500 Mbps on the device, a maximum of 1 Gbps Tx and 0 Mbps Rx, or, 100 Mbps Tx and 900 Mbps Rx or any other ratio within the aggregate 1 Gbps throughput limit, is supported.
 - On virtual platforms, if you configure a throughput of 500 Mbps on the device, a maximum of 500 Mbps Tx throughput is supported. Rx is not throttled.
- From Cisco IOS XE Cupertino 17.9.1a:
 - On physical platforms, throughput throttling behaviour described above (starting with 17.8.1a) continues to apply.
 - On virtual platforms, if you configure a throughput of 500 Mbps on the device, a maximum of 1 Gbps Tx throughput is supported. Rx continues to remain unthrottled.

• Example: Throttling when throughput is equal to or lesser than 250 Mbps

Let us suppose that you order license PID DNA-C-250M-A-3Y. This means that 250 Mbps is the bi-directional throughput, and 500 Mbps is the aggregate throughput. The release-wise configuration and behaviour is as follows:

- Until Cisco IOS XE Cupertino 17.8.x, on physical and virtual platforms: If you configure a throughput of 250 Mbps on the device, the maximum Tx throughput supported is 250 Mbps and the maximum Rx throughput is 250 Mbps - it is not aggregated. (Except on virtual platforms where Rx is not throttled.)



Note On C8200-1N-4T-L, if you configure a numeric value of 250 Mbps, a maximum of 250 Mbps is available in each direction. But if you configure a tier-based value (T2), 500 Mbps is available for use in any Tx and Rx ratio.

- From Cisco IOS XE Cupertino 17.9.1a, *only on virtual platforms*, if you configure a throughput of 250 Mbps on the device, the aggregate amounts to 500 Mbps, which requires an HSECK9 license. If you have installed SLAC for the HSECK9 license, then the maximum Tx throughput available is 500 Mbps. Rx throughput continues to remain unthrottled. By contrast, if you configure a throughput of 100 Mbps on a virtual device, then the maximum Tx throughput available is 200 Mbps. Rx throughput remains unthrottled.

The recommended way to arrive at the required throughput for your network is to first calculate the aggregate throughput (Tx and Rx) and divide that by 2 to arrive at the bidirectional throughput value. Finally, select the license PID that is equal to or greater than the bidirectional throughput (tier-based or numeric).

The tables below provide throughput specifications for all devices in the Cisco Catalyst 8000 Edge Platforms Family:



Note Separate tables are provided for throughput specifications in the autonomous mode and SD-WAN controller mode.

Throughput and System Hardware Throttling Specifications in the Autonomous Mode

- Supported throughputs: All the throughput values you can configure on the device. These are the only throughput values you can configure on the specified device. The column heading also mentions the default throughput for a PID.
- Hardware throttled throughput: The throttling limit imposed by the system's hardware, for a supported throughput level. This column in the tables below tell you if hardware is throttled for each supported throughput level and what that hardware throttled level is. Where the value is listed as unthrottled, it means that throughput is not throttled even if you configure a limit.
- Require HSECK9?: Indicates if a supported throughput level requires an HSECK9 license (anything lesser than or equal to 250 Mbps does not require HSECK9).
- Supported Release & Throughput Throttling Behavior: This column provides a few different details. The applicable release for the specified throttling behaviour, if what is finally available is bi-directional or aggregate, and if the throughput being referred to is encrypted or unencrypted. Note that throughput always refers to encrypted throughput for physical platforms; for for virtual platforms it is both, encrypted and unencrypted.

C8300-1N1S-4T2X						
Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Bi-directional, encrypted
500M	500M	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
1G	1G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
2.5G	unthrottled	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8300-2N2S-6T						
Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Bi-directional; encrypted
500M	500M	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
1G	1G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8300-1N1S-6T						
Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Bi-directional; encrypted
500M	500M	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
1G	1G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8300-2N2S-4T2X

Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Bi-directional; encrypted
500M	500M	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
1G	1G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
2.5G	unthrottled	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8200-1N-4T

Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Bi-directional; encrypted
500M	500M	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8200-1N-4T-L

Supported Throughputs (default 10M)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M, 15M, 25M, 50M, 100M, 250M	250M	No	>= 17.5.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

Note On C8200-1N-4T-L, if you configure a numeric value of 250 Mbps, a maximum of 250 Mbps is available in each direction. But if you configure tier-based value T2 (which requires an HSECK9 license), 500 Mbps is available for use in any Tx and Rx ratio.

C8500-12X40C

Supported Throughputs (default 2.5G)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
2.5G	2.5G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8500-12X40C						
5G	5G	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
10G	unthrottled	Yes	>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8500-12X						
Supported Throughputs (default 2.5G)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
2.5G	2.5G		>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
5G	5G		>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
10G	unthrottled		>= 17.4.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8500L-8S4X						
Supported Throughputs (default 1G)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
1G	1G	Yes	>= 17.5.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
2.5G	2.5G	Yes	>= 17.5.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
5G	5G	Yes	>= 17.5.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted
10G	unthrottled	Yes	>= 17.5.1	Bi-directional; encrypted	>=17.8.1a	Aggregate, encrypted

C8500-20X6C						
Supported Throughputs (default T4)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
T4	50G	Yes	-	-	>=17.8.1a	Aggregate, encrypted
T5	unthrottled	Yes	-	-	>=17.8.1a	Aggregate, encrypted

C8000v						
Supported Throughputs (default)	Hardware Throttled Throughput	Require HSECK9?	Supported Release & Throughput Throttling Behavior		Supported Release & Throughput Throttling Behavior	
10M	10M	No	>= 17.4.1	Bi-directional; encrypted and unencrypted throughput	>=17.9.1a	Aggregate; encrypted and unencrypted throughput
25M	25M	No				
50M	50M	No				
100M	100M	No				
250M	250M	No				
500M	500M	Yes				
1G	1G	Yes				
2.5G	2.5G	Yes				
5G	5G	Yes				
10G	10G	Yes				
Note This is a virtual platform; Rx is always unthrottled.						

Throughput and System Hardware Throttling Specifications in the SD-WAN Controller Mode

PID	Throughput Without HSECK9	Throughput With HSECK9 (>=17.4.1 and <17.8.1a; Bi-directional)	Throughput With HSECK9 (>17.8.1a; Aggregate)
C8300-1N1S-4T2X (default 250M)	250M	unthrottled	unthrottled
C8300-2N2S-6T (default 250M)	250M	1G	2G
C8300-1N1S-6T (default 250M)	250M	1G	2G
C8300-2N2S-4T2X (default 250M)	250M	unthrottled	unthrottled
C8200-1N-4T (default 250M)	250M	500M	1G
C8200-1N-4T-L (default 250M)	250M	250M	500M

PID	Throughput Without HSECK9	Throughput With HSECK9 ($\geq 17.4.1$ and $< 17.8.1a$; Bi-directional)	Throughput With HSECK9 ($> 17.8.1a$; Aggregate)
C8500-12X4QC (default unthrottled)	unthrottled	unthrottled	unthrottled
C8500-12X (default unthrottled)	unthrottled	unthrottled	unthrottled
C8500L-8S4X (default unthrottled)	unthrottled	unthrottled	unthrottled
C8500-20X6C (default T4)	unthrottled	-	unthrottled
C8000v (default 250M)	250M	unthrottled	unthrottled

Throughput as a Tier

Tier-based throughput configuration is supported starting with Cisco IOS XE Cupertino 17.7.1a.

A tier represents a throughput level. Starting with the lowest throughput level, the available tiers are Tier 0 (T0), Tier 1 (T1), Tier 2 (T2), and Tier 3 (T3). T2 and higher tiers require an HSECK9 license.

The tier-based throughput value you are entitled to is in the license PID and it is bi-directional. It is the maximum throughput that is allowed *in each direction* (Tx and Rx). The aggregate throughput is the *sum* of the throughput in both directions and therefore double the bi-directional throughput.

For example, if the license PID is DNA-C-**T0**-A-3Y, T0 is the bi-directional throughput, and the throughput value you configure on the device. When you configure this value, T0 Tx and T0 Rx, is supported. See [table Tier and Numeric Throughput Mapping, on page 83](#) for information about how numeric throughput values are mapped to tiers and the DNA licenses that are available with each tier.

Note the following:

- All tiers are not available with all Cisco DNA licenses. For example, T3 is not available with the Network Essentials and DNA-Essentials licenses. This also means that if you have T3 as the configured throughput, you cannot change the boot level license to Network Essentials and DNA Essentials. The [Tier and Numeric Throughput Mapping, on page 83](#) table clarifies this.
- Different platforms support different maximum throughput levels, therefore each tier means a different value for different platforms. For example, T2 means 1G throughput for C8300-2N2S-4T2, 500M for C8200-1N-4T, and 250M for C8200-1N-4T-L. The [Tier and Numeric Throughput Mapping, on page 83](#) table clarifies this.

Starting with Cisco IOS XE Cupertino 17.8.1a, throttling behaviour has changed as follows: *Only on physical platforms*, and when you configure T2 or higher tiers, aggregate throughput throttling is effective. This means that traffic is throttled in an aggregate manner irrespective of the distribution of Tx and Rx traffic.

Starting with Cisco IOS XE Cupertino 17.9.1a, throttling behaviour has changed as follows: *On virtual platforms*, when you configure a tier (*any tier*), aggregate throughput throttling is effective. This enhancement does not change the throttling behaviour that has always been applicable to virtual platforms: any throttling applies only to Tx data. Rx data is always unthrottled.

• **Example: Throttling when throughput is T2 or a higher tier**

Let us suppose that you order license PID DNA-C-**T2**-A-3Y. With T2, the bi-directional throughput can be upto 1 Gbps and the aggregate throughput can be upto 2 Gbps. The release-wise configuration and behaviour is as follows:

- Until Cisco IOS XE Cupertino 17.7.x, on physical and virtual platforms: You configure T2 on the device, and depending on the device, a maximum of up to 1 Gbps Tx and up to 1 Gbps Rx throughput is supported. Except on virtual platforms where Rx is not throttled.
- From Cisco IOS XE Cupertino 17.8.1a:
On physical platforms if you configure T2, depending on the device, up to 2 Gbps of aggregate throughput is available for use in any Tx and Rx ratio.



Note On C8200-1N-4T-L, if you configure T2, 500 Mbps is available for use in any upstream and downstream ratio. But if you configure a numeric value of 250M, a maximum of 250 Mbps is available in each direction.

On virtual platforms if you configure T2, a maximum of 1 Gbps Tx is supported. Rx is not throttled.

- From Cisco IOS XE Cupertino 17.9.1a:
On physical platforms, the throughput throttling behaviour described above (starting with 17.8.1a) continues to apply.
On virtual platforms, if you configure T2, up to 2 Gbps of aggregate throughput is supported. Accordingly, Tx is throttled at the aggregate level and Rx continues to remain unthrottled.

• **Example: Throttling when throughput is T0 or T1**

Let us suppose that you order license PID DNA-C-**T1**-A-3Y. With T1, 100 Mbps is the bi-directional throughput, 200 Mbps is the aggregate throughput. The release-wise configuration and behaviour is as follows:

- Until Cisco IOS XE Cupertino 17.8.x, on physical and virtual platforms: if you configure a throughput of T1 on the device. A maximum of 100 Mbps Tx and 100 Mbps Rx throughput is available. (Except on virtual platforms where Rx is not throttled).
- From Cisco IOS XE Cupertino 17.9.1a, only on virtual platforms, if you configure a throughput of T1 on the device, Tx is throttled to a maximum of 200 Mbps. Rx continues to remain unthrottled.

Tier and Numeric Throughput Mapping

The following tables provide information about how numeric throughput values are mapped to tiers and the DNA licenses that are available with each tier.



Note When you purchase a license PID with a tier-based throughput value of *T1*, an HSECK9 license is automatically provided. However, the maximum throughput on the device is still throttled to 250 Mbps *in each direction*.

- [Table 13: Tier and Numeric Throughput Mapping for Virtual Platforms \(C8000v\), Cisco IOS XE Cupertino 17.9.1a and Later Releases](#)
- [Table 14: Tier and Numeric Throughput Mapping for Physical Platforms, Cisco IOS XE Cupertino 17.8.1a and Later Releases](#)
- [Table 15: Tier and Numeric Throughput Mapping for Physical and Virtual Platforms, Cisco IOS XE Cupertino 17.7.x and Earlier Releases](#)

Y: Network Premium and DNA Premium

Y: Network Advantage and DNA Advantage

Y: Network Essentials and DNA Essentials

Table 13: Tier and Numeric Throughput Mapping for Virtual Platforms (C8000v), Cisco IOS XE Cupertino 17.9.1a and Later Releases

Tier (Agg. Value):	T0 (Tx 50M)		T1 (Tx 200M)		T2* (Tx 2 Gbps)			T3* (Tx 20 Gbps)			
					*HSECK9 License Required.						
Configured Numeric Value:	15M	25M	50M	100M	250M	500M	1G	2.5G	5G	10G	
Available DNA Licenses:	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	

Table 14: Tier and Numeric Throughput Mapping for Physical Platforms, Cisco IOS XE Cupertino 17.8.1a and Later Releases

Tier (Agg.):	T0 (50M Agg)			T1 (200M Bi-directional)		T2* (2G Agg.)			T3* (20G Agg. or unthrottled)			T4* (50G Agg.)	T5* (Unthrottled)	
						*HSECK9 License Required								
Configured Numeric Value:	10M	15M	25M	50M	100M	250M	500M	1G	2.5G	5G	10G	-	-	
C8300-1N1S-6T	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>					
C8300-2N2S-6T	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>					

C8300-1N1S-4T2X	YYY	YYY	YYY	YYY	YYY	YYY	YYY	YYY	YY				
C8300-2N2S-4T2X	YYY	YYY	YYY	YYY	YYY	YYY	YYY	YYY	YY				
C8200-1N-4T	YYY	YYY	YYY	YYY	YYY	YYY	YYY						
C8200-1N-4T-L	YYY	YYY	YYY	YYY	YYY	YYY							
C8500-12X									YY	YY	YY		
C8500-12X4QC									YY	YY	YY		
C8500L-8S4X								YY	YY	YY	YY		
C8500-20X6C												YY	YY

Table 15: Tier and Numeric Throughput Mapping for Physical and Virtual Platforms, Cisco IOS XE Cupertino 17.7.x and Earlier Releases

Tier:	T0		T1			T2*			T3*		
						*HSECK9 License Required					
Configured Numeric Value:	10M	15M	25M	50M	100M	250M	500M	1G	2.5G	5G	10G
C8300-1N1S-6T	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>		
C8300-2N2S-6T	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>			
C8300-1N1S-4T2X	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>		
C8300-2N2S-4T2X	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>		
C8200-1N-4T	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>				
C8200-1N-4T-L	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>					
C8500-12X									<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>
C8500-12X4QC									<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>
C8500L-8S4X								<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>
C8000v	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	<div><div>Y</div><div>Y</div></div>	

Numeric vs. Tier-Based Throughput Configuration

With the introduction of tier-based throughput configuration in Cisco IOS XE Cupertino 17.7.1a, when you configure throughput on the device, both numeric and tier-based options are available. This section provides information about when to configure a numeric throughput value and when to configure tier-based throughput.

Cisco Smart Software Manager (CSSM) is a portal that enables you to manage all your Cisco software licenses. All the license PIDs you purchase are listed in the CSSM Web UI at: <https://software.cisco.com> → Manage

licenses. Log in to the portal and in the corresponding Smart Account and Virtual Account, navigate to **Inventory > Licences**, to display the numeric and tier-based licenses in the account. Figure [Figure 2: Numeric and Tier Values Displayed in the CSSM Web UI, on page 87](#) shows you how to distinguish between the two.

- If you purchase a numeric license PID, the license is displayed with the numeric throughput value *and* tier-based value in the CSSM Web UI. For such a license, we recommend that you configure only a numeric throughput value.

See [Configuring a Numeric Throughput, on page 92](#).

- If you purchase a tier-based license PID, the license is displayed with only the tier value in the CSSM Web UI. For such a license, you can either configure a tier-based throughput value to match the display in the CSSM Web UI, or you can configure a numeric throughput value.

See [Configuring a Tier-Based Throughput, on page 95](#) or [Configuring a Numeric Throughput, on page 92](#).



Note

There is no functional impact if you have tier-based license PID in CSSM and you configure a numeric throughput value on the device.

Figure 2: Numeric and Tier Values Displayed in the CSSM Web UI

+	Routing DNA Advantage: Tier 2	→ Tier-Based	Prepaid
+	Routing DNA Advantage: Tier 2: 1G	→ Numeric	Prepaid
+	Routing DNA Advantage: Tier 2: 250M		Prepaid
+	Routing DNA Advantage: Tier 2: 500M		Prepaid
+	Routing DNA Advantage: Tier 3		Prepaid
+	Routing DNA Advantage: Tier 3: 5G		Prepaid
+	Routing DNA Advantage: Tier 4		Prepaid
+	Routing DNA Essentials: Tier 1: 100M		Prepaid
+	Routing DNA Essentials: Tier 2		Prepaid
+	Routing DNA Essentials: Tier 2: 1G		Prepaid
+	Routing DNA Essentials: Tier 2: 250M		Prepaid
+	Routing DNA Essentials: Tier 2: 500M		Prepaid
+	Routing DNA Essentials: Tier 3		Prepaid
+	Routing DNA Premier: Tier 1: 100M		Prepaid
+	Routing DNA Premier: Tier 2: 1G		Prepaid

The following scenarios further clarify when you can *convert* from numeric to tier-based throughput configuration, or from tier-based throughput configuration to numeric, when conversion is required, and when it is optional:

- You have configured a numeric throughput value on the device and the license PID is a numeric license: *You must not* convert to tier-based throughput value.

- You have configured a numeric throughput value on the device and the license PID is a tier-based license: You can convert the throughput configuration to tier-based value - but this is optional. There is no functional impact if you do not convert to a tier-based throughput value.

If you want to convert to a tier-based value, see [Converting From a Numeric Throughput Value to a Tier, on page 99](#)

- You are upgrading to a release where tier-based throughput values are supported and the license PID is tier-based: You can convert the throughput to tier-based value after upgrade - but this is optional. There is no functional impact if you do not convert to a tier-based throughput value.

See [Upgrading from a Release Supporting Numeric Throughput to a Release Supporting Tiers, on page 102](#).

- You are upgrading to a release where tier-based throughput values are supported, and your license PID is numeric: *You must not* convert to a tier-based throughput value.
- You are downgrading to a release where only numeric throughput values are supported and your license PID and throughput configuration are tier-based: *You must* change configuration to a numeric throughput value, *before you downgrade*.

See [Downgrading from a Release Supporting Tiers to a Release Supporting Only Numeric Throughput, on page 103](#).

How to Configure Available Licenses and Throughput

This section provides information about the tasks you must complete, for the licenses available on the Cisco Catalyst 8000 Edge Platforms Family - before you can start using them.

For a Cisco DNA license: **Configure a Boot Level License → Configure Numeric or Tier-Based Throughput → Implement a Smart Licensing Using Policy Topology → Report License Usage (If Applicable)**.

For an HSECK9 license: **Configure a Boot Level License → Implement a Smart Licensing Using Policy Topology → Install SLAC³ → Enable HSECK9 on applicable platforms⁴ → Configure Numeric or Tier-Based Throughput → Report License Usage (If Applicable)**.

For a Cisco UBE, or Cisco Unified CME, or Cisco Unified SRST license: **Implement a Smart Licensing Using Policy Topology → Report License Usage (If Applicable)**.

Configuring a Boot Level License

If you have purchased a Cisco DNA license for a new device, or if you have an existing device and you want to change (upgrade or downgrade, add or remove) the currently configured license on your device, complete the following task.

This sets a boot level license and requires a reload before the configured changes are effective.

³ If a SLAC has been factory-installed by Cisco manufactory (in case of new hardware), skip this step

⁴ Enter the **license feature hseck9** command in global configuration mode for Catalyst 8200, and 8300 Series Edge Platforms only.

SUMMARY STEPS

1. **show version**
2. **configure terminal**
3. Depending on whether the device is a physical or virtual one, configure the applicable command:
 - For physical platforms: **[no] license boot level {network-advantage [addon dna-advantage] | network-essentials [addon dna-essentials] | network-premier [addon dna-premier] }**
 - For virtual platforms: **[no] license boot level {network-advantage {addon dna-advantage} | network-essentials {addon dna-essentials} | network-premier {addon dna-premier} }**
4. **exit**
5. **copy running-config startup-config**
6. **reload**
7. **show version**
8. **show license summary**
9. Complete usage reporting - if required

DETAILED STEPS

	Command or Action	Purpose									
Step 1	show version Example: Device# show version <output truncated> Technology Package License Information: <table border="1"> <thead> <tr> <th>Technology</th><th>Type</th><th>Technology-package</th></tr> </thead> <tbody> <tr> <td>Technology-package</td><td></td><td>Current Next</td></tr> <tr> <td>Reboot</td><td></td><td></td></tr> </tbody> </table> Smart License Perpetual network-advantage network-advantage Smart License Subscription dna-advantage dna-advantage <output truncated>	Technology	Type	Technology-package	Technology-package		Current Next	Reboot			Displays the currently set boot level license. In the accompanying example, Network Advantage and DNA Advantage licences are configured on the device.
Technology	Type	Technology-package									
Technology-package		Current Next									
Reboot											
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.									
Step 3	Depending on whether the device is a physical or virtual one, configure the applicable command: <ul style="list-style-type: none"> • For physical platforms: [no] license boot level {network-advantage [addon dna-advantage] network-essentials [addon dna-essentials] network-premier [addon dna-premier] } • For virtual platforms: [no] license boot level {network-advantage {addon dna-advantage} 	Sets a boot level license. On all platforms, first configure a network-stack license. Only after this can you configure the corresponding add-on license. In the command syntax note how the configuration of a DNA-stack add-on license is optional on physical platforms, but mandatory on virtual platforms.									

	Command or Action	Purpose									
	network-essentials {addon dna-essentials} network-premier {addon dna-premier} } Example: <pre>Device(config)# license boot level network-premier addon dna-premier % use 'write' command to make license boot config take effect on next boot</pre>	<p>The accompanying example, shows configuration on a C8300-1N1S-4T2X router, which is a physical platform. The network-stack license, Network Premier and the corresponding add-on license, DNA-Premier are configured.</p>									
Step 4	exit Example: <pre>Device# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.									
Step 5	copy running-config startup-config Example: <pre>Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] <output truncated></pre>	Saves your entries in the configuration file.									
Step 6	reload Example: <pre>Device# reload Proceed with reload? [confirm] *Dec 8 01:04:12.287: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command. <output truncated></pre>	Reloads the device. License levels configured in Step 3 are effective and displayed only after this reload.									
Step 7	show version Example: <pre>Device# show version <output truncated> Technology Package License Information:</pre> <table border="1"> <thead> <tr> <th>Technology</th><th>Type</th><th>Technology-package</th></tr> </thead> <tbody> <tr> <td>Technology-package</td><td></td><td>Current</td></tr> <tr> <td>Reboot</td><td></td><td>Next</td></tr> </tbody> </table> <pre>Smart License Perpetual network-premier network-premier Smart License Subscription dna-premier dna-premier <output truncated></pre>	Technology	Type	Technology-package	Technology-package		Current	Reboot		Next	<p>Displays the currently set boot level license.</p> <p>In the accompanying example, the output confirms that Network Premier and DNA-Premier licenses are configured.</p>
Technology	Type	Technology-package									
Technology-package		Current									
Reboot		Next									
Step 8	show license summary Example: <pre>Device# show license summary Account Information:</pre>	Displays a summary of license usage, which includes information about licenses being used, the count, and status.									

	Command or Action	Purpose
	<pre>Smart Account: Eg-SA As of Dec 08 08:10:33 2021 UTC Virtual Account: Eg-VA License Usage: License Entitlement Tag Count Status network-premier_T2 (NWSTACK_T2_P) 1 IN USE dna-premier_T2 (DSTACK_T2_P) 1 IN USE</pre>	
Step 9	Complete usage reporting - if required	<p>After you configure a license level, you may have to send a RUM report (Resource Utilization Measurement Report) to CSSM to report license usage information. To know if reporting is required, you can wait for a system message or refer to the policy using show commands.</p> <ul style="list-style-type: none"> The system message, which indicates that reporting is required: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will be required in [dec] days. [dec] is the amount of time (in days) left to meet reporting requirements. If using show commands, refer to the output of the show license status privileged EXEC command and check the <code>Next ACK deadline</code> field. This means a RUM report must be sent and the acknowledgement (ACK) from CSSM must be installed by this date. <p><i>How you send the RUM report, depends on the topology you have implemented in the Smart Licensing Using Policy environment. For more information, see How to Configure Smart Licensing Using Policy: Workflows by Topology.</i></p>

Installing SLAC for an HSECK9 License

A Smart Licensing Authorization Code (SLAC) is generated in and obtained from Cisco Smart Software Manager (CSSM) portal.

There are multiple ways in which a product may be connected to the CSSM, in order to obtain a SLAC. Each way of connecting to CSSM is called a topology. You must implement one of the supported topologies so you can then install SLAC in the corresponding method.

For information about all the methods, see the [Supported Topologies](#) section of the [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#) document.



Note Ensure that a boot level license is already configured on the device. See [Configuring a Boot Level License, on page 88](#). In the output of the show version privileged EXEC command ensure that a license is mentioned in the `License Level` field.

Required Tasks After Installing SLAC

Complete the following required tasks after installing SLAC - only if applicable to the platform:

Platform	Required Tasks After Installing SLAC
For Catalyst 8200 and 8300 Series Edge Platforms	Enter the license feature hseck9 command in global configuration mode. This <i>enables</i> the HSECK9 license on these platforms.
For the C8500L models of the Catalyst 8500 Series Edge Platforms	Reload the device after installing SLAC.

Configuring a Numeric Throughput

This task shows you how to change the numeric throughput level on physical and virtual platforms. If you do not configure a throughput level, the platform's default throughput level is effective.

Configuration of a throughput level requires a reload on physical platforms (Catalyst 8200, 8300, and 8500 Series Edge Platforms). A reload is not required for virtual platforms (Catalyst 8000V Edge Software).

Before you begin

- Read the [Throughput as a Numeric Value , on page 76](#) and [Numeric vs. Tier-Based Throughput Configuration, on page 85](#) sections.
- Ensure that a boot level license is already configured on the device. See [Configuring a Boot Level License, on page 88](#). In the output of the show version privileged EXEC command ensure that a license is mentioned in the `License Level` field.
- If you are configuring throughput greater than 250 Mbps, ensure that you have already installed a Smart Licensing Authorization Code (SLAC) according to the method that applies to your topology in the Smart Licensing Using Policy environment. See [Installing SLAC for an HSECK9 License, on page 91](#).
- Note the throughput you are entitled to. This is indicated in the Cisco DNA license PID you purchase.

SUMMARY STEPS

1. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**
2. **configure terminal**
3. Depending on whether the device is a physical or virtual one, configure the applicable command:

- For physical platforms: **platform hardware throughput crypto** {100M | 10M | 15M | 1G | 2.5G | 250M | 25M | 500M | 50M}
- For virtual platforms: **platform hardware throughput level MB** {100 | 1000 | 10000 | 15 | 25 | 250 | 2500 | 50 | 500 | 5000}

4. **exit**
5. **copy running-config startup-config**
6. **reload**
7. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>Depending on whether the device is a physical or virtual one, enter the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: show platform hardware throughput crypto • For virtual platforms: show platform hardware throughput level <p>Example:</p> <pre>Device# show platform hardware throughput crypto</pre> <p>Current configured crypto throughput level: 250M Level is saved, reboot is not required Current enforced crypto throughput level: 250M Crypto Throughput is throttled at 250M Default Crypto throughput level: 10M Current boot level is network-advantage</p> <p>OR</p> <pre>Device# show platform hardware throughput level</pre> <p>The current throughput level is 1000000 kb/s</p>	<p>Displays the currently running throughput on the device.</p> <p>In the accompanying examples,</p> <ul style="list-style-type: none"> • The show platform hardware throughput crypto sample output is of a physical platform (a C8300-2N2S-4T2X). Here the throughput level is throttled at 250M. • The show platform hardware throughput level sample output is of a virtual platform (a C8000V).
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>Depending on whether the device is a physical or virtual one, configure the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: platform hardware throughput crypto {100M 10M 15M 1G 2.5G 250M 25M 500M 50M} • For virtual platforms: platform hardware throughput level MB {100 1000 10000 15 25 250 2500 50 500 5000} 	<p>Configures the throughput level. The displayed throughput options depend on the device.</p> <p>The following apply to both physical and virtual platforms:</p> <ul style="list-style-type: none"> • At a minimum, you must have configured a network-stack license already. Otherwise the command is not recognized as a valid one on the command line interface.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config)# platform hardware throughput crypto ? 100M 100 mbps bidirectional thput 10M 10 mbps bidirectional thput 15M 15 mbps bidirectional thput 1G 2 gbps aggregate thput 2.5G 5 gbps aggregate thput 250M 250 mbps bidirectional thput 25M 25 mbps bidirectional thput 500M 1gbps aggregate thput 50M 50 mbps bidirectional thput</pre> <pre>Device(config)# platform hardware throughput crypto 1G % These values don't take effect until the next reboot. Please save the configuration.</pre> <p>OR</p> <pre>Device(config)# platform hardware throughput level MB 5000 %Throughput has been set to 5000 Mbps.</pre>	<ul style="list-style-type: none"> If you are configuring throughput greater than 250 Mbps, you must have already installed SLAC. Options greater than 250 Mbps are displayed only if SLAC is installed. <p>In the accompanying examples,</p> <ul style="list-style-type: none"> 1 Gbps is configured on the physical platform. Aggregate throughput throttling (Cisco IOS XE Cupertino 17.8.1a and later) is effective. After reboot, irrespective of the distribution of traffic in the upstream and downstream direction, an aggregate throughput limit of 2 Gbps is effective. 5000 Mbps is configured on the virtual platform. A maximum of 5000 Mbps upstream and 5000 Mbps downstream throughput is supported.
Step 4	<p>exit</p> <p>Example:</p> <pre>Device# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre>	Saves your entries in the configuration file.
Step 6	<p>reload</p> <p>Example:</p> <pre>Device# reload</pre>	<p>Reloads the device.</p> <p>Note Perform this step only if the device you are configuring throughput on is a physical platform (Catalyst 8200, 8300, and 8500 Series Edge Platforms).</p> <p>Skip this step if you are configuring throughput on a virtual platform (Catalyst 8000V Edge Software).</p>
Step 7	Depending on whether the device is a physical or virtual one, enter the applicable command:	Displays the currently running throughput on the device.

	Command or Action	Purpose
	<ul style="list-style-type: none"> • For physical platforms: show platform hardware throughput crypto • For virtual platforms: show platform hardware throughput level <p>Example:</p> <pre>Device# show platform hardware throughput crypto Current configured crypto throughput level: 1G Level is saved, reboot is not required Current enforced crypto throughput level: 1G Crypto Throughput is throttled at 2G(Aggregate) Default Crypto throughput level: 10M</pre> <p>OR</p> <pre>Device# show platform hardware throughput level The current throughput level is 5000000 kb/s</pre>	<p>Note On physical platforms, you can also enter the show platform hardware qfp active feature ipsec state privileged EXEC command to display the configured throughput level.</p>

Configuring a Tier-Based Throughput

This task shows you how to configure a tier-based throughput level on physical and virtual platforms. If you do not configure a throughput level, the platform's default throughput level is effective.

Tier-based throughput levels are supported starting with Cisco IOS XE Cupertino 17.7.1a only.

Configuration of a throughput level requires a reload on physical platforms (Catalyst 8200, 8300, and 8500 Series Edge Platforms). A reload is not required for virtual platforms (Catalyst 8000V Edge Software).

Before you begin

- Read the [Throughput as a Tier, on page 82](#) and [Numeric vs. Tier-Based Throughput Configuration, on page 85](#) sections.
- Ensure that a boot level license is already configured on the device. See [Configuring a Boot Level License, on page 88](#). In the output of the **show version** privileged EXEC command, ensure that the license is mentioned.
- If you want to configure Tier 3 (T3) ensure that the boot level license is Network Advantage/ DNA Advantage, or Network Premier/DNA Premier. T3 is not supported with Network Essentials and DNA Essentials.
- If you are configuring Tier 2 (T2) or a higher tier, ensure that you have already installed a Smart Licensing Authorization Code (SLAC) according to the method that applies to your topology in the Smart Licensing Using Policy environment. See [Installing SLAC for an HSECK9 License, on page 91](#).
 - On physical platforms, T2 or higher tiers are not displayed if SLAC is not installed.
 - On virtual platforms, all tier options are displayed even if SLAC is not installed. But SLAC is required if you want to configure T2 or a higher tier.
- Note the throughput you are entitled to. This is indicated in the Cisco DNA license PID you purchase.

SUMMARY STEPS

1. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**
2. **show license authorization**
3. **configure terminal**
4. Depending on whether the device is a physical or virtual one, configure the applicable command:
 - For physical platforms: **platform hardware throughput crypto {T0 | T1 | T2 | T3}**
 - For virtual platforms: **platform hardware throughput level MB {T0 | T1 | T2 | T3 }**
5. **exit**
6. **copy running-config startup-config**
7. **reload**
8. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>Depending on whether the device is a physical or virtual one, enter the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: show platform hardware throughput crypto • For virtual platforms: show platform hardware throughput level <p>Example:</p> <pre>Device# show platform hardware throughput crypto show platform hardware throughput crypto Current configured crypto throughput level: 250M Level is saved, reboot is not required Current enforced crypto throughput level: 250M Crypto Throughput is throttled at 250M Default Crypto throughput level: 10M Current boot level is network-premier</pre> <p>OR</p> <pre>Device# show platform hardware throughput level The current throughput level is 10000 kb/s</pre>	<p>Displays the currently running throughput on the device.</p> <p>In the accompanying examples:</p> <ul style="list-style-type: none"> • The show platform hardware throughput crypto sample output is of a physical platform (a C8300-2N2S-4T2X). Here throughput is currently throttled at 250 Mbps. • The show platform hardware throughput level sample output is of a virtual platform (a C8000V). Here the current throughput level is 10 Mbps.
Step 2	<p>show license authorization</p> <p>Example:</p> <pre>Device# show license authorization Overall status: Active: PID:C8300-2N2S-4T2X,SN:FDO2250A0J5 Status: SMART AUTHORIZATION INSTALLED on Mar</pre>	<p>(Optional) Displays SLAC information on the product instance.</p> <p>In the accompanying example:</p> <ul style="list-style-type: none"> • SLAC is installed on the physical platform. This is so we can configure T2 in the subsequent steps.

	Command or Action	Purpose
	<pre>02 05:05:19 2022 UTC Last Confirmation code: 418b11b3 Authorizations: Router US Export Lic. for DNA (DNA_HSEC): Description: U.S. Export Restriction Compliance license for DNA based Routers Total available count: 1 Enforcement type: EXPORT RESTRICTED Term information: Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5 Authorization type: SMART AUTHORIZATION INSTALLED License type: PERPETUAL Term Count: 1 Purchased Licenses: No Purchase Information Available OR Device# show license authorization Overall status: Active: PID:C8000V,SN:9I8GRCH8CMN Status: NOT INSTALLED</pre>	<ul style="list-style-type: none"> SLAC is not available on the virtual platform. Note how this affects throughput configuration in the subsequent steps.
Step 3	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 4	<p>Depending on whether the device is a physical or virtual one, configure the applicable command:</p> <ul style="list-style-type: none"> For physical platforms: platform hardware throughput crypto {T0 T1 T2 T3} For virtual platforms: platform hardware throughput level MB {T0 T1 T2 T3 } <p>Example:</p> <pre>Device(config)# platform hardware throughput crypto ? 100M 100 mbps bidirectional thput 10M 10 mbps bidirectional thput 15M 15 mbps bidirectional thput 1G 2 gbps aggregate thput 2.5G 5 gbps aggregate thput</pre>	<p>Configures a tier-based throughput. The throughput options that are displayed, depend on the device.</p> <p>Note Only tiers are mentioned in command, for the sake of clarity. When you enter the command on the CLI, numeric and tier values are displayed - as shown in the accompanying examples.</p> <p>The following apply to both physical and virtual platforms:</p> <ul style="list-style-type: none"> You have configured a boot level license already. Otherwise the command for throughput configuration is not recognized as a valid one on the command line interface. If you are configuring T2 or a higher tier, you have installed SLAC.

	Command or Action	Purpose
	<pre> 250M 250 mbps bidirectional thput 25M 25 mbps bidirectional thput 500M 1gbps aggregate thput 50M 50 mbps bidirectional thput T0 T0(up to 15 mbps) bidirectional thput T1 T1(up to 100 mbps) bidirectional thput T2 T2(up to 2 gbps) aggregate thput T3 T3(up to 5 gbps) aggregate thput Device(config)# platform hardware throughput crypto T2 % These values don't take effect until the next reboot. Please save the configuration. *Mar 02 05:06:19.042: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD: New throughput level not applied until reload; please save config OR Device(config)# platform hardware throughput level MB ? 100 Mbps 1000 Mbps 10000 Mbps 15 Mbps 25 Mbps 250 Mbps 2500 Mbps 50 Mbps 500 Mbps 5000 Mbps T0 Tier0(up to 15M throughput) T1 Tier1(up to 100M throughput) T2 Tier2(up to 1G throughput) T3 Tier3(up to 10G throughput) T4 Tier4(unthrottled) Device(config)# platform hardware throughput level MB T2 %Requested throughput will be set once HSEC authorization code is installed </pre>	<p>Note</p> <p>On a physical platform, you will not be able to configure T2 or a higher tier if SLAC is not installed.</p> <p>On a virtual platform, if you configure T2 or a higher tier without SLAC, the product instance automatically tries to reach CSSM to request and install SLAC. If it is successful, throughput is set to the configured tier. If it is not successful, the system sets the throughput to 250 Mbps. If and when SLAC is installed, the throughput is automatically set to the last configured value.</p> <p>In the accompanying examples:</p> <ul style="list-style-type: none"> On the physical platform (platform hardware throughput crypto), tiers T2 and higher tiers are displayed, because SLAC is installed. If SLAC were not available, T1 would have been the highest tier displayed. Further, aggregate throughput throttling (Cisco IOS XE Cupertino 17.8.1a and later) is effective. After reboot, irrespective of the distribution of traffic in the upstream and downstream direction, an aggregate throughput limit of 2 Gbps is supported. On the virtual platform (platform hardware throughput level MB), all tiers are displayed. After T2 is configured, the system message alerts you to the fact that the configuration is not set, because SLAC is not installed.
Step 5	<p>exit</p> <p>Example:</p> <pre>Device# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	<p>copy running-config startup-config</p> <p>Example:</p>	Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]	
Step 7	reload Example: Device# reload Proceed with reload? [confirm] *Mar 02 05:07:00.979: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.	Reloads the device. Note A reload is required only for physical platforms.
Step 8	Depending on whether the device is a physical or virtual one, enter the applicable command: <ul style="list-style-type: none"> For physical platforms: show platform hardware throughput crypto For virtual platforms: show platform hardware throughput level Example: Device# show platform hardware throughput crypto Current configured crypto throughput level: T2 Level is saved, reboot is not required Current enforced crypto throughput level: 1G Crypto Throughput is throttled at 2G(Aggregate) Default Crypto throughput level: 10M Current boot level is network-premier OR Device# show platform hardware throughput level The current throughput level is 250000 kb/s	Displays the currently running throughput on the device. In the accompanying examples: <ul style="list-style-type: none"> On the physical platform, the tier value is set to T2. Note On physical platforms, you can also enter the show platform hardware qfp active feature ipsec state privileged EXEC command to display the configured throughput level. <ul style="list-style-type: none"> On the virtual platform, throughput is set to 250 Mbps. If and when SLAC is installed, the throughput will be automatically set to the last configured value, which is T2.

Converting From a Numeric Throughput Value to a Tier

This task shows you how to convert a numeric throughput value to a tier-based throughput value. To know how numeric throughput values are mapped to tier values refer to the table here: [Tier and Numeric Throughput Mapping](#).

Converting the throughput level requires a reload on physical platforms (Catalyst 8200, 8300, and 8500 Series Edge Platforms). A reload is not required for virtual platforms (Catalyst 8000V Edge Software).

Before you begin

- Read the [Numeric vs. Tier-Based Throughput Configuration, on page 85](#) section.
- If you are converting numeric throughput that is equal or greater than 250 Mbps, ensure that a SLAC is installed on the device. See [Installing SLAC for an HSECK9 License, on page 91](#).
- The software version running on the product instance is Cisco IOS XE Cupertino 17.7.1a or a later release.

SUMMARY STEPS

1. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**
2. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **license throughput crypto auto-convert**
 - For virtual platforms: **license throughput level auto-convert**
3. **copy running-config startup-config**
4. **reload**
5. Depending on whether the device is a physical or virtual one, enter the applicable command:
 - For physical platforms: **show platform hardware throughput crypto**
 - For virtual platforms: **show platform hardware throughput level**
6. Verify that conversion is complete.
 - For physical platforms: **license throughput crypto auto-convert**
 - For virtual platforms: **license throughput level auto-convert**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>Depending on whether the device is a physical or virtual one, enter the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: show platform hardware throughput crypto • For virtual platforms: show platform hardware throughput level <p>Example:</p> <pre>Device# show platform hardware throughput crypto Current configured crypto throughput level: 500M Level is saved, reboot is not required Current enforced crypto throughput level: 500M Crypto Throughput is throttled at 500M Default Crypto throughput level: 10M Current boot level is network-premier</pre> <p>OR</p> <pre>Device# show platform hardware throughput level The current throughput level is 100000 kb/s</pre>	Displays the currently running throughput on the device.
Step 2	<p>Depending on whether the device is a physical or virtual one, enter the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: license throughput crypto auto-convert • For virtual platforms: license throughput level auto-convert 	Converts the numeric throughput to a tier-based throughput value. The converted tier value is displayed on the CLI.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device# license throughput crypto auto-convert Crypto throughput auto-convert from level 500M to T2 % These values don't take effect until the next reboot. Please save the configuration. *Dec 8 03:21:01.401: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD: New throughput level not applied until reload; please save config OR Device# license throughput level auto-convert %Throughput tier set to T1 (100 Mbps) % Tier conversion is successful. Please write memory to save the tier config</pre>	
Step 3	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]</pre>	<p>Saves your entries in the configuration file.</p> <p>Note Even though the command you use to convert from numeric to tier-based throughput is a privileged EXEC command, it changes running configuration from a numeric value to a tier-based value. You must therefore save configuration for the next reload to be displayed with a tier value.</p>
Step 4	<p>reload</p> <p>Example:</p> <pre>Device# reload Proceed with reload? [confirm] *Dec 8 03:24:09.534: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command</pre>	<p>Reloads the device.</p> <p>Note A reload is required only on physical platforms.</p>
Step 5	<p>Depending on whether the device is a physical or virtual one, enter the applicable command:</p> <ul style="list-style-type: none"> • For physical platforms: show platform hardware throughput crypto • For virtual platforms: show platform hardware throughput level <p>Example:</p> <pre>Device# show platform hardware throughput crypto Current configured crypto throughput level: T2 Level is saved, reboot is not required Current enforced crypto throughput level: 1G Crypto Throughput is throttled at 1G Default Crypto throughput level: 10M Current boot level is network-premier</pre>	<p>Displays the currently running throughput on the device.</p>

	Command or Action	Purpose
	OR Device# show platform hardware throughput level The current throughput level is 100000 kb/s	
Step 6	Verify that conversion is complete. <ul style="list-style-type: none"> For physical platforms: license throughput crypto auto-convert For virtual platforms: license throughput level auto-convert Example: Device# license throughput crypto auto-convert Crypto throughput is already tier based, no need to convert. OR Device# license throughput level auto-convert % Tier conversion not possible since the device is already in tier licensing	Tip To cross-check that conversion is complete, you can also enter the conversion command again. If the numeric throughput value has already been converted, the system displays a message confirming this.

Upgrading from a Release Supporting Numeric Throughput to a Release Supporting Tiers

If you are upgrading to Cisco IOS XE Cupertino 17.7.1 or later release *and* the license PID is a tier-based one, you can convert throughput configuration to a tier-based value, or you can retain the numeric throughput configuration.



Note There is no functional impact if you have tier-based license PID in CSSM and a numeric throughput value is configured on the device.

If you want to convert to a tier-based value note the required action depending on the throughput level that is configured:

Throughput Configuration Before Upgrade	Action Before Upgrade	Action After Upgrade to 17.7.1 or Later
Lesser than 250 Mbps	No action required.	Converting From a Numeric Throughput Value to a Tier, on page 99
Equal to 250 Mbps	Obtain an HSECK9 license and install SLAC if you want to convert to T2.	Converting From a Numeric Throughput Value to a Tier, on page 99
Greater than 250 Mbps	No action required.	Converting From a Numeric Throughput Value to a Tier, on page 99

Downgrading from a Release Supporting Tiers to a Release Supporting Only Numeric Throughput

If you are downgrading to a release where only numeric throughput configuration is supported, you *must* convert tier-based throughput configuration to a numeric throughput value before downgrade. This is applicable even if the license PID is a tier-based license PID.

**Caution**

If a tier-based throughput value was configured before downgrade and you downgrade without changing to a numeric value, tier configuration is not recognized by a pre-17.7.1 image and configuration fails. Further, throughput may not be restored to the pre-downgrade level and you have to configure a numeric throughput level after downgrade.

Throughput Configuration Before Downgrade	Action Before Downgrade	Action After Downgrade to a pre-17.7.1 Version
Numeric	No action required.	No action required.
Tier	Configuring a Numeric Throughput, on page 92	No action required.

Available Licensing Models

The licensing model defines *how* you account for or report the licenses that you use, to Cisco. The following licensing models are available on the Cisco Catalyst 8000 Edge Platforms Family:

Smart Licensing Using Policy

With this licensing model, you purchase the licenses you want to use, configure them on the device, and then report license usage – as required. You do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it - unless you are using export-controlled and enforced licenses.

This licensing model is supported on all products in the Cisco Catalyst 8000 Edge Platforms Family.

For more information, see [Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#).

Pay As You Go (PAYG) Licensing

**Note**

This licensing model is available only on Catalyst 8000V Edge Software.

Cisco Catalyst 8000V supports the PAYG licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace - in both the autonomous mode and the controller mode. The Cisco Catalyst 8000V hourly-billed Amazon Machine Image (AMI) or the Pay As You Go licensing model allows you to consume an instance for a defined period of time.

- In the autonomous mode, you can directly launch an instance from the AWS or Azure Marketplace and start using it. The licenses are embedded in the image and the selected license package and configured throughput level are effective when you launch the instance
- In the controller mode, which is supported from Cisco IOS-XE Bengaluru 17.5.1, you must first onboard the device into Cisco SD-WAN as per [Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing](#). After this, when you launch the instance from AWS, the device comes-up with the license already installed for unlimited throughput.

Managed Service Licensing Agreement

Managed Service Licensing Agreement (MSLA) is a consumption-based software licensing model designed for Cisco's Managed Service Provider business.

- **MSLA in Cisco SD-WAN Controller Mode**

In the Cisco SD-WAN controller mode, an MSLA is supported on all products in the Cisco Catalyst 8000 Edge Platforms Family. For more information, see:

[Managed Service Licensing Agreement \(MSLA\) for Cisco SD-WAN At-a-Glance](#)

[Cisco SD-WAN Getting Started Guide](#) → *Manage Licenses for Smart Licensing Using Policy*.

[Cisco vManage How-Tos for Cisco IOS XE SD-WAN Devices](#) → *Manage Licenses for Smart Licensing Using Policy*.

- **MSLA in Autonomous Mode**

In the autonomous mode, an MSLA is available only with Catalyst 8000V Edge Software, starting from Cisco IOS XE Cupertino 17.9.1a.

Here, you begin by entering into an MSLA with Cisco, and purchase licenses with subscription IDs.

Licenses with subscription IDs can be ordered on [Cisco commerce workspace](#) (CCW). Ordered licenses are deposited in the specified Smart Account and Virtual Account in CSSM, with the corresponding subscription IDs.

To complete licensing workflows, you must implement a supported topology. After CSSM receives license usage information, you are billed based on the throughput and the Cisco DNA subscription tier that is activated and in-use. For more information, see: [MSLA](#) and [Utility Mode](#).



CHAPTER 10

Consolidated Package Management

This chapter discusses how consolidated packages are managed and are used to run the Cisco Catalyst 8500 Series Edge Platforms.



Note This process is not applicable for C8500L-8S4X.

It contains the following sections:

- [Running the Cisco Catalyst 8500 Series Edge Platforms: An Overview, on page 105](#)
- [Software File Management Using Command Sets, on page 106](#)
- [Managing and Configuring the Router to Run Using Consolidated Packages, on page 107](#)
- [Installing the Software Using install Commands, on page 109](#)

Running the Cisco Catalyst 8500 Series Edge Platforms: An Overview

The Cisco Catalyst 8500 Series Edge Platforms can be run using a complete consolidated package.

This section covers the following topics:

Running the Cisco Catalyst 8500 Series Edge Platforms Using a Consolidated Package: An Overview

The Cisco Catalyst 8500 Series Edge Platforms can be configured to run using a consolidated package.

When the router is configured to run using a consolidated package, the entire consolidated package file is copied onto the router or accessed by the router via TFTP or another network transport method. The router runs using the consolidated package file.

When a Cisco Catalyst 8500 Series Edge Platforms is configured to run using the consolidated package file, more memory is required to process router requests because the router has to search one larger file for every request. The peak amount of memory available for passing network traffic is therefore lower when the router is configured to run using a consolidated package.

A Cisco Catalyst 8500 Series Edge Platforms configured to run using a consolidated package is booted by booting the consolidated package file.

A consolidated package can be booted and utilized using TFTP or another network transport method. Running the router using a consolidated package may be the right method of running the router in certain networking environments.

The consolidated package should be stored on bootflash:, usb[0-1]:, or a remote file system when this method is used to run the router.

Running the Cisco Catalyst 8500 Series Edge Platforms: A Summary

This section summarizes the advantages and disadvantages of each method of running your Cisco Catalyst 8500 Series Edge Platforms.

The advantages of running your router using a consolidated package include:

- Simplified installation—Only one software file needs to be managed instead of several separate images.
- Storage—A consolidated package can be used to run the router while being stored in bootflash:, on a USB Flash disk, or on a network server. A consolidated package can be booted and utilized using TFTP or another network transport method.

Software File Management Using Command Sets

Software files can be managed on the Cisco Catalyst 8500 Series Edge Platforms using three distinct command sets. This section provides overviews of the following command sets:

The request platform Command Set

The **request platform software package** command is part of the larger **request platform** command set being introduced on the Cisco Catalyst 8500 Series Edge Platforms. For additional information on each **request platform** command and the options available with each command, see the *Cisco IOS Configuration Fundamentals Command Reference*.

The **request platform software package** command, which can be used to upgrade individual subpackages and a complete consolidated package, is used to upgrade software on the Cisco Catalyst 8500 Series Edge Platforms. Notably, the **request platform software package** command is the recommended way of performing an individual subpackage upgrade, and also provides the only method of no-downtime upgrades of individual subpackages on the router when the router is running individual subpackages.

The **request platform software package** command requires that the destination device or process be specified in the command line, so the commands can be used to upgrade software on both an active or a standby processor. The **request platform software package** command allows for no downtime software upgrades in many scenarios.

The basic syntax of the command is **request platform software package install rp *rp-slot-number* file *file-URL***, where *rp-slot-number* is the number of the RP slot and *file-URL* is the path to the file being used to upgrade the Cisco Catalyst 8500 Series Edge Platforms. The command has other options; see the **request platform software package** command references for information on all of the options available with this command set.

The copy Command

To upgrade a consolidated package on the Cisco Catalyst 8500 Series Edge Platforms, copy the consolidated package onto a file system, usually bootflash: or usb[0-1]: on the router, using the **copy** command as you would on most other Cisco routers. After making this copy, configure the router to boot using the consolidated package file.

See the **copy** command reference for a list of the options that are available with the **copy** command.

Managing and Configuring the Router to Run Using Consolidated Packages

This section discusses the following topics:

Quick Start Software Upgrade

The following instructions provide a quick start version of upgrading the software running the Cisco Catalyst 8500 Series Edge Platforms. These instructions assume you have access to the consolidated package and that the files will be stored in a bootflash: file system and has enough room for the file or files.

For more detailed installation examples, see the other sections of this chapter.

To upgrade the software using a quick start version, perform the following steps:

SUMMARY STEPS

1. Copy the consolidated package into bootflash: using the **copy URL-to-image bootflash:** command.
2. Enter the **dir bootflash:** command to verify your consolidated package in the directory.
3. Set up the boot parameters for your boot. Set the configuration register to 0x2 by entering the **config-register 0x2102** global configuration command, and enter the **boot system flash bootflash:image-name**
4. Enter **copy running-config startup-config** to save your configuration.
5. Enter the **reload** command to reload the router and finish the boot. The upgraded software should be running when the reload completes.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | Copy the consolidated package into bootflash: using the copy URL-to-image bootflash: command. |
| Step 2 | Enter the dir bootflash: command to verify your consolidated package in the directory. |
| Step 3 | Set up the boot parameters for your boot. Set the configuration register to 0x2 by entering the config-register 0x2102 global configuration command, and enter the boot system flash bootflash:image-name |
| Step 4 | Enter copy running-config startup-config to save your configuration. |
| Step 5 | Enter the reload command to reload the router and finish the boot. The upgraded software should be running when the reload completes. |
-

Managing and Configuring a Router to Run Using a Consolidated Package

This section documents the following procedures:

Managing and Configuring a Consolidated Package Using the copy Command

To upgrade a consolidated package on the Cisco Catalyst 8500 Series Edge Platforms using the **copy** command, copy the consolidated package into the bootflash: directory on the router using the **copy** command as you would on most other Cisco routers. After making this copy, configure the router to boot using the consolidated package file.

In the following example, the consolidated package file is copied onto the bootflash: file system from TFTP. The config-register is then set to boot using **boot system** commands, and the **boot system** commands instruct the router to boot using the consolidated package stored in the bootflash: file system. The new configuration is then saved using the **copy running-config startup-config** command, and the system is then reloaded to complete the process.

```
Router# dir bootflash:
Directory of bootflash:/
  11   drwx           16384   Dec 4 2007 04:32:46 -08:00  lost+found
86401  drwx           4096   Dec 4 2007 06:06:24 -08:00  .ssh
14401  drwx           4096   Dec 4 2007 06:06:36 -08:00  .rollback_timer
28801  drwx           4096   Mar 18 2008 17:31:17 -07:00  .prst_sync
43201  drwx           4096   Dec 4 2007 04:34:45 -08:00  .installer
  13   -rw-          45977   Apr 9 2008 16:48:46 -07:00  target_support_output.tgz.tgz
928862208 bytes total (712273920 bytes free)
Router# copy tftp bootflash:
```

```
Router# dir bootflash:
```

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router# reload
```

Managing and Configuring a Consolidated Package Using the request platform software package install Command

In the following example, the **request platform software package install** command is used to upgrade a consolidated package running on RP 0. The **force** option, which forces the upgrade past any prompt (such as already having the same consolidated package installed), is used in this example.

```
Router# request platform software package install rp 0 file bootflash: force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
```



```
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

WARNING:
WARNING: Candidate software will be installed upon reboot
WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned. New software will load on reboot.
```

Router# **reload**



Note A reload must be performed to finish this procedure. The [Managing and Configuring a Consolidated Package Using the copy Command, on page 108](#) includes an example of how to configure the router to boot using the consolidated package, and then an example of what happens after the reload is performed to finish the installation.

Installing the Software Using install Commands

From Cisco IOS XE Cupertino 17.7.1a, Cisco Catalyst 8000 Edge platforms are shipped in install mode by default. Users can boot the platform, and upgrade or downgrade to Cisco IOS XE software versions using a set of **install** commands.

Restrictions for Installing the Software Using install Commands

- ISSU is not covered in this feature.
- Install mode requires a reboot of the system.

Information About Installing the Software Using install Commands

From Cisco IOS XE Cupertino 17.7.1a release, for routers shipped in install mode, a set of **install** commands can be used for starting, upgrading and downgrading of platforms in install mode. This update is applicable to the Cisco Catalyst 8000 Edge platforms.

The following table describes the differences between Bundle mode and Install mode:

Table 16: Bundle Mode vs Install Mode

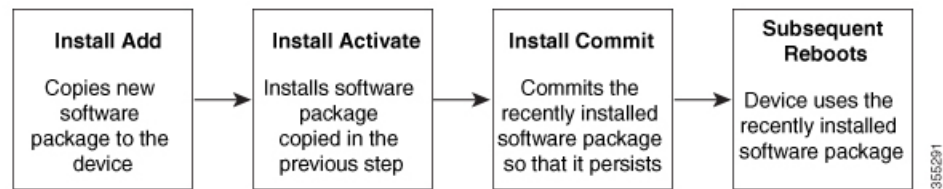
Bundle Mode	Install Mode
This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image.	This mode uses the local (bootflash) packages.conf file for the boot process.
This mode uses a single .bin file.	.bin file is replaced with expanded .pkg files in this mode.
CLI: <code>#boot system file <filename></code>	CLI: <code>#install add file bootflash: [activate commit]</code>
To upgrade in this mode, point the boot system to the new image.	To upgrade in this mode, use the install commands.
Image Auto-Upgrade: When a new Field-Replaceable Unit (FRU) is inserted in a modular chassis, manual intervention is required to get the new FRU running with the same version as the active FRUs.	Image Auto-Upgrade: When a new FRU is inserted in a modular chassis, the joining FRU is auto-upgraded to the image version in sync with the active FRUs.
Rollback: Rollback to the previous image with multiple Software Maintenance Updates (SMUs) may require multiple reloads.	Rollback: Enables rollback to an earlier version of Cisco IOS XE software, including multiple patches in single reload.

Install Mode Process Flow

The install mode process flow comprises three commands to perform installation and upgrade of software on platforms—**install add**, **install activate**, and **install commit**.

The following flow chart explains the install process with **install** commands:

Process with Install Commit



The **install add** command copies the software package from a local or remote location to the platform. The location can be FTP, HTTP, HTTPS, or TFTP. The command extracts individual components of the .package file into subpackages and packages.conf files. It also validates the file to ensure that the image file is specific to the platform on which it is being installed.

The **install activate** command performs the required validations and provisions the packages previously added using the **install add** command. It also triggers a system reload.

The **install commit** command confirms the packages previously activated using the **install activate** command, and makes the updates persistent over reloads.



Note Installing an update replaces any previously installed software image. At any time, only one image can be installed in a device.

The following set of install commands is available:

Table 17: List of install Commands

Command	Syntax	Purpose
install add	install add file <i>location:filename.bin</i>	<p>Copies the contents of the image, package, and SMUs to the software repository. File location may be local or remote. This command does the following:</p> <ul style="list-style-type: none"> Validates the file—checksum, platform compatibility checks, and so on. Extracts individual components of the package into subpackages and packages.conf Copies the image into the local inventory and makes it available for the next steps.

Command	Syntax	Purpose
install activate	install activate	<p>Activates the package added using the install add command.</p> <ul style="list-style-type: none"> • Use the show install summary command to see which image is inactive. This image will get activated. • System reloads on executing this command. Confirm if you want to proceed with the activation. Use this command with the prompt-level none keyword to automatically ignore any confirmation prompts.
(install activate) auto abort-timer	install activate auto-abort timer <i><30-1200></i>	<p>The auto-abort timer starts automatically, with a default value of 120 minutes. If the install commit command is not executed within the time provided, the activation process is terminated, and the system returns to the last-committed state.</p> <ul style="list-style-type: none"> • You can change the time value while executing the install activate command. • The install commit command stops the timer, and continues the installation process. • The install activate auto-abort timer stop command stops the timer without committing the package. • Use this command with the prompt-level none keyword to automatically ignore any confirmation prompts. • This command is valid only in the three-step install variant.

Command	Syntax	Purpose
install commit	install commit	<p>Commits the package activated using the install activate command, and makes it persistent over reloads.</p> <ul style="list-style-type: none"> • Use the show install summary command to see which image is uncommitted. This image will get committed.
install abort	install abort	<p>Terminates the installation and returns the system to the last-committed state.</p> <ul style="list-style-type: none"> • This command is applicable only when the package is in activated status (uncommitted state). • If you have already committed the image using the install commit command, use the install rollback to command to return to the preferred version.
install remove	install remove {file <filename> inactive}	<p>Deletes inactive packages from the platform repository. Use this command to free up space.</p> <ul style="list-style-type: none"> • file: Removes specified files. • inactive: Removes all the inactive files.

Command	Syntax	Purpose
install rollback to	install rollback to {base label committed id}	<p>Rolls back the software set to a saved installation point or to the last-committed installation point. The following are the characteristics of this command:</p> <ul style="list-style-type: none"> • Requires reload. • Is applicable only when the package is in committed state. • Use this command with the prompt-level none keyword to automatically ignore any confirmation prompts. <p>Note If you are performing install rollback to a previous image, the previous image must be installed in install mode. Only SMU rollback is possible in bundle mode.</p>
install deactivate	install deactivate file <filename>	<p>Removes a package from the platform repository. This command is supported only for SMUs.</p> <ul style="list-style-type: none"> • Use this command with the prompt-level none keyword to automatically ignore any confirmation prompts.

The following show commands are also available:

Table 18: List of show Commands

Command	Syntax	Purpose
show install log	show install log	Provides the history and details of all install operations that have been performed since the platform was booted.
show install package	show install package <filename>	Provides details about the .pkg/.bin file that is specified.

Command	Syntax	Purpose
show install summary	show install summary	<p>Provides an overview of the image versions and their corresponding install states for all the FRUs.</p> <ul style="list-style-type: none"> • The table that is displayed will state for which FRUs this information is applicable. • If all the FRUs are in sync in terms of the images present and their state, only one table is displayed. • If, however, there is a difference in the image or state information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install active	show install active	<p>Provides information about the active packages for all the FRUs.</p> <p>If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.</p>
show install inactive	show install inactive	<p>Provides information about the inactive packages, if any, for all the FRUs.</p> <p>If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.</p>
show install committed	show install committed	<p>Provides information about the committed packages for all the FRUs.</p> <p>If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.</p>

Command	Syntax	Purpose
show install uncommitted	show install uncommitted	Provides information about uncommitted packages, if any, for all the FRUs. If there is a difference in the information among the FRUs, each FRU that differs from the rest of the stack is listed in a separate table.
show install rollback	show install rollback {point-id label}	Displays the package associated with a saved installation point.
show version	show version [rp-slot] [installed [user-interface] provisioned running]	Displays information about the current package, along with hardware and platform information.

Booting the Platform in Install Mode

You can install, activate, and commit a software package using a single command (one-step install) or multiple separate commands (three-step install).

If the platform is working in bundle mode, the one-step install procedure must be used to initially convert the platform from bundle mode to install mode. Subsequent installs and upgrades on the platform can be done with either one-step or three-step variants.

One-Step Installation or Converting from Bundle Mode to Install Mode



Note

- All the CLI actions (for example, add, activate, and so on) are executed on all the available FRUs.
- The configuration save prompt will appear if an unsaved configuration is detected.
- The reload prompt will appear after the second step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.
- If the prompt-level is set to None, and there is an unsaved configuration, the install fails. You must save the configuration before reissuing the command.

Use the one-step install procedure described below to convert a platform running in bundle boot mode to install mode. After the command is executed, the platform reboots in install boot mode.

Later, the one-step install procedure can also be used to upgrade the platform.

This procedure uses the **install add file activate commit** command in privileged EXEC mode to install a software package, and to upgrade the platform to a new version.

SUMMARY STEPS

1. **enable**
2. **install add file location:** *filename* [**activate commit**]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device>enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	install add file location: <i>filename</i> [activate commit] Example: Device#install add file bootflash:c8000e-universalk9_HD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SPA bin activate commit	Copies the software install package from a local or remote location (through FTP, HTTP, HTTPS, or TFTP) to the platform and extracts the individual components of the .package file into subpackages and packages.conf files. It also performs a validation and compatibility check for the platform and image versions, activates the package, and commits the package to make it persistent across reloads. The platform reloads after this command is run.
Step 3	exit Example: Device#exit	Exits privileged EXEC mode and returns to user EXEC mode.

Three-Step Installation

**Note**

- All the CLI actions (for example, add, activate, and so on) are executed on all the available FRUs.
- The configuration save prompt will appear if an unsaved configuration is detected.
- The reload prompt will appear after the install activate step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.

The three-step installation procedure can be used only after the platform is in install mode. This option provides more flexibility and control to the customer during installation.

This procedure uses individual **install add**, **install activate**, and **install commit** commands for installing a software package, and to upgrade the platform to a new version.

SUMMARY STEPS

1. **enable**
2. **install add file location:** *filename*
3. **show install summary**
4. **install activate** [**auto-abort-timer** *<time>*]

5. **install abort**
6. **install commit**
7. **install rollback to committed**
8. **install remove** {file filesystem: filename | inactive}
9. **show install summary**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device>enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	install add file location: <i>filename</i> Example: Device#install add file bootflash:c8000e-universal-k9-ED_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin	Copies the software install package from a remote location (through FTP, HTTP, HTTPS, or TFTP) to the platform, and extracts the individual components of the .package file into subpackages and packages.conf files.
Step 3	show install summary Example: Device#show install summary	(Optional) Provides an overview of the image versions and their corresponding install state for all the FRUs.
Step 4	install activate [auto-abort-timer <time>] Example: Device# install activate auto-abort-timer 120	Activates the previously added package and reloads the platform. <ul style="list-style-type: none"> When doing a full software install, do not provide a package filename. In the three-step variant, auto-abort-timer starts automatically with the install activate command; the default for the timer is 120 minutes. If the install commit command is not run before the timer expires, the install process is automatically terminated. The platform reloads and boots up with the last committed version.
Step 5	install abort Example: Device#install abort	(Optional) Terminates the software install activation and returns the platform to the last committed version. <ul style="list-style-type: none"> Use this command only when the image is in activated state, and not when the image is in committed state.
Step 6	install commit Example: Device#install commit	Commits the new package installation and makes the changes persistent over reloads.

	Command or Action	Purpose
Step 7	install rollback to committed Example: Device#install rollback to committed	(Optional) Rolls back the platform to the last committed state.
Step 8	install remove {file filesystem: filename inactive} Example: Device#install remove inactive	(Optional) Deletes software installation files. <ul style="list-style-type: none"> • file: Deletes a specific file • inactive: Deletes all the unused and inactive installation files.
Step 9	show install summary Example: Device#show install summary	(Optional) Displays information about the current state of the system. The output of this command varies according to the install commands run prior to this command.
Step 10	exit Example: Device#exit	Exits privileged EXEC mode and returns to user EXEC mode.

Upgrading in Install Mode

Use either the one-step installation or the three-step installation to upgrade the platform in install mode.

Downgrading in Install Mode

Use the **install rollback** command to downgrade the platform to a previous version by pointing it to the appropriate image, provided the image you are downgrading to was installed in install mode.

The **install rollback** command reloads the platform and boots it with the previous image.



Note The **install rollback** command succeeds only if you have not removed the previous file using the **install remove inactive** command.

Alternatively, you can downgrade by installing the older image using the **install** commands.

Terminating a Software Installation

You can terminate the activation of a software package in the following ways:

- When the platform reloads after activating a new image, the auto-abort-timer is triggered (in the three-step install variant). If the timer expires before issuing the **install commit** command, the installation process is terminated, and the platform reloads and boots with the last committed version of the software image.

Alternatively, use the **install auto-abort-timer stop** command to stop this timer, without using the **install commit** command. The new image remains uncommitted in this process.

- Using the **install abort** command returns the platform to the version that was running before installing the new software. Use this command before issuing the **install commit** command.

Configuration Examples for Installing the Software Using install Commands

The following is an example of the one-step installation or converting from bundle mode to install mode:

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
  activate commit
install_add_activate_commit: START Thu Oct 28 21:57:21 UTC 2021

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...

[OK]Modified configuration has been saved

*Oct 28 21:57:39.818: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
file
*Oct 28 21:57:39.925: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
one-shot
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bininstall_add_activate_commit:
Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.07.01.0.1515
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_lt3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_ngwic_tle1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

```
This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby

*Oct 28 22:05:49.484: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds  [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0

Building configuration...
  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

[OK]
*Oct 28 22:06:55.375: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
fileSend model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Oct 28 22:07:22 UTC 2021

Router#
*Oct 28 22:07:22.661: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.binOct
28 22:07:26.864: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action
requested

□

Press RETURN to get started!
```

The following is an example of the three-step installation:

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin

install_add: START Thu Oct 28 22:36:43 UTC 2021

*Oct 28 22:36:44.526: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
add
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bininstall_add:
Adding PACKAGE
install_add: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.07.01.0.1601
SUCCESS: install_add  Thu Oct 28 22:40:25 UTC 2021

Router#
```

```

*Oct 28 22:40:25.971: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin

Router# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS Thu Oct 28 22:09:30 Universal 2021
[0|install_op_boot(INFO, )]: cleanup_trap remote_invocation 0 operation install_op_boot
.. 0 .. 0
[1|display_install_log]: START Thu Oct 28 22:12:11 UTC 2021
[2|install_add]: START Thu Oct 28 22:36:43 UTC 2021
[2|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[2|install_add(CONSOLE, )]: Adding PACKAGE
[2|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[2|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[remote|install_add]: START Thu Oct 28 22:37:12 UTC 2021
[remote|install_add]: END SUCCESS Thu Oct 28 22:40:10 UTC 2021
[remote|install_add(INFO, )]: cleanup_trap remote_invocation 1 operation install_add .. 0
.. 0
[2|install_add(INFO, )]: Remote output from R0
[2|install_add(INFO, )]: install_add: START Thu Oct 28 22:37:12 UTC 2021
Expanding image file:
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
Verifying parameters
Expanding superpackage
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
... parameters verified
Validating package type
... package type validated
Copying package files
  c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

  c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

  c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

  c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

  c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

  c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

```

```

WARNING: A different version of provisioning file packages.conf already exists in bootflash:

WARNING: The provisioning file from the expanded bundle will be saved as
WARNING: bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_0.conf
... package files copied
SUCCESS: Finished expanding all-in-one software package.
Image file expanded
SUCCESS: install_add Thu Oct 28 22:40:10 UTC 2021
[2|install_add]: END SUCCESS Thu Oct 28 22:40:25 UTC 2021
[2|install_add(INFO, )]: cleanup_trap remote_invocation 0 operation install_add .. 0 .. 0
[3|COMP_CHECK]: START Thu Oct 28 22:40:26 UTC 2021
[3|COMP_CHECK]: END FAILED exit(1) Thu Oct 28 22:40:27 UTC 2021
[3|COMP_CHECK(INFO, )]: cleanup_trap remote_invocation 0 operation COMP_CHECK .. 1 .. 1
[4|install_activate]: START Thu Oct 28 22:42:53 UTC 2021
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate(CONSOLE, )]: Activating PACKAGE
[4|install_activate(INFO, )]: Acquiring transaction lock...
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: tmp lock does not exist: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: local_trans_lock: /bootflash/.installer/install_local_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: validate_lock: lock_duration is 7200
[4|install_activate(INFO, )]: install type stored in lock PACKAGE, install type PACKAGE,
install operation install_activate
[4|install_activate(INFO, )]: lock duration: 7200
[4|install_activate(INFO, )]: extend trans lock done.
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate( FATAL)]: Cannot proceed activate because of user input
[4|install_activate(INFO, )]: cleanup_trap remote_invocation 0 operation install_activate
.. 6 .. 0
[5|install_add]: START Thu Oct 28 22:45:48 UTC 2021
[5|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[5|install_add(CONSOLE, )]: Adding PACKAGE
[5|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[5|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[5|install_add( FATAL)]: Super package already added. Add operation not allowed. install
remove inactive can be used to discard added packages

Router# install activate
install_activate: START Thu Oct 28 23:57:57 UTC 2021
install_activate: Activating PACKAGE

*Oct 28 23:57:57.823: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
activateFollowing packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_lt3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_l0g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

```

```

/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_ngwic_tle1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

```

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---

Performing Activate on Active/Standby

```

*Oct 29 00:04:19.400: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Activate package(s) on R0

```

--- Starting list of software package changes ---

Old files list:

Modified

```
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_ngwic_tle1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

Modified

```
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

```
Modified c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
```

New files list:

Added

```
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
```

Added

```
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
```



```

    Added
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

    Added
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

    Added
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Added c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Finished list of software package changes
[1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

Send model notification for install_activate before reload
Install will reload the system now!
SUCCESS: install_activate  Fri Oct 29 00:05:09 UTC 2021

Router#
*Oct 29 00:05:09.504: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install activate PACKAGEOct 29 00:05:14.494: %PMAN-5-EXITACTION: R0/0: pvp: Process manager
is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running      : Boot ROM1
Last reset cause           : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

```

□

Press RETURN to get started!

□

```
Router# install commit
install_commit: START Fri Oct 29 00:13:58 UTC 2021
install_commit: Committing PACKAGE

--- Starting Commit ---
Performing Commit on Active/Standby

*Oct 29 00:13:59.552: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit [1] Commit package(s) on R0
[1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

SUCCESS: install_commit Fri Oct 29 00:14:03 UTC 2021

Router#
*Oct 29 00:14:03.712: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit PACKAGE
```

The following is an example of downgrading in install mode:

```
ROUTER# install activate file bootflash:c8000be-universalk9.17.06.01a.SPA.bin activate
commit

install_add_activate_commit: START Fri Dec 10 18:07:17 GMT 2021

*Dec 10 18:07:18.405 GMT: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot bootflash:c8000be-universalk9.17.06.01a.SPA.bininstall_add_activate_commit:
Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
[1] Add package(s) on R0
[1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.06.01a.0.298
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.17.06.01a.SPA.pkg
/bootflash/c8000be-mono-universalk9.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_lt3e3.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_l0g.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_prince.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_xdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ssd.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_shdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ge.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_cwan.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.17.06.01a.SPA.pkg
```

```
/bootflash/c8000be-firmware_nim_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_ngwic_tle1.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dreamliner.17.06.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby
  [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0
Building configuration...

  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

[OK]
*Dec 10 18:14:57.782 GMT: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config fileSend model notification for install_add_activate_commit before reload
/usr/binos/conf/install_util.sh: line 164: /bootflash/.prst_sync/reload_info: No such file
or directory
/usr/binos/conf/install_util.sh: line 168: /bootflash/.prst_sync/reload_info: No such file
or directory
cat: /bootflash/.prst_sync/reload_info: No such file or directory
Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Dec 10 18:15:23 GMT 2021

ROUTER#
*Dec 10 18:15:23.955 GMT: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot PACKAGE bootflash:c8000be-universalk9.17.06.01a.SPA.binDec 10 18:15:27.708:
%PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 17.3(5r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
ROUTER platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□

ROUTER#
ROUTER# show version
```

Cisco IOS XE Software, Version 17.06.01a
 Cisco IOS Software [Bengaluru], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.6.1a, RELEASE SOFTWARE (fc2)
 Technical Support: <http://www.cisco.com/techsupport>
 Copyright (c) 1986-2021 by Cisco Systems, Inc.
 Compiled Sat 21-Aug-21 03:27 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
 All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: 17.3(5r)

ROUTER uptime is 0 minutes
 Uptime for this control processor is 2 minutes
 System returned to ROM by LocalSoft
 System image file is "bootflash:packages.conf"
 Last reload reason: LocalSoft

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

Technology	Type	Technology-package Current	Technology-package Next Reboot
Smart License	Perpetual	None	None
Smart License	Subscription	None	None

The current crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco ROUTER (1RU) processor with 3747220K/6147K bytes of memory.
 Processor board ID FDO2521M27S
 Router operating mode: Autonomous
 5 Gigabit Ethernet interfaces
 2 2.5 Gigabit Ethernet interfaces
 2 Cellular interfaces
 32768K bytes of non-volatile configuration memory.
 8388608K bytes of physical memory.
 7573503K bytes of flash memory at bootflash:..
 1875361792K bytes of NVMe SSD at harddisk:..
 16789568K bytes of USB flash at usb0:..

Configuration register is 0x2102

The following is an example of terminating a software installation:

```
Router# install abort
install_abort: START Fri Oct 29 02:42:51 UTC 2021

This install abort would require a reload. Do you want to proceed? [y/n]
*Oct 29 02:42:52.789:
  %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install aborty
--- Starting Abort ---
Performing Abort on Active/Standby

  [1] Abort package(s) on R0
  [1] Finished Abort on R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort

Send model notification for install_abort before reload
Install will reload the system now!
SUCCESS: install_abort  Fri Oct 29 02:44:47 UTC 2021

Router#
*Oct 29 02:44:47.866: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install_abort PACKAGEOct 29 02:44:51.577: %PMAN-5-EXITACTION: R0/0: pvp: Process manager
is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running   : Boot ROM1
Last reset cause        : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□
```

The following are sample outputs for show commands:

show install log

```
Device# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Thu Oct 28 22:09:30 Universal 2021
```

show install summary

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
```

```

-----
C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
IMG   C    17.07.01.0.1515
-----
Auto abort timer: inactive
-----

```

show install package filesystem: filename

```

Device# show install package
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
Package: c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
Size: 831447859
Timestamp: 2021-10-23 17:08:14 UTC
Canonical path:
/bootflash/c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin

```

```

Raw disk-file SHA1sum:
5c4e7617a6c71ffbcc73dcd034ab58bf76605e3f
Header size:      1192 bytes
Package type:     30000
Package flags:    0
Header version:   3

```

```

Internal package information:
Name: rp_super
BuildTime: 2021-10-21_13.00
ReleaseDate: 2021-10-21_03.11
BootArchitecture: i686
RouteProcessor: radium
Platform: C8000BE
User: mcpre
PackageName: universalk9
Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
CardTypes:

```

```

Package is bootable from media and tftp.
Package contents:

```

```

Package:
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
Size: 2966620
Timestamp: 2021-10-21 20:10:44 UTC

```

```

Raw disk-file SHA1sum:
501d59d5f152ca00084a0da8217bf6f6b95dddb1
Header size:      1116 bytes
Package type:     40000
Package flags:    0
Header version:   3

```

```

Internal package information:
Name: firmware_nim_ge
BuildTime: 2021-10-21_13.00
ReleaseDate: 2021-10-21_03.11
BootArchitecture: none
RouteProcessor: radium
Platform: C8000BE
User: mcpre
PackageName: firmware_nim_ge
Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117

```

CardTypes:

Package is not bootable.

Package:

c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

Size: 10204252

Timestamp: 2021-10-21 20:10:43 UTC

Raw disk-file SHA1sum:

a57bed4ddecfd08af3b456f69d11aaeb962865ea

Header size: 1116 bytes

Package type: 40000

Package flags: 0

Header version: 3

Internal package information:

Name: firmware_prince

BuildTime: 2021-10-21_13.00

ReleaseDate: 2021-10-21_03.11

BootArchitecture: none

RouteProcessor: radium

Platform: C8000BE

User: mcpre

PackageName: firmware_prince

Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117

CardTypes:

Package is not bootable.

show install active

Device# show install active

[R0] Active Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

Type St Filename/Version

IMG C 17.07.01.0.1515

Auto abort timer: inactive

show install inactive

Device# show install inactive

[R0] Inactive Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

Type St Filename/Version

No Inactive Packages

show install committed

Device# show install committed

[R0] Committed Package(s) Information:

State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated & Committed, D - Deactivated & Uncommitted

Type St Filename/Version

IMG C 17.07.01.0.1515

```

-----
Auto abort timer: inactive
-----

show install uncommitted

Device# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
No Uncommitted Packages

```

Troubleshooting Software Installation Using install Commands

Problem Troubleshooting the software installation

Solution Use the following show commands to view installation summary, logs, and software versions.

- **show install summary**
- **show install log**
- **show version**
- **show version running**

Problem Other installation issues

Solution Use the following commands to resolve installation issue:

- **dir <install directory>**
- **more location:packages.conf**
- **show tech-support install**: this command automatically runs the **show** commands that display information specific to installation.
- **request platform software trace archive target bootflash <location>**: this command archives all the trace logs relevant to all the processes running on the system since the last reload, and saves this information in the specified location.



CHAPTER 11

Software Upgrade Processes

If you want to upgrade the ROMMON and IOS at the same time, perform the steps given below:

- Copy the XE image to the router and configure the boot system to point to the new image.
- Copy the ROMMON package to the router and perform the ROMMON upgrade.
- Reload the router and verify that it boots to the IOS prompt on the new XE image.
- Verify that the new ROMMON image was successfully installed using a show platform.



CHAPTER 12

Factory Reset

This chapter describes Factory Reset feature and how it can be used to protect or restore a router to an earlier, fully functional state.

- [Feature Information for Factory Reset, on page 135](#)
- [Information About Factory Reset, on page 135](#)
- [Software and Hardware Support for Factory Reset, on page 137](#)
- [Prerequisites for Performing Factory Reset, on page 137](#)
- [Restrictions for Performing a Factory Reset, on page 138](#)
- [When to Perform Factory Reset, on page 138](#)
- [How to Perform a Factory Reset, on page 138](#)
- [What Happens after a Factory Reset, on page 139](#)

Feature Information for Factory Reset

Table 19: Feature Information for Factory Reset

Feature Name	Releases	Feature Information
Factory Reset	Cisco IOS XE Fuji 16.7.1	This feature was introduced.
Option to retain RUM reports, SLR, and HSEC key using the factory-reset keep-licensing-info command	Cisco IOS XE Bengaluru 17.5.1	This feature was introduced.
Secure Factory Reset	Cisco IOS XE Bengaluru 17.6.1	Added the factory-reset all secure command.

Information About Factory Reset

Factory Reset is a process of clearing the current running and start-up configuration information on a device, and resetting the device to an earlier, fully-functional state.

The factory reset process uses the **factory-reset all** command to take backup of existing configuration, and then reset the router to an earlier, fully functional state. In a high availability setup, the factory reset process

is executed on the active Route Processor (RP), and then synchronized to the standby RP. The duration of the factory reset process is dependent on the storage size of the router. It can vary between 30 minutes on a C8500 consolidated platform, and up to 3 hours on a high availability setup.

From Cisco IOS XE Bengaluru 17.6 release and later, you can use the **factory-reset all secure** command to reset the router and securely clear the files stored in the bootflash memory.

Table 20: Data Erased or Retained during Factory Reset

Command Name	Data Erased	Data Retained
factory-reset all secure	Non-volatile random-access memory (NVRAM) data	Data from remote field-replaceable units (FRUs).
	OBFL (Onboard Failure Logging) logs	Value of configuration register
	Licenses	Contents of USB
	User data, startup, and running configuration	Credentials (Secure Unique Device Identifier [SUDI] certificates, public key infrastructure (PKI) keys, and FIPS-related keys)
	ROMMON variables	
	All writeable file systems and personal data. Note If the current boot image is a remote image or stored on a USB, NIM-SSD, or such, ensure that you take a backup of the image before performing factory reset.	

Command Name	Data Erased	Data Retained
factory-reset keep-licensing-info	<ul style="list-style-type: none"> • License Boot level configuration • Throughput level configuration • Smart license transport type • Smart license URL data 	<ul style="list-style-type: none"> • Real User Monitoring (RUM) Reports (open/unacknowledged license usage report) • Usage reporting details (last ACK received, next ACK scheduled, last/next report push) • Unique Device Identification (UDI) trust codes • Customer policy received from CSSM • SLAC, SLR authorization codes return codes • Factory installed purchase information

After the factory reset process is complete, the router reboots to ROMMON mode. If you have the zero-touch provisioning (ZTP) capability setup, after the router completes the factory reset procedure, the router reboots with ZTP configuration.

Software and Hardware Support for Factory Reset

- This feature is supported on all Cisco Catalyst 8500 and 8500L Series Edge Platforms, Cisco Catalyst 8500 and 8500L Series Route Processor 2 (RP2), and Cisco Catalyst 8500 and 8500L Series Route Processor 3 (RP3).
- Factory Reset process is supported on standalone routers as well as on routers configured for high availability.

Prerequisites for Performing Factory Reset

- Ensure that all the software images, configurations and personal data is backed up before performing factory reset.
- Ensure that there is uninterrupted power supply when factory reset is in progress.
- The factory reset process takes a backup of the boot image if the system is booted from an image stored locally (bootflash or hard disk). If the current boot image is a remote image or stored on a USB, NIM-SSD or such, ensure that you take a backup of the image before performing factory reset.
- The **factory-reset all secure** command erases all files, including the boot image, even if the image is stored locally. If the current boot image is a remote image or stored on a USB, NIM-SSD, or such, ensure that you take a backup of the image before performing secure factory reset.

- Ensure that ISSU/ISSD (In- Service Software Upgrade or Downgrade) is not in progress before performing factory reset.

Restrictions for Performing a Factory Reset

- Any software patches that are installed on the router are not restored after the factory reset operation.
- If the factory reset command is issued through a Virtual Teletype (VTY) session, the session is not restored after the completion of the factory reset process.

When to Perform Factory Reset

- Return Material Authorization (RMA): If a router is returned back to Cisco for RMA, it is important that all sensitive information is removed.
- Router is compromised: If the router data is compromised due to a malicious attack, the router must be reset to factory configuration and then reconfigured once again for further use.
- Repurposing: The router needs to be moved to a new topology or market from the existing site to a different site.

How to Perform a Factory Reset

Before you begin

Refer Table 2 to determine which information is going to be deleted and retained. Based on the information you require, execute the appropriate command mentioned below.

Step 1 Log in to a Cisco Catalyst 8500 or 8500L device.

Important If the current boot image is a remote image or is stored in a USB or a NIM-SSD, ensure that you take a backup of the image before starting the factory reset process.

Step 2 This step is divided into two parts (a and b). If you need to retain the licensing information while performing the **factory-reset** command, follow step 2. a. If you do not need to retain the licensing information and want all the data to be erased, perform step 2. b.

a) Execute **factory-reset keep-licensing-info** command to retain the licensing data.

The system displays the following message when you use the **factory-reset keep-licensing-info** command:

```
Router# factory-reset keep-licensing-info
```

```
The factory reset operation is irreversible for Keeping license usage. Are you sure? [confirm]
This operation may take 20 minutes or more. Please do not power cycle.
```

```
Dec 1 20:58:38.205: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process exit with
reload chassis code
/bootflash failed to mount
```

```
Dec 01 20:59:44.264: Factory reset operation completed.
Initializing Hardware ...
```

```
Current image running: Boot ROM1
```

```
Last reset cause: LocalSoft
```

```
ISR4331/K9 platform with 4194304 Kbytes of main memory
rommon 1
```

- b) Execute the **factory-reset all secure 3-pass** command to securely erase all data.

The system displays the following message when you use the **factory-reset all secure 3-pass** command:

```
Router# factory-reset all secure 3-pass
```

```
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
This operation may take hours. Please do not power cycle.
```

```
*Jun 19 00:53:33.385: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Jun
19 00:53:42.856: %PMAN-5-EXITACTION:
```

```
Enabling factory reset for this reload cycle
```

```
Jun 19 00:54:06.914: Factory reset secure operation. Write 0s. Please do not power cycle.
```

```
Jun 19 01:18:36.040: Factory reset secure operation. Write 1s. Please do not power cycle.
```

```
Jun 19 01:43:49.263: Factory reset secure operation. Write random. Please do not power cycle.
```

```
Jun 19 02:40:29.770: Factory reset secure operation completed.
```

```
Initializing Hardware ....
```

Step 3 Enter **confirm** to proceed with the factory reset.

Note The duration of the factory reset process depends on the storage size of the router. It can extend between 30 minutes and up to 3 hours on a high availability setup. If you want to quit the factory reset process, press the **Escape** key.

What Happens after a Factory Reset

After the factory reset is successfully completed, the router boots up. However, before the factory reset process started, if the configuration register was set to manually boot from ROMMON, the router stops at ROMMON.

After you configure Smart Licensing, execute the **#show license status** command, to check whether Smart Licensing is enabled for your instance.



Note If you had Specific License Reservation enabled before you performed the factory reset, use the same license and enter the same license key that you received from the smart agent.



CHAPTER 13

High Availability Overview

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

The unique hardware and software architecture of the Cisco 8500 Series Catalyst Edge Platform is designed to maximize router uptime during any network event, and thereby provide maximum uptime and resilience within any network scenario.

This guide covers the aspects of High Availability that are unique to the Cisco 8500 Series Catalyst Edge Platform. It is not intended as a comprehensive guide to High Availability, nor is it intended to provide information on High Availability features that are available on other Cisco routers that are configured and implemented identically on the Cisco 8500 Series Catalyst Edge Platform. The Cisco IOS feature documents and guides should be used in conjunction with this chapter to gather information about High Availability-related features that are available on multiple Cisco platforms and work identically on the Cisco 8500 Series Catalyst Edge Platform.

- [Finding Feature Information in This Module, on page 141](#)
- [Contents, on page 142](#)
- [Software Redundancy on the Cisco 8500 Series Catalyst Edge Platform, on page 142](#)
- [Stateful Switchover, on page 143](#)
- [IPsec Failover, on page 144](#)
- [Bidirectional Forwarding Detection, on page 144](#)

Finding Feature Information in This Module

Your software release might not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

This section discusses various aspects of High Availability on the Cisco 8500 Series Catalyst Edge Platform and contains the following sections:

Software Redundancy on the Cisco 8500 Series Catalyst Edge Platform

This section covers the following topics:

Software Redundancy Overview

On the Cisco 8500 Series Catalyst Edge Platform, IOS runs as one of many processes within the operating system. This is different than on traditional Cisco IOS, where all processes are run within Cisco IOS. See the [“IOS as a Process” section on page 2-7](#) for more information regarding IOS as a process on the Cisco 8500 Series Catalyst Edge Platform.

This architecture allows for software redundancy opportunities that are not available on other platforms that run Cisco IOS software. Specifically, a standby IOS process can be available on the same Route Processor as the active IOS process. This standby IOS process can be switched to in the event of an IOS failure.

On the Cisco 8500 Series Catalyst Edge Platform, the second IOS process can run only on the standby Route Processor.

Configuring two Cisco IOS processes

On the Cisco 8500 Series Catalyst Edge Platform, Cisco IOS runs as one of the many processes. This architecture supports software redundancy opportunities. Specifically, a standby Cisco IOS process is available on the same Route Processor as the active Cisco IOS process. In the event of a Cisco IOS failure, the system switches to the standby Cisco IOS process.

SUMMARY STEPS

1. enable
2. **configure terminal**
3. redundancy
4. mode SSO
5. **exit**
6. reload

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example:	<ul style="list-style-type: none">• Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	redundancy Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 4	mode SSO Example: Router(config)# mode SSO	Configures SSO. When this command is entered, the redundant supervisor engine is reloaded and begins to work in SSO mode.
Step 5	exit Example: Router(config)# exit Example: Router #	Exits configuration mode and returns to global configuration mode.
Step 6	reload Example: Router # reload	Reloads IOS.

Example

```
Router# configure terminal
Router(config)# redundancy
Router(config)# mode SSO
Router(config)# exit
Router# reload
```

Stateful Switchover

On the Cisco 8500 Series Catalyst Edge Platform, Stateful Switchover (SSO) can be used to enable a second IOS process.

Stateful Switchover is particularly useful in conjunction with Nonstop Forwarding. SSO allows the dual IOS processes to maintain state at all times, and Nonstop Forwarding lets a switchover happen seamlessly when a switchover occurs

For additional information on NSF/SSO, see the [Cisco Nonstop Forwarding](#) document.

SSO-Aware Protocol and Applications

SSO-supported line protocols and applications must be SSO-aware. A feature or protocol is SSO-aware if it maintains, either partially or completely, undisturbed operation through an RP switchover. State information for SSO-aware protocols and applications is synchronized from active to standby to achieve stateful switchover for those protocols and applications.

The dynamically created state of SSO-unaware protocols and applications is lost on switchover and must be reinitialized and restarted on switchover.

To see which protocols are SSO-aware on your router, use the following commands **show redundancy client** or **show redundancy history**.

IPsec Failover

IPsec failover is a feature that increases the total uptime (or availability) of a customer's IPsec network. Traditionally, this is accomplished by employing a redundant (standby) router in addition to the original (active) router. If the active router becomes unavailable for any reason, the standby router takes over the processing of IKE and IPsec. IPsec failover falls into two categories: stateless failover and stateful failover.

The IPsec on the Cisco 8500 Series Catalyst Edge Platform supports only stateless failover. Stateless failover uses protocols such as the Hot Standby Router Protocol (HSRP) to provide primary to secondary cutover and also allows the active and standby VPN gateways to share a common virtual IP address.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable.

On the Cisco 8500 Series Catalyst Edge Platform, BFD for IPv4 Static Routes and BFD for BGP are fully supported.

For more information on BFD, see the [Bidirectional Forwarding Detection](#) document.



CHAPTER 14

Using the Management Ethernet Interface

The Cisco 8500 Series Catalyst Edge Platform have one Gigabit Ethernet Management Ethernet interface.

- [Finding Feature Information in This Module, on page 145](#)
- [Contents, on page 145](#)
- [Gigabit Ethernet Management Interface Overview, on page 145](#)
- [Gigabit Ethernet Port Numbering, on page 146](#)
- [IP Address Handling in ROMmon and the Management Ethernet Port, on page 146](#)
- [Gigabit Ethernet Management Interface VRF, on page 146](#)
- [Common Ethernet Management Tasks, on page 147](#)

Finding Feature Information in This Module

Your software release might not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

This guide covers the following topics:

Gigabit Ethernet Management Interface Overview

The purpose of this interface is to allow users to perform management tasks on the router; it is basically an interface that should not and often cannot forward network traffic but can otherwise access the router, often via Telnet and SSH, and perform most management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when the SPA interfaces are inactive.

The following aspects of the Management Ethernet interface should be noted:

- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The Ethernet Management Interface cannot be used as a Lawful Intercept MD source interface.

- The Management Ethernet interface is part of its own VRF. This is discussed in more detail in the [Gigabit Ethernet Management Interface VRF, on page 146](#).

Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

The port can be accessed in configuration mode like any other port on the Cisco 8500 Series Catalyst Edge Platform:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

IP Address Handling in ROMmon and the Management Ethernet Port

On the Cisco 8500 Series Catalyst Edge Platform, IP addresses can be configured in ROMmon (the **IP_ADDRESS=** and **IP_SUBNET_MASK=** commands) and through the use of the IOS command-line interface (the **ip address** command in interface configuration mode).

Assuming the IOS process has not begun running on the Cisco 8500 Series Catalyst Edge Platform, the IP address that was set in ROMmon acts as the IP address of the Management Ethernet interface. In cases where the IOS process is running and has taken control of the Management Ethernet interface, the IP address specified when configuring the Gigabit Ethernet 0 interface in the IOS CLI becomes the IP address of the Management Ethernet interface. The ROMmon-defined IP address is only used as the interface address when the IOS process is inactive.

For this reason, the IP addresses specified in ROMmon and in the IOS CLI can be identical and the Management Ethernet interface will function properly in single RP configurations.

Gigabit Ethernet Management Interface VRF

The Gigabit Ethernet Management interface is automatically part of its own VRF. This VRF, which is named “Mgmt-intf,” is automatically configured on the Cisco 8500 Series Catalyst Edge Platform and is dedicated to the Management Ethernet interface; no other interfaces can join this VRF. Therefore, this VRF does not participate in the MPLS VPN VRF or any other network-wide VRF. The Mgmt-intf VRF supports loopback interface.

Placing the management ethernet interface in its own VRF has the following effects on the Management Ethernet interface:

- Many features must be configured or used inside the VRF, so the CLI may be different for certain Management Ethernet functions on the Cisco 8500 Series Catalyst Edge Platform than on Management Ethernet interfaces on other routers.
- Prevents transit traffic from traversing the router. Because all built-in port and the Management Ethernet interface are automatically in different VRFs, no transit traffic can enter the Management Ethernet interface and leave a built-in port, or vice versa.

- Improved security of the interface. Because the Mgmt-intf VRF has its own routing table as a result of being in its own VRF, routes can only be added to the routing table of the Management Ethernet interface if explicitly entered by a user.

The Management Ethernet interface VRF supports both IPv4 and IPv6 address families.

Common Ethernet Management Tasks

Because users can perform most tasks on a router through the Management Ethernet interface, many tasks can be done by accessing the router through the Management Ethernet interface.

This section documents tasks that might be common or slightly tricky on the Cisco 8500 Series Catalyst Edge Platform. It is not intended as a comprehensive list of all tasks that can be done using the Management Ethernet interface.

This section covers the following processes:

Viewing the VRF Configuration

The VRF configuration for the Management Ethernet interface is viewable using the **show running-config vrf** command.

This example shows the default VRF configuration:

```
Router# show running-config vrf
Building configuration...
Current configuration : 351 bytes
vrf definition Mgmt-intf
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
(some output removed for brevity)
```

Viewing Detailed VRF Information for the Management Ethernet VRF

To see detailed information about the Management Ethernet VRF, enter the **show vrf detail Mgmt-intf** command:

```
Router# show vrf detail Mgmt-intf
```

Setting a Default Route in the Management Ethernet Interface VRF

To set a default route in the Management Ethernet Interface VRF, enter the following command

ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 next-hop-IP-address

Setting the Management Ethernet IP Address

The IP address of the Management Ethernet port is set like the IP address on any other interface.

Below are two simple examples of configuring an IPv4 address and an IPv6 address on the Management Ethernet interface.

IPv4 Example

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address
A.B.C.D A.B.C.D
```

IPv6 Example

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ipv6 address X:X:X:X::X
```

Telnetting over the Management Ethernet Interface

Telnetting can be done through the VRF using the Management Ethernet interface.

In the following example, the router telnets to 172.17.1.1 through the Management Ethernet interface VRF:

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

Pinging over the Management Ethernet Interface

Pinging other interfaces using the Management Ethernet interface is done through the VRF.

In the following example, the router pings the interface with the IP address of 172.17.1.1 through the Management Ethernet interface:

```
Router# ping vrf Mgmt-intf 172.17.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Copy Using TFTP or FTP

To copy a file using TFTP through the Management Ethernet interface, the **ip tftp source-interface GigabitEthernet 0** command must be entered before entering the **copy tftp** command because the **copy tftp** command has no option of specifying a VRF name.

Similarly, to copy a file using FTP through the Management Ethernet interface, the **ip ftp source-interface GigabitEthernet 0** command must be entered before entering the **copy ftp** command because the **copy ftp** command has no option of specifying a VRF name.

TFTP Example

```
Router(config)# ip tftp source-interface gigabitEthernet 0
```

FTP Example

```
Router(config)# ip ftp source-interface gigabitEthernet 0
```

NTP Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server over the Management Ethernet interface, enter the **ntp server vrf Mgmt-intf** command and specify the IP address of the device providing the update.

The following CLI provides an example of this procedure.

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

SYSLOG Server

To specify the Management Ethernet interface as the source IP or IPv6 address for logging purposes, enter the **logging host <ip-address> vrf Mgmt-intf** command.

The following CLI provides an example of this procedure.

```
Router(config)# logging host <ip-address> vrf Mgmt-intf
```

SNMP-Related Services

To specify the Management Ethernet interface as the source of all SNMP trap messages, enter the **snmp-server source-interface traps gigabitEthernet 0** command.

The following CLI provides an example of this procedure:

```
Router(config)# snmp-server source-interface traps gigabitEthernet 0
```

Domain Name Assignment

The IP domain name assignment for the Management Ethernet interface is done through the VRF.

To define the default domain name as the Management Ethernet VRF interface, enter the **ip domain-name vrf Mgmt-intf domain** command.

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

DNS service

To specify the Management Ethernet interface VRF as a name server, enter the **ip name-server vrf Mgmt-intf IPv4-or-IPv6-address** command.

```
Router(config)# ip name-server vrf Mgmt-intf  
IPv4-or-IPv6-address
```

RADIUS or TACACS+ Server

To group the Management VRF as part of a AAA server group, enter the **ip vrf forward Mgmt-intf** command when configuring the AAA server group.

The same concept is true for configuring a TACACS+ server group. To group the Management VRF as part of a TACACS+ server group, enter the **ip vrf forwarding Mgmt-intf** command when configuring the TACACS+ server group.

RADIUS Server Group Configuration

```
Router(config)# aaa group server radius hello  
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

TACACS+ Server Group Example

```
outer(config)# aaa group server tacacs+ hello  
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

VTY lines with ACL

To ensure an access control list (ACL) is attached to vty lines that are and are not using VRF, use the **vrf-also** option when attaching the ACL to the vty lines.

```
Router(config)# line vty 0 4  
Router(config-line)# access-class 90 in vrf-also
```



CHAPTER 15

Configuring Bridge Domain Interfaces

The Cisco 8500 Series Catalyst Edge Platform support the bridge domain interface (BDI) feature for packaging Layer 2 Ethernet segments into Layer 3 IP.

- [Restrictions for Bridge Domain Interfaces, on page 151](#)
- [Information About Bridge Domain Interface, on page 152](#)
- [Configuring Bridge-Domain Virtual IP Interface, on page 160](#)

Restrictions for Bridge Domain Interfaces

The following are the restrictions pertaining to bridge domain interfaces:

- Only 4096 bridge domain interfaces are supported per system.
- For a bridge domain interface, the maximum transmission unit (MTU) size can be configured between 1500 and 9216 bytes.
- Bridge domain interfaces support only the following features:
 - IPv4 Multicast
 - QoS marking and policing. Shaping and queuing are not supported
 - IPv4 VRF
 - IPv6 unicast forwarding
 - Dynamic routing such as BGP, OSPF, EIGRP, RIP, IS-IS, and STATIC
 - Hot Standby Router Protocol (HSRP)
 - Virtual Router Redundancy Protocol (VRRP) from IOS XE 3.8.0 onwards.
- Bridge domain interfaces do not support the following features:
 - PPP over Ethernet (PPPoE)
 - Bidirectional Forwarding Detection (BFD) protocol
 - QoS
 - Network-Based Application Recognition (NBAR) or Advanced Video Coding (AVC)

Information About Bridge Domain Interface

Bridge domain interface is a logical interface that allows bidirectional flow of traffic between a Layer 2 bridged network and a Layer 3 routed network traffic. Bridge domain interfaces are identified by the same index as the bridge domain. Each bridge domain represents a Layer 2 broadcast domain. Only one bridge domain interface can be associated with a bridge domain.

Bridge domain interface supports the following features:

- IP termination
- Layer 3 VPN termination
- Address Resolution Protocol (ARP), G-ARP, and P-ARP handling
- MAC address assignment

Prior to configuring a bridge domain interface, you must understand the following concepts:

- Ethernet Virtual Circuit Overview
- Bridge Domain Interface Encapsulation
- Assigning a MAC Address
- Support for IP Protocols
- Support for IP Forwarding
- Packet Forwarding
- Bridge Domain Interface Statistics

Ethernet Virtual Circuit Overview

An Ethernet Virtual Circuit (EVC) is an end-to-end representation of a single instance of a Layer 2 service that is offered by a provider. It embodies the different parameters on which the service is being offered. In the Cisco EVC Framework, the bridge domains are made up of one or more Layer 2 interfaces known as service instances. A service instance is the instantiation of an EVC on a given port on a given router. Service instance is associated with a bridge domain based on the configuration.

An incoming frame can be classified as service instance based on the following criteria:

- Single 802.1Q VLAN tag, priority-tagged, or 802.1ad VLAN tag
- Both QinQ (inner and outer) VLAN tags, or both 802.1ad S-VLAN and C-VLAN tags
- Outer 802.1p CoS bits, inner 802.1p CoS bits, or both
- Payload Ethernet type (five choices are supported: IPv4, IPv6, PPPoE-all, PPOE-discovery, and PPPoE-session)

Service instance also supports alternative mapping criteria:

- Untagged—Mapping to all the frames lacking a 802.1Q or 802.1ad header
- Default—Mapping to all the frames

Bridge Domain Interface Encapsulation

Security Group classification includes both Source and Destination Group, which is specified by source SGT and DGT. SGT Based PBR feature provides the PBR route-map match clause for SGT/DGT based packet classification. SGT Based PBR feature supports configuration of unlimited number of tags, but it is recommended to configure the tags based on memory available in the platform.

An EVC provides the ability to employ different encapsulations on each Ethernet flow point (EFP) present in a bridge domain. A BDI egress point may not be aware of the encapsulation of an egress packet because the packet may have egressed from one or more EFPs with different encapsulations.

In a bridge domain, if all the EFPs have different encapsulations, the BDI must be untagged (using the `no 802.1Q` tag). Encapsulate all the traffic in the bridge domain (popped or pushed) at the EFPs. Configure rewrite at each EFP to enable encapsulation of the traffic on the bridge domain.

In a bridge domain, if all the EFPs have the same encapsulation, configure the encapsulations on the BDI using the encapsulation command. Enabling encapsulation at the BDI ensures effective pushing or popping of tags, thereby eliminating the need for configuring the rewrite command at the EFPs. For more information on configuring the encapsulations on the BDI, see the [How to Configure a Bridge Domain Interface](#).

Assigning a MAC Address

All the bridge domain interfaces on the Cisco Catalyst 8500 Series Edge Platforms share a common MAC address. The first bridge domain interface on a bridge domain is allocated a MAC address. Thereafter, the same MAC address is assigned to all the bridge domain interfaces that are created in that bridge domain.



Note You can configure a static MAC address on a bridge domain interface using the **mac-address** command.

Support for IP Protocols

Bridge domain interfaces enable the Cisco 8500 Series Catalyst Edge Platform to act as a Layer 3 endpoint on the Layer 2 bridge domain for the following IP-related protocols:

- ARP
- DHCP
- HTTP
- ICMP
- NTP
- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

Support for IP Forwarding

Bridge domain interface supports the following IP forwarding features:

- IPv4 input and output access control lists (ACL)
- IPv4 input and output QoS policies. The operations supported for the input and output service policies on a bridge domain interface are:
 - Classification
 - Marking

- Policing
- IPv4 L3 VRFs

Packet Forwarding

A bridge domain interface provides bridging and forwarding services between the Layer 2 and Layer 3 network infrastructure.

Layer 2 to Layer 3

During a packet flow from a Layer 2 network to a Layer 3 network, if the destination MAC address of the incoming packet matches the bridge domain interface MAC address, or if the destination MAC address is a multicast address, the packet or a copy of the packet is forwarded to the bridge domain interface.



Note MAC address learning cannot be performed on the bridge domain interface.

Layer 3 to Layer 2

When a packet arrives at a Layer 3 physical interface of a router, a route lookup action is performed. If route lookup points to a bridge domain interface, then the bridge domain interface adds the layer 2 encapsulation and forwards the frame to the corresponding bridge domain. The byte counters are updated.

During a Layer 2 lookup on a bridge domain to which the bridge domain interface belongs, the bridge domain forwards the packets to the correct service instance based on the destination MAC address.

Link States of a Bridge Domain and a Bridge Domain Interface

Bridge domain interface acts as a routable IOS interface on Layer 3 and as a port on a bridge domain. Both bridge domain interfaces and bridge domains operate with individual administrative states.

Shutting down a bridge domain interface stops the Layer 3 data service, but does not override or impact the state of the associated bridge domain.

Shutting down a bridge domain stops Layer 2 forwarding across all the associated members including service instances and bridge domain interfaces. The associated service instances influence operational state of a bridge domain. Bridge domain interface cannot be operational unless one of the associated service instances is up.



Note Because a bridge domain interface is an internal interface, the operational state of bridge domain interface does not affect the bridge domain operational state.

BDI Initial State

The initial administrative state of a BDI depends on how the BDI is created. When you create a BDI at boot time in the startup configuration, the default administrative state for the BDI is up. It will remain in this state unless the startup configuration includes the shutdown command. This behavior is consistent with all the other interfaces. When you create a BDI dynamically at command prompt, the default administrative state is down.

BDI Link State

A BDI maintains a link state that comprises of three states: administratively down, operationally down, and up. The link state of a BDI is derived from two independent inputs: the BDI administrative state set by the corresponding users and the fault indication state from the lower levels of the interface states. It defines a BDI link state based on the state of the two inputs.

Fault Indication State	BDI Admin{start straddle 2 columns}{end straddle 2 columns}	
{start emdash} {end emdash}	Shutdown	No Shutdown
No faults asserted	Admin-down	Up
At least one fault asserted	Admin-down	Operationally-Down

Bridge Domain Interface Statistics

For virtual interfaces, such as the bridge domain interface, protocol counters are periodically queried from the QFP.

When packets flow from a Layer 2 bridge domain network to a Layer 3 routing network through the bridge domain interface, the packets are treated as bridge domain interface input packets and bytes. When packets arrive at a Layer 3 interface and are forwarded through the bridge domain interface to a Layer 2 bridge domain, the packets are treated as output packets and bytes, and the counters are updated accordingly.

A BDI maintains a standard set of Layer 3 packet counters as the case with all Cisco IOS interfaces. Use the `show interface` command to view the Layer 3 packet counters.

The convention of the counters is relative to the Layer 3 cloud. For example, input refers to the traffic entry to the Layer 3 cloud from the Layer 2 BD, while output refers to the traffic exit from the Layer 3 cloud to the Layer 2 BD.

Use the **`show interfaces accounting`** command to display the statistics for the BDI status. Use the **`show interface <if-name>`** command to display the overall count of the packets and bytes that are transmitted and received.

Creating or Deleting a Bridge Domain Interface

When you define an interface or subinterface for a Cisco IOS router, you name it and specify how it is assigned an IP address. You can create a bridge domain interface before adding a bridge domain to the system. This new bridge domain interface will be activated after the associated bridge domain is configured.



Note When a bridge domain interface is created, a bridge domain is automatically created.

When you create the bridge domain interface and the bridge domain, the system maintains the required associations for mapping the bridge domain-bridge domain interface pair.

The mapping of bridge domain and bridge domain interface is maintained in the system. The bridge domain interface uses the index of the associated bridge domain to show the association.

Bridge Domain Interface Scalability

The following table lists the bridge domain interface scalability numbers, based on the type of Cisco 8500 Series Catalyst Edge Platform Forwarding Processors.

Table 21: Bridge Domain Interface Scalability Numbers Based on the Type of Cisco 8500 Series Catalyst Edge Platform Forwarding Processor

Description
Maximum bridge domain interfaces per router

Bridge-Domain Virtual IP Interface

The Virtual IP Interface (VIF) feature helps to associate multiple BDI interfaces with a BD instance. The BD-VIF interface inherits all the existing L3 features of IOS logical IP interface.



Note You must configure every BD-VIF interface with a unique MAC address and it should belong to a different VRF.

The Virtual IP Interface (VIF) feature has the following limitations:

- BD-VIF interface does not support IP multicast.
- Number of BD-VIF interfaces with automatically generated MAC address varies on the basis of platforms.
- BD-VIF Interface does not support MPLS.
- The maximum number of BD-VIF interfaces per bridge-domain and the total number of BD-VIF interface for per system vary based on the type of platforms.

The maximum number of BD-VIF supported on Cisco Catalyst 8500 Series Edge Platforms are:

- C8500-12X4QC supports maximum 100 BD-VIF for a Bridge Domain
- C8500-12X (support maximum 16 BD-VIF for a Bridge Domain)

From Cisco IOS XE 17.7 release, BD-VIF supports Flexible Netflow (FNF).

How to Configure a Bridge Domain Interface

To configure a bridge domain interface, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface BDI** *{interface number}*
4. **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*
5. Do one of the following:

6. **match security-group destination tag** *sgt-number*
7. **mac address** *{mac-address}*
8. **no shut**
9. **shut**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface BDI <i>{interface number}</i> Example: <pre>Router(config-if)# interface BDI3</pre>	Specifies a bridge domain interface on a Cisco 8500 Series Catalyst Edge Platform.
Step 4	encapsulation <i>encapsulation dot1q <first-tag> [second-dot1q <second-tag>]</i> Example: <pre>Router(config-if)# encapsulation dot1Q 1 second-dot1q 2</pre>	Defines the encapsulation type. The example shows how to define dot1q as the encapsulation type.
Step 5	Do one of the following: Example: ip address <i>ip-address mask</i> Example: Example: ipv6 address <i>{X:X:X:X::X link-local X:X:X:X::X/prefix [anycast eui-64] autoconfig [default]}</i> Example: <pre>Router(config-if)# ip address 2.2.2.1 255.255.255.0</pre> Example: Example:	Specifies either the IPv4 or IPv6 address for the bridge domain interface.

Example

	Command or Action	Purpose
	Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64	
Step 6	match security-group destination tag sgt-number Example: Router(config-route-map)# match security-group destination tag 150	Configures the value for security-group destination security tag.
Step 7	mac address {mac-address} Example: Router(config-if)# mac-address 1.1.3	Specifies the MAC address for the bridge domain interface.
Step 8	no shut Example: Router(config-if)# no shut	Enables the bridge domain interface on the Cisco 8500 Series Catalyst Edge Platform.
Step 9	shut Example: Router(config-if)# shut	Disables the bridge domain interface on the Cisco 8500 Series Catalyst Edge Platform.

Example

The following example shows the configuration of a bridge domain interface at IP address 2.2.2.1 255.255.255.0:

```
Router# configure terminal
Router(config)# interface BDI3
Router(config-if)# encapsulation dot1q 1 second-dot1q 2
Router(config-if)# ip address 2.2.2.1 255.255.255.0
Router(config-if)# mac-address 1.1.3
Router(config-if)# no shut
Router(config-if)# exit
```

Displaying and Verifying Bridge Domain Interface Configuration

SUMMARY STEPS

1. enable
2. show interfaces bdi
3. show platform software interface fp active name
4. show platform hardware qfp active interface if-name
5. debug platform hardware qfp feature
6. platform trace runtime process forwarding-manager module

7. platform trace boottime process forwarding-manager module interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	show interfaces bdi Example: <pre>Router# show interfaces BDI3</pre>	Displays the configuration summary of the corresponding BDI.
Step 3	show platform software interface fp active name Example: <pre>Router# show platform software interface fp active name BDI4</pre>	Displays the bridge domain interface configuration in a Forwarding Processor.
Step 4	show platform hardware qfp active interface if-name Example: <pre>Router# show platform hardware qfp active interface if-name BDI4</pre>	Displays the bridge domain interface configuration in a data path.
Step 5	debug platform hardware qfp feature Example: <pre>Router# debug platform hardware qfp active feature l2bd client all</pre>	The selected CPP L2BD Client debugging is on.
Step 6	platform trace runtime process forwarding-manager module Example: <pre>Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info</pre>	Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Forwarding Manager process.
Step 7	platform trace boottime process forwarding-manager module interfaces Example: <pre>Router(config)# platform trace boottime slot</pre>	Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Route Processor Forwarding Manager process during bootup.

	Command or Action	Purpose
	R0 bay 1 process forwarding-manager forwarding-manager level max	

What to do next

For additional information on the commands and the options available with each command, see the Cisco IOS Configuration Fundamentals Command Reference Guide located at:

{start hypertext}http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html{end hypertext}

Configuring Bridge-Domain Virtual IP Interface

```
enable
configure terminal
[no] interface BD-VIF interface-number
    [[no] vrf forwarding vrf-name]
    [[no] mac address mac-address]
    [[no] ip address ip-address mask]
    [[no] ipv6 address {X:X:X:X::X link-local | X:X:X:X:X/prefix [anycast | eui-64] | autoconfig [default]}]]
exit
```

To delete BD-VIF interface, use the 'no' form of the command.

Associating VIF Interface with a Bridge Domain

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

Verifying Bridge-Domain Virtual IP Interface

All existing show commands for interface and IP interface can be used for the BD-VIF interface.

show interface bd-vif *bd-vif-id*

show ip interface bd-vif *bd-vif-id*

show bd-vif interfaces in fman-fp

show pla sof inter fp ac brief | i BD_VIF

Example Configuration Bridge-Domain Virtual IP Interface

Detail sample:

```
interface Port-channell
mtu 9000
no ip address
```

```
!Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channell service-instance 1756
member bd-vif5001
member bd-vif5002
```




CHAPTER 16

Packet Trace

First Published: August 03, 2016

The Packet-Trace feature provides a detailed understanding of how data packets are processed by the Cisco IOS XE platform, and thus helps customers to diagnose issues and troubleshoot them more efficiently. This module provides information about how to use the Packet-Trace feature.

- [Information About Packet Trace, on page 163](#)
- [Usage Guidelines for Configuring Packet Trace, on page 164](#)
- [Configuring Packet Trace, on page 164](#)
- [Configuring Packet Tracer with UDF Offset , on page 166](#)
- [Displaying Packet-Trace Information, on page 169](#)
- [Removing Packet-Trace Data, on page 170](#)
- [Configuration Examples for Packet Trace , on page 170](#)
- [Additional References, on page 177](#)
- [Feature Information for Packet Trace, on page 178](#)

Information About Packet Trace

The Packet-Trace feature provides three levels of inspection for packets: accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet processing capability. However, Packet Trace limits inspection to packets that match the debug platform condition statements, and is a viable option even under heavy-traffic situations in customer environments.

The following table explains the three levels of inspection provided by packet trace.

Table 22: Packet-Trace Level

Packet-Trace Level	Description
Accounting	Packet-Trace accounting provides a count of packets that enter and leave the network processor. Packet-Trace accounting is a lightweight performance activity, and runs continuously until it is disabled.

Packet-Trace Level	Description
Summary	At the summary level of packet trace, data is collected for a finite number of packets. Packet-Trace summary tracks the input and output interfaces, the final packet state, and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface.
Path data	<p>The packet-trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet-Trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data.</p> <p>Path data also has two optional capabilities: packet copy and Feature Invocation Array (FIA) trace. The packet-copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3 or layer 4). The FIA- trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing.</p> <p>Note Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. Therefore, path-data level should be used in limited capacity or in situations where packet performance change is acceptable.</p>

Usage Guidelines for Configuring Packet Trace

Consider the following best practices while configuring the Packet-Trace feature:

- Use of ingress conditions when using the Packet-Trace feature is recommended for a more comprehensive view of packets.
- Packet-trace configuration requires data-plane memory. On systems where data-plane memory is constrained, carefully consider how you will select the packet-trace values. A close approximation of the amount of memory consumed by packet trace is provided by the following equation:

memory required = (statistics overhead) + number of packets * (summary size + data size + packet copy size).

When the Packet-Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

Configuring Packet Trace

Perform the following steps to configure the Packet-Trace feature.

**Note**

The amount of memory consumed by the Packet-Trace feature is affected by the packet-trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting normal services. You can check the current data-plane DRAM memory consumption by using the **show platform hardware qfp active infrastructure exmem statistics** command.

SUMMARY STEPS

1. **enable**
2. **debug platform packet-trace packet** *pkt-num* [**fia-trace** | **summary-only**] [**circular**] [**data-size** *data-size*]
3. **debug platform packet-trace** {**punt** | **inject**|**copy**|**drop**|**packet**|**statistics**}
4. **debug platform condition** [**ipv4** | **ipv6**] [**interface** *interface*][**access-list** *access-list -name* | *ipv4-address / subnet-mask* | *ipv6-address / subnet-mask*] [**ingress** | **egress** | **both**]
5. **debug platform condition start**
6. **debug platform condition stop**
7. **show platform packet-trace** [**configuration** | **statistics** | **summary** | **packet** {**all** | *pkt-num*}]
8. **clear platform condition all**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	debug platform packet-trace packet <i>pkt-num</i> [fia-trace summary-only] [circular] [data-size <i>data-size</i>] Example: Router# debug platform packet-trace packets 2048 summary-only	Collects summary data for a specified number of packets. Captures feature path data by default, and optionally performs FIA trace. <i>pkt-num</i> —Specifies the maximum number of packets maintained at a given time. fia-trace —Provides detailed level of data capture, including summary data, feature-specific data. Also displays each feature entry visited during packet processing. summary-only —Enables the capture of summary data with minimal details. circular —Saves the data of the most recently traced packets. <i>data-size</i> —Specifies the size of data buffers for storing feature and FIA trace data for each packet in bytes. When very heavy packet processing is performed on packets, users can increase the size of the data buffers if necessary. The default value is 2048.

	Command or Action	Purpose
Step 3	debug platform packet-trace {punt inject copy drop packet statistics} Example: Router# debug platform packet-trace punt	Enables tracing of punted packets from data to control plane.
Step 4	debug platform condition [ipv4 ipv6] [interface interface][access-list access-list -name ipv4-address / subnet-mask ipv6-address / subnet-mask] [ingress egress both] Example: Router# debug platform condition interface g0/0/0 ingress	Specifies the matching criteria for tracing packets. Provides the ability to filter by protocol, IP address and subnet mask, access control list (ACL), interface, and direction.
Step 5	debug platform condition start Example: Router# debug platform condition start	Enables the specified matching criteria and starts packet tracing.
Step 6	debug platform condition stop Example: Router# debug platform condition start	Deactivates the condition and stops packet tracing.
Step 7	show platform packet-trace {configuration statistics summary packet {all pkt-num}} Example: Router# show platform packet-trace 14	Displays packet-trace data according to the specified option. See {start cross reference} Table 21-1 {end cross reference} for detailed information about the show command options.
Step 8	clear platform condition all Example: Router(config)# clear platform condition all	Removes the configurations provided by the debug platform condition and debug platform packet-trace commands.
Step 9	exit Example: Router# exit	Exits the privileged EXEC mode.

Configuring Packet Tracer with UDF Offset

Perform the following steps to configure the Packet-Trace UDF with offset:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udf udf name header {inner | outer} {13|14} offset offset-in-bytes length length-in-bytes**
4. **udf udf name {header | packet-start} offset-base offset length**
5. **ip access-list extended {acl-name |acl-num}**
6. **ip access-list extended { deny | permit } udf udf-name value mask**
7. **debug platform condition [ipv4 | ipv6] [interface interface] [access-list access-list -name | ipv4-address / subnet-mask | ipv6-address / subnet-mask] [ingress | egress |both]**
8. **debug platform condition start**
9. **debug platform packet-trace packet pkt-num [fia-trace | summary-only] [circular] [data-size data-size]**
10. **debug platform packet-trace {punt | inject|copy | drop |packet | statistics}**
11. **debug platform condition stop**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	udf udf name header {inner outer} {13 14} offset offset-in-bytes length length-in-bytes Example: Router(config)# udf TEST_UDF_NAME_1 header inner 13 64 1 Router(config)# udf TEST_UDF_NAME_2 header inner 14 77 2 Router(config)# udf TEST_UDF_NAME_3 header outer 13 65 1 Router(config)# udf TEST_UDF_NAME_4 header outer 14 67 1	Configures individual UDF definitions. You can specify the name of the UDF, the networking header from which offset, and the length of data to be extracted. The inner or outer keywords indicate the start of the offset from the unencapsulated Layer 3 or Layer 4 headers, or if there is an encapsulated packet, they indicate the start of offset from the inner L3/L4. The length keyword specifies, in bytes, the length from the offset. The range is from 1 to 2.
Step 4	udf udf name {header packet-start} offset-base offset length Example:	<ul style="list-style-type: none"> • header—Specifies the offset base configuration. • packet-start—Specifies the offset base from packet-start. packet-start” can vary depending on if

	Command or Action	Purpose
	<pre>Router(config)# udf TEST_UDF_NAME_5 packet-start 120 1</pre>	<p>packet-trace is for an inbound packet or outbound packet. If the packet-trace is for an inbound packet then the packet-start will be layer2. For outbound, the packet-start will be layer3.</p> <ul style="list-style-type: none"> • offset—Specifies the number of bytes offset from the offset base. To match the first byte from the offset base (Layer 3/Layer 4 header), configure the offset as 0. • length—Specifies the number of bytes from the offset. Only 1 or 2 bytes are supported. To match additional bytes, you must define multiple UDFs.
Step 5	<p>ip access-list extended {<i>acl-name</i> <i>acl-num</i>}</p> <p>Example:</p> <pre>Router(config)# ip access-list extended acl2</pre>	Enables extended ACL configuration mode. The CLI enters the extended ACL configuration mode in which all subsequent commands apply to the current extended access list. Extended ACLs control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL.
Step 6	<p>ip access-list extended { deny permit } udf udf-name value mask</p> <p>Example:</p> <pre>Router(config-acl)# permit ip any any udf TEST_UDF_NAME_5 0xD3 0xFF</pre>	Configures the ACL to match on UDFs along with the current access control entries (ACEs). The bytes defined in ACL is 0xD3. Masks are used with IP addresses in IP ACLs to specify what should be permitted and denied.
Step 7	<p>debug platform condition [ipv4 ipv6] [interface <i>interface</i>] [access-list <i>access-list-name</i> <i>ipv4-address / subnet-mask</i> <i>ipv6-address / subnet-mask</i>] [ingress egress both]</p> <p>Example:</p> <pre>Router# debug platform condition interface gi0/0/0 ipv4 access-list acl2 both</pre>	Specifies the matching criteria for tracing packets. Provides the ability to filter by protocol, IP address and subnet mask, access control list (ACL), interface, and direction.
Step 8	<p>debug platform condition start</p> <p>Example:</p> <pre>Router# debug platform condition start</pre>	Enables the specified matching criteria and starts packet tracing.
Step 9	<p>debug platform packet-trace packet <i>pkt-num</i> [fia-trace summary-only] [circular] [data-size <i>data-size</i>]</p> <p>Example:</p> <pre>Router# debug platform packet-trace packet 1024 fia-trace data-size 2048</pre>	<p>Collects summary data for a specified number of packets. Captures feature path data by default, and optionally performs FIA trace.</p> <p>pkt-num—Specifies the maximum number of packets maintained at a given time.</p> <p>fia-trace—Provides detailed level of data capture, including summary data, feature-specific data. Also</p>

	Command or Action	Purpose
		<p>displays each feature entry visited during packet processing.</p> <p>summary-only—Enables the capture of summary data with minimal details.</p> <p>circular—Saves the data of the most recently traced packets.</p> <p>data-size—Specifies the size of data buffers for storing feature and FIA trace data for each packet in bytes. When very heavy packet processing is performed on packets, users can increase the size of the data buffers if necessary. The default value is 2048.</p>
Step 10	debug platform packet-trace {punt inject copy drop packet statistics} Example: <pre>Router# debug platform packet-trace punt</pre>	Enables tracing of punted packets from data to control plane.
Step 11	debug platform condition stop Example: <pre>Router# debug platform condition start</pre>	Deactivates the condition and stops packet tracing.
Step 12	exit Example: <pre>Router# exit</pre>	Exits the privileged EXEC mode.

Displaying Packet-Trace Information

Use these **show** commands to display packet-trace information.

Table 23: show Commands

Command	Description
show platform packet-trace configuration	Displays packet trace configuration, including any defaults.
show platform packet-trace statistics	Displays accounting data for all the traced packets.
show platform packet-trace summary	Displays summary data for the number of packets specified.
show platform packet-trace {all pkt-num} [decode]	Displays the path data for all the packets or the packet specified. The decode option attempts to decode the binary packet into a more human- readable form.

Removing Packet-Trace Data

Use these commands to clear packet-trace data.

Table 24: clear Commands

Command	Description
clear platform packet-trace statistics	Clears the collected packet-trace data and statistics.
clear platform packet-trace configuration	Clears the packet-trace configuration and the statistics.

Configuration Examples for Packet Trace

This section provides the following configuration examples:

Example: Configuring Packet Trace

This example describes how to configure packet trace and display the results. In this example, incoming packets to Gigabit Ethernet interface 0/0/1 are traced, and FIA-trace data is captured for the first 128 packets. Also, the input packets are copied. The **show platform packet-trace packet 0** command displays the summary data and each feature entry visited during packet processing for packet 0.

```
Router>
enable
Router# debug platform packet-trace packet 128 fia-trace
Router# debug platform packet-trace punt
Router# debug platform condition interface g0/0/1 ingress
Router# debug platform condition start
Router#! ping to UUT
Router# debug platform condition stop
Router# show platform packet-trace packet 0
Packet: 0          CBUG ID: 9
Summary
  Input      : GigabitEthernet0/0/1
  Output     : GigabitEthernet0/0/0
  State      : FWD
  Timestamp
    Start    : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
    Stop     : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
Feature: IPV4
  Source      : 198.51.100.2
  Destination : 198.51.100.2
  Protocol    : 1 (ICMP)
Feature: FIA_TRACE
  Entry       : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
  Timestamp   : 3685243309297
Feature: FIA_TRACE
  Entry       : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
  Timestamp   : 3685243311450
Feature: FIA_TRACE
  Entry       : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
```

```

Timestamp : 3685243312427
Feature: FIA_TRACE
Entry      : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
Timestamp  : 3685243313230
Feature: FIA_TRACE
Entry      : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
Timestamp  : 3685243315033
Feature: FIA_TRACE
Entry      : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
Timestamp  : 3685243315787
Feature: FIA_TRACE
Entry      : 0x80321450 - IPV4_VFR_REFRAG
Timestamp  : 3685243316980
Feature: FIA_TRACE
Entry      : 0x82014700 - IPV6_INPUT_L2_REWRITE
Timestamp  : 3685243317713
Feature: FIA_TRACE
Entry      : 0x82000080 - IPV4_OUTPUT_FRAG
Timestamp  : 3685243319223
Feature: FIA_TRACE
Entry      : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
Timestamp  : 3685243319950
Feature: FIA_TRACE
Entry      : 0x8059aff4 - PACTRAC_OUTPUT_STATS
Timestamp  : 3685243323603
Feature: FIA_TRACE
Entry      : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
Timestamp  : 3685243326183

```

```

Router# clear platform condition all
Router# exit

```

Linux Forwarding Transport Service (LFTS) is a transport mechanism to forward packets punted from the CPP into applications other than IOSd. This example displays the LFTS-based intercepted packet destined for binos application.

```

Router# show platform packet-trace packet 10
Packet: 10      CBUG ID: 52
Summary
Input   : GigabitEthernet0/0/0
Output  : internal0/0/rp:1
State   : PUNT 55 (For-us control)
Timestamp
Start   : 597718358383 ns (06/06/2016 09:00:13.643341 UTC)
Stop    : 597718409650 ns (06/06/2016 09:00:13.643392 UTC)
Path Trace
Feature: IPV4
Input   : GigabitEthernet0/0/0
Output  : <unknown>
Source  : 10.64.68.2
Destination : 224.0.0.102
Protocol : 17 (UDP)
SrcPort  : 1985
DstPort  : 1985
Feature: FIA_TRACE
Input   : GigabitEthernet0/0/0
Output  : <unknown>
Entry   : 0x8a0177bc - DEBUG_COND_INPUT_PKT
Lapsed time : 426 ns
Feature: FIA_TRACE
Input   : GigabitEthernet0/0/0
Output  : <unknown>
Entry   : 0x8a017788 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time : 386 ns

```

```

Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : <unknown>
  Entry  : 0x8a01778c - IPV4_INPUT_FOR_US_MARTIAN
  Lapsed time : 13653 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017730 - IPV4_INPUT_LOOKUP_PROCESS_EXT
  Lapsed time : 2360 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017be0 - IPV4_INPUT_IPOPTIONS_PROCESS_EXT
  Lapsed time : 66 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017bfc - IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
  Lapsed time : 680 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d60 - IPV4_INTERNAL_ARL_SANITY_EXT
  Lapsed time : 320 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017a40 - IPV4_VFR_REFRAG_EXT
  Lapsed time : 106 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d2c - IPV4_OUTPUT_DROP_POLICY_EXT
  Lapsed time : 1173 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017940 - INTERNAL_TRANSMIT_PKT_EXT
  Lapsed time : 20173 ns
LFTS Path Flow: Packet: 10      CBUG ID: 52
Feature: LFTS
Pkt Direction: IN
Punt Cause   : 55
subCause    : 0

```

Example: Using Packet Trace

This example provides a scenario in which packet trace is used to troubleshoot packet drops for a NAT configuration on a Cisco ASR 1006 Router. This example shows how you can effectively utilize the level of detail provided by the Packet-Trace feature to gather information about an issue, isolate the issue, and then find a solution.

In this scenario, you can detect that there are issues, but are not sure where to start troubleshooting. You should, therefore, consider accessing the Packet-Trace summary for a number of incoming packets.

```

Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary

```


Pkt	Input	Output	State	Reason
0	Gi0/0/0	Gi0/0/0	DROP	402 (NoStatsUpdate)
1	internal0/0/rp:0	internal0/0/rp:0	PUNT	21 (RP<->QFP keepalive)
2	internal0/0/recycle:0	Gi0/0/0	FWD	

The output shows that packets are dropped due to NAT configuration on Gigabit Ethernet interface 0/0/0, which enables you to understand that an issue is occurring on a specific interface. Using this information, you can limit which packets to trace, reduce the number of packets for data capture, and increase the level of inspection.

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input      : GigabitEthernet0/0/0
  Output     : internal0/0/rp:1
  State      : PUNT 55 (For-us control)
  Timestamp
    Start    : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop     : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input      : GigabitEthernet0/0/0
    Output     : <unknown>
    Source     : 10.64.68.3
    Destination : 224.0.0.102
    Protocol   : 17 (UDP)
    SrcPort    : 1985
    DstPort    : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source       : 10.64.68.122
    Destination  : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source       : 10.64.68.122
    Destination  : 10.64.68.255
    Interface    : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src          : 10.64.68.122(1053)
    dst          : 10.64.68.255(1947)
    length       : 48
```

```
Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input      : GigabitEthernet0/0/0
  Output     : internal0/0/rp:0
  State      : PUNT 55 (For-us control)
  Timestamp
    Start    : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop     : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
```

Example: Using Packet Trace

```

Path Trace
  Feature: IPV4(Input)
    Input      : GigabitEthernet0/0/0
    Output     : <unknown>
    Source     : 10.78.106.2
    Destination : 224.0.0.102
    Protocol   : 17 (UDP)
    SrcPort    : 1985
    DstPort    : 1985

IOSd Path Flow: Packet: 10      CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
  Packet Rcvd From DATAPLANE
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source       : 10.78.106.2
    Destination  : 224.0.0.102
    Interface    : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src      : 881 10.78.106.2(1985)
    dst      : 224.0.0.102(1985)
    length   : 60

Router#show platform packet-trace packet 12
Packet: 12      CBUG ID: 767
Summary
  Input      : GigabitEthernet3
  Output     : internal0/0/rp:0
  State      : PUNT 11 (For-us data)
  Timestamp
    Start    : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop     : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
  Path Trace
    Feature: IPV4(Input)
      Input      : GigabitEthernet3
      Output     : <unknown>
      Source     : 12.1.1.1
      Destination : 12.1.1.2
      Protocol   : 6 (TCP)
      SrcPort    : 46593
      DstPort    : 23
  IOSd Path Flow: Packet: 12      CBUG ID: 767
    Feature: INFRA
      Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source       : 12.1.1.1
    Destination  : 12.1.1.2
    Interface    : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source       : 12.1.1.1
    Destination  : 12.1.1.2

```

```

Interface      : GigabitEthernet3

Feature: TCP
Pkt Direction: IN
tcp0: I NoTCB 12.1.1.1:46593 12.1.1.2:23 seq 1925377975 OPTS 4 SYN WIN 4128

Router# show platform packet-trace summary
Pkt  Input      Output      State  Reason
0    INJ.2      Gil        FWD
1    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
2    INJ.2      Gil        FWD
3    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
4    INJ.2      Gil        FWD
5    INJ.2      Gil        FWD
6    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
7    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
8    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
9    Gil        internal0/0/rp:0  PUNT  11  (For-us data)
10   INJ.2      Gil        FWD
11   INJ.2      Gil        FWD
12   INJ.2      Gil        FWD
13   Gil        internal0/0/rp:0  PUNT  11  (For-us data)
14   Gil        internal0/0/rp:0  PUNT  11  (For-us data)
15   Gil        internal0/0/rp:0  PUNT  11  (For-us data)
16   INJ.2      Gil        FWD

```

The following example displays the packet trace data statistics.

```

Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count  Code  Cause
    3      56   RP injected for-us control
  Drop     0
  Consume  0

      PKT_DIR_IN
      Dropped    Consumed    Forwarded
INFRA          0           0           0
TCP             0           0           0
UDP             0           0           0
IP              0           0           0
IPV6            0           0           0
ARP             0           0           0

      PKT_DIR_OUT
      Dropped    Consumed    Forwarded
INFRA          0           0           0
TCP             0           0           0
UDP             0           0           0
IP              0           0           0
IPV6            0           0           0
ARP             0           0           0

```

The following example displays packets that are injected and punted to the forwarding processor from the control plane.

Example: Using Packet Trace

```
Router#debug platform condition ipv4 10.118.74.53/32 both
Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256
```

```
Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0          CBUG ID: 674
Summary
  Input       : GigabitEthernet1
  Output      : internal0/0/rp:0
  State       : PUNT 11 (For-us data)
  Timestamp
    Start     : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop      : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
```

```
Path Trace
Feature: IPV4(Input)
  Input       : GigabitEthernet1
  Output      : <unknown>
  Source      : 10.118.74.53
  Destination : 198.51.100.38
  Protocol    : 17 (UDP)
  SrcPort     : 2640
  DstPort     : 500
```

```
IOSd Path Flow: Packet: 0      CBUG ID: 674
Feature: INFRA
Pkt Direction: IN
  Packet Rcvd From DATAPLANE
```

```
Feature: IP
Pkt Direction: IN
  Packet Enqueued in IP layer
  Source      : 10.118.74.53
  Destination : 198.51.100.38
  Interface   : GigabitEthernet1
```

```
Feature: IP
Pkt Direction: IN
FORWARDED To transport layer
  Source      : 10.118.74.53
  Destination : 198.51.100.38
  Interface   : GigabitEthernet1
```

```
Feature: UDP
Pkt Direction: IN
DROPPED
UDP: Checksum error: dropping
Source      : 10.118.74.53(2640)
Destination : 198.51.100.38(500)
```

```
Router#show platform packet-tracer packet 2
Packet: 2          CBUG ID: 2
```

```
IOSd Path Flow:
Feature: TCP
Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN WIN 4128
```

```
Feature: TCP
Pkt Direction: OUT
FORWARDED
TCP: Connection is in SYNRCVD state
ACK      : 2346709419
```

```

SEQ          : 3052140910
Source       : 198.51.100.38(22)
Destination  : 198.51.100.55(52774)

```

```

Feature: IP
Pkt Direction: OUTRoute out the generated packet.srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

```

```

Feature: IP
Pkt Direction: OUTInject and forward successful srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

```

```

Feature: TCP
Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN WIN 4128
Summary
Input      : INJ.2
Output     : GigabitEthernet1
State      : FWD
Timestamp
Start      : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
Stop       : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)

```

```

Path Trace
Feature: IPV4(Input)
Input      : internal0/0/rp:0
Output     : <unknown>
Source     : 172.18.124.38
Destination : 172.18.124.55
Protocol   : 6 (TCP)
SrcPort    : 22
DstPort    : 52774
Feature: IPSec
Result     : IPSEC_RESULT_DENY
Action     : SEND_CLEAR
SA Handle  : 0
Peer Addr  : 55.124.18.172
Local Addr : 38.124.18.172

```

Router#

Additional References

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL: {start hypertext} http://www.cisco.com/go/mibs {end hypertext}

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	{start hypertext} http://www.cisco.com/cisco/web/support/index.html {end hypertext}

Feature Information for Packet Trace

{start cross reference} Table 21-4 {end cross reference} lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to {start hypertext} <http://www.cisco.com/go/cfn> {end hypertext}. An account on Cisco.com is not required.



Note {start cross reference} Table 21-4 {end cross reference} lists only the software releases that support a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 25: Feature Information for Packet Trace

Feature Name	Releases	Feature Information
Packet Trace	Cisco IOS XE 3.10S	<p>The Packet Trace feature provides information about how data packets are processed by the Cisco IOS XE software.</p> <p>In Cisco IOS XE Release 3.10S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • debug platform packet-trace packet <i>pkt-num</i> [fia-trace summary-only] [data-size <i>data-size</i>] [circular] • debug platform packet-trace copy packet {input output both} [size <i>num-bytes</i>] [L2 L3 L4] • show platform packet-trace {configuration statistics summary packet {all <i>pkt-num</i>}}
	Cisco IOS XE 3.11S	<p>In Cisco IOS XE Release 3.11S, this feature was enhanced to include the following features:</p> <ul style="list-style-type: none"> • Matched versus traced statistics. • Trace stop timestamp in addition to trace start timestamp. <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • debug platform packet-trace drop [code <i>drop-num</i>] • show platform packet-trace packet {all <i>pkt-num</i>} [decode]
	Cisco IOS XE Denali 16.3.1	<p>In Cisco IOS XE Denali 16.3.1, this feature was enhanced to include Layer3 packet tracing along with IOSd.</p> <p>The following commands were introduced or modified: debug platform packet-trace punt.</p>
	Cisco IOS XE Amsterdam 17.3.1	<p>The output of the show platform packet-trace command now includes additional trace information for packets either originated from IOSd or destined to IOSd or other BinOS processes.</p>



CHAPTER 17

EVPN VPWS over SR-TE Preferred Path

The Ethernet VPN Virtual Private Wire Service (EVPN VPWS) functionality implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. This enhancement extends EVPN VPWS to support the specification of an SR-TE policy using the **preferred path** feature.

- [Feature Information for EVPN VPWS over SR-TE Preferred Path, on page 181](#)
- [Restrictions for EVPN VPWS over SR-TE Preferred Path, on page 181](#)
- [Information About EVPN VPWS over SR-TE Preferred Path, on page 182](#)
- [How to Configure EVPN VPWS over SR-TE Preferred Path, on page 182](#)
- [Verifying EVPN VPWS over SR-TE Preferred Path, on page 183](#)

Feature Information for EVPN VPWS over SR-TE Preferred Path

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use the Cisco Feature Navigator to find information about platform support and Cisco software image support. To access the Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 26: Feature Information for EVPN VPWS over SR-TE Preferred Path

Feature Name	Releases	Feature Information
EVPN VPWS over SR-TE Preferred Path	Cisco IOS XE Cupertino 17.7.1a	This feature was introduced.

Restrictions for EVPN VPWS over SR-TE Preferred Path

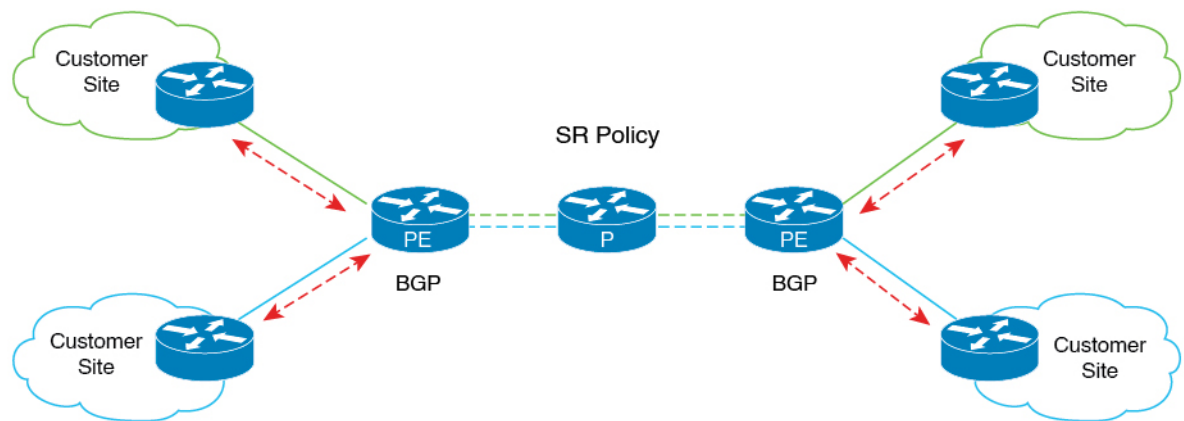
- SR On-Demand Next Hop (ODN) policy is not supported; only SR static policy is supported.
- SR Per-Flow Policy (PFP) is not supported; only SR Per-Destination Policy (PDP) is supported.
- Interior Gateway Protocol (IGP) is Intermediate System-to-Intermediate system (IS-IS).

Information About EVPN VPWS over SR-TE Preferred Path

The EVPN VPWS functionality implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. This enhancement enables EVPN VPWS to support the specification of an SR-TE policy using the **preferred path** feature. This feature includes the **fallback disable** option, which disables the default behavior of falling back on an alternate path if the preferred path is down.

The following figure illustrates the architecture:

Figure 3: EVPN VPWS over SR-TE Architecture



357825

How to Configure EVPN VPWS over SR-TE Preferred Path

The following sections provide information about the tasks involved in configuring EVPN VPWS over the SR-TE preferred path.

Configuring EVPN VPWS over SR-TE Preferred Path

The following example shows how to enable EVPN VPWS over the configured SR-TE preferred path:

```
l2vpn evpn instance 100 point-to-point
rd 100:100
route-target export 100:100
route-target import 100:100
!
vpws context vc100
  preferred-path segment-routing traffic-eng policy p-100
  service target 100 source 100
interface GigabitEthernet0/0/3
service instance 100 ethernet
encapsulation dot1q 100
```

Configuring EVPN VPWS over SR-TE Preferred Path with Fallback Disable

The **fallback disable** command prevents a device from using the default path if the preferred path SR policy goes down.

```
l2vpn evpn instance 100 point-to-point
rd 100:100
route-target export 100:100
route-target import 100:100
vpws context vc100
service target 100 source 100
member GigabitEthernet0/0/3 service-instance 100
preferred-path segment-routing traffic-eng policy p-100 disable-fallback
```

Removing Fallback Disable from EVPN VPWS over SR-TE Preferred Path

The following example shows how to remove the fallback disable option in EVPN VPWS over SR-TE preferred path:

```
l2vpn evpn instance 100 point-to-point
vpws context vc100
preferred-path segment-routing traffic-eng policy p-100
```

Disabling EVPN VPWS over SR-TE Preferred Path Configuration

The following example shows how to disable the EVPN VPWS over SR-TE preferred path configuration:

```
l2vpn evpn instance 100 point-to-point
vpws context vc100
no preferred-path segment-routing traffic-eng policy p-100 disable-fallback
```

Verifying EVPN VPWS over SR-TE Preferred Path

The following sample outputs show how to verify the EVPN VPWS over SR-TE preferred path and fallback disable configurations.

- The following is a sample output showing the EVPN VPWS configuration over an SR-TE preferred path:

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
EVPN ID: 100
VPWS Service Instance ID: Source 1, Target 2
Labels: Local 17, Remote 17
Next Hop Address: 6.6.6.6
Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
Output interface: Tu65536, imposed label stack {16016 17}
Preferred path: active
Default path: ready
```

```
device# show l2vpn evpn vpws vc preferred-path
Tunnel      EVPN ID  Source  Target  Name      Status
-----
Tunnel165536  100      1        2        vc100     up
```

- The following is a sample output showing the EVPN VPWS configuration over an SR-TE preferred path, with fallback disabled:

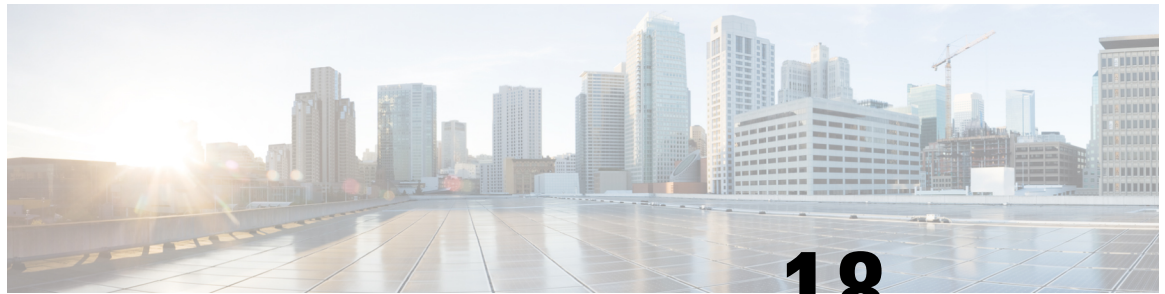
```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Tu65536, imposed label stack {16016 17}
  Preferred path: active
  Default path: disabled
Dataplane:
SSM segment/switch IDs: 25037/12290 (used), PWID: 1
Rx Counters
1241 input transit packets, 463266 bytes
0 drops
Tx Counters
828 output transit packets, 402840 bytes
0 drops
24 VC FSM state transitions, Last 10 shown
DpUp: Act -> Est, Mon Sep 06 23:32:43.809 (2w2d ago)
RemDn: Est -> RemWait, Mon Sep 06 23:32:43.809 (2w2d ago)
RemUp: RemWait -> Act, Mon Sep 06 23:32:43.816 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:32:43.816 (2w2d ago)
DpDn: Est -> Act, Mon Sep 06 23:35:57.944 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:43:50.071 (2w2d ago)
DpDn: Est -> Act, Mon Sep 06 23:46:15.361 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:54:11.508 (2w2d ago)
DpDn: Est -> Act, Tue Sep 07 00:00:11.248 (2w2d ago)
DpUp: Act -> Est, Tue Sep 07 00:06:27.355 (2w2d ago)
```

- The following is a sample output showing the EVPN VPWS configuration over an SR-TE preferred path, with fallback disable option removed:

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Tu65536, imposed label stack {16016 17}
  Preferred path: active
  Default path: ready
```

- The following is a sample output showing the EVPN VPWS configuration over an SR-TE preferred path disabled:

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Gi0/0/0, imposed label stack {16 16}
  Preferred path: not configured
  Default path: active
```



CHAPTER 18

Configuring SFP+

SUMMARY STEPS

- 1. **enable** *source-interface gigabitethernet slot/port*
- 2. **configure terminal**
- 3. **interface** *tengigabitethernet slot/port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable <i>source-interface gigabitethernet slot/port</i> Example: Router# enable	Enables the privileged EXEC mode. If prompted, enter your password.
Step 2	configure terminal Example: Router# configure terminal	Enters the global configuration mode.
Step 3	interface <i>tengigabitethernet slot/port</i> Example: Router(config)# interface tengigabitethernet 4/11	Specifies the 10-Gigabit Ethernet interface to be configured. Here: slot/port—Specifies the location of the interface.



CHAPTER 19

Cisco ThousandEyes Enterprise Agent Application Hosting

This chapter provides information on Cisco ThousandEyes Enterprise Agent Application Hosting. The following sections are included in this chapter:

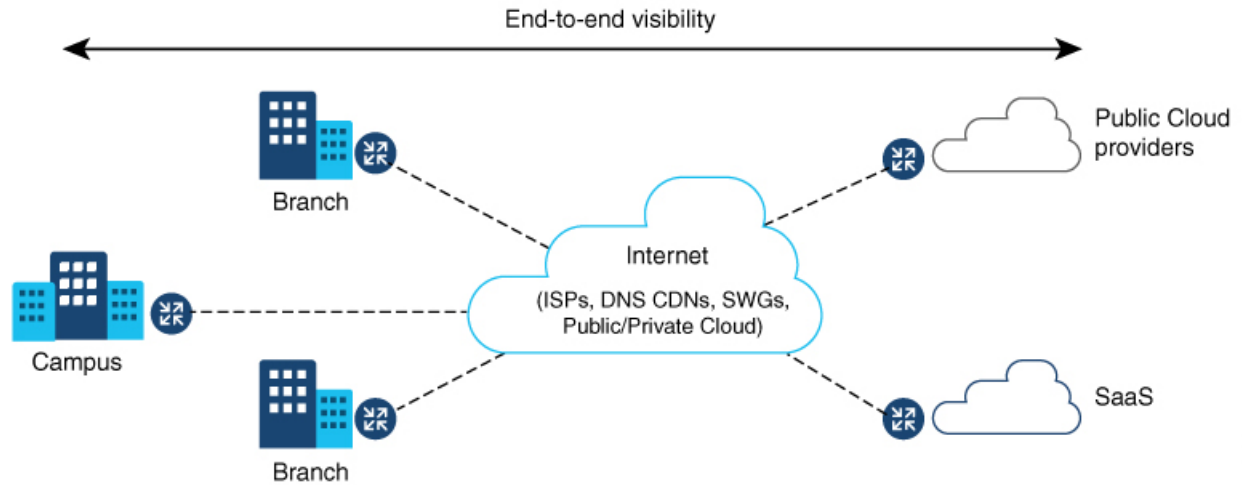
- [Cisco ThousandEyes Enterprise Agent Application Hosting, on page 187](#)
- [Supported Platforms and System Requirements, on page 188](#)
- [Workflow to Install and Run the Cisco ThousandEyes Application, on page 189](#)
- [Modifying the Agent Parameters, on page 193](#)
- [Uninstalling the Application, on page 193](#)
- [Troubleshooting the Cisco ThousandEyes Application, on page 194](#)

Cisco ThousandEyes Enterprise Agent Application Hosting

Cisco ThousandEyes is a network intelligence platform that allows you to use its agents to run a variety of tests from its agents to monitor the network and application performance. This application enables you to view end-to-end paths across networks and services that impact your business. Cisco ThousandEyes application actively monitors the network traffic paths across internal, external, and internet networks in real time, and helps to analyse the network performance. Also, Cisco ThousandEyes application provides application availability insights that are enriched with routing and device data for a multidimensional view of digital experience.

From Cisco IOS XE Release 17.8.1, you can use application-hosting capabilities to deploy the Cisco ThousandEyes Enterprise Agent as a container application on Cisco Catalyst 8500 and Catalyst 8500L Series Edge Platforms. This agent application runs as a docker image using Cisco IOx docker-type option. For more information on how to configure Cisco ThousandEyes in controller mode, see [Cisco SD-WAN Systems and Interfaces Configuration Guide](#).

Figure 4: Network View through ThousandEyes Application



Feature Information for Cisco ThousandEyes Enterprise Agent Application Hosting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 27: Feature Information for ThousandEyes Enterprise Agent Application Hosting

Feature Name	Releases	Feature Information
Cisco ThousandEyes Enterprise Agent Application Hosting	Cisco IOS XE 17.8.1	With the integration of ThousandEyes Agent Application running on routing platforms using the app-hosting capabilities as container, you can have visibility into application experience with deep insights into the Internet, cloud providers, and enterprise networks.

Supported Platforms and System Requirements

The following table lists the supported platforms and system requirements.

Platforms	Bootflash	FRU Storage	DRAM
Cisco Catalyst 8500 Series Edge Platforms			
C8500-12X4QC	32 GB	(Default) 32 GB eUSB (Optional) HDD	16 GB

Platforms	Bootflash	FRU Storage	DRAM
C8500-12X	32 GB	(Default) 32 GB eUSB (Optional) HDD	16 GB
Cisco Catalyst 8500L Series Edge Platforms			
C8500L-8S4X	16 GB	(Default) 32GB M.2 USB	16 GB

**Note**

The minimum DRAM and bootflash storage requirement for running Cisco ThousandEyes Enterprise Agent is 8 GB. If the device does not have enough memory or storage, we recommend that you upgrade DRAM or add an external storage such as SSD/M.2 USB. When the available resources are not sufficient to run other applications, Cisco IOx generates an error message.

Workflow to Install and Run the Cisco ThousandEyes Application

To install and run the Cisco ThousandEyes image on a device, perform these steps:

- Step 1** Create a new account on the Cisco ThousandEyes portal.
- Step 2** Download the Cisco ThousandEyes application package from the [software downloads](#) page and ensure that you use the agent version 4.2.2.
- Step 3** Copy the image on the device.
- Step 4** Install and launch the image.
- Step 5** Connect the agent to the controller.

Note When you order platforms that support Cisco ThousandEyes application with Cisco IOS XE 17.8.1 software, the Cisco ThousandEyes application package is available in the bootflash of the device.

Workflow to Host the Cisco ThousandEyes Application

To install and launch the application, perform these steps:

Before you begin

Create a new account on the Cisco ThousandEyes portal and generate the token. The Cisco ThousandEyes agent application uses this token to authenticate and check into the correct Cisco ThousandEyes account. you see a message stating that your token is invalid and you want to troubleshoot the issue, see [Troubleshooting the Cisco ThousandEyes Application, on page 194](#).



Note If you configure the correct token and Domain Name Server (DNS) information, the device is discovered automatically.

Step 1 Enable Cisco IOX application environment on the device.

- Use the following commands for non-SD-WAN (autonomous mode) images:

```
config terminal
  iox
end
write
```

- Use the following commands for SD-WAN (controller mode) images:

```
config-transaction
  iox
commit
```

Step 2 If the IOx command is accepted, wait for a few seconds and check whether the IOx process is up and running by using the **show iox** command. The output must display that the show IOxman process is running.

Device #show iox

IOx Infrastructure Summary:

```
IOx service (CAF) 1.11.0.0      : Running
IOx service (HA)                : Not Supported
IOx service (IOxman)            : Running
IOx service (Sec storage)       : Not Supported
Libvirt 1.3.4                   : Running
```

Step 3 Ensure that the ThousandEyes application LXC tarball is available in the device *bootflash*:

Step 4 Create a virtual port group interface to enable the traffic path to the Cisco ThousandEyes application:

```
interface VirtualPortGroup 0
  ip address 192.168.35.1 255.255.255.0
exit
```

Step 5 Configure the app-hosting application with the generated token:

```
app-hosting appid te
  app-vnic gateway1 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.35.2 netmask 255.255.255.0
  app-default-gateway 192.168.35.1 guest-interface 0
  app-resource docker
    prepend-pkg-opts ☐ Required to get the default run-time options from package.yaml

    run-opts 1 "--hostname thousandeyes"
    run-opts 2 "-e TEAGENT_ACCOUNT_TOKEN=<ThousandEyes token>"
    run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy.something.other:80"

    name-server0 75.75.75.75 ☐ ISP's DNS server
  end

app-hosting appid te
```

```
app-resource docker
prepend-pkg-opts
run-opts 2 "--hostname
```

Note You can use the proxy configuration only if the Cisco ThousandEyes agent does not have an internet access without a proxy. Also, the hostname is optional. If you do not provide the hostname during the installation, the device hostname is used as the Cisco ThousandEyes agent hostname. The device hostname is displayed on the Cisco ThousandEyes portal. The DNS name server information is optional. If the Cisco ThousandEyes agent uses a private IP address, ensure that you establish a connection to the device through NAT.

Step 6 Configure the **start** command to run the application automatically when the application is installed on the device using the **install** command:

```
app-hosting appid te
start
```

Step 7 On C8500-L platform, convert the device to app-heavy mode and reload the device using the following commands:

```
Device(config)#platform resource app-heavy
Please reboot to activate this template
```

```
C8500L(config)#end
C8500L#wr mem
Building configuration...
[OK]
C8500L#
```

```
C8500L#reload
Proceed with reload? [confirm]
```

Step 8 Install the ThousandEyes application:

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

Select a location to install the ThousandEyes application from these options:

```
Device# app-hosting install appid te package ?
bootflash: Package path ☐ ISR4K case if image is locally available in bootflash:
harddisk:   Package path ☐ Cat8K case if image is locally available in M.2 USB
https:      Package path ☐ Download over the internet if image is not locally present in
router. URL to ThousandEyes site hosting agent image to be provided here
```

Step 9 Check if the application is up and running:

```
Device#show app-hosting list
App id                               State
-----
te                                   RUNNING
```

Note If any of these steps fail, use the **show logging** command and check the IOx error message. If the error message is about insufficient disk space, clean the storage media (bootflash or hard disk) to free up the space. Use the **show app-hosting resource** command to check the CPU and disk memory.

Downloading and Copying the Image to the Device

To download and copy the image to bootflash, perform these steps:

Step 1 Check if the Cisco ThousandEyes image is precopied to *bootflash:/<directory name>*.

Step 2 If the image is not available in the device directory, perform these steps:

- a) If the device has a direct access to internet, use the *https:.* option in the **application install** command. This option downloads the image from the Cisco ThousandEyes software downloads page into *bootflash:/apps* and installs the application.

```
Device# app-hosting install appid <appid string> package [bootflash: | flash | http | https://
| ftp | ] URL to image location hosted on ThousandEyes portal
```

```
Device# app-hosting install appid tel1000 package
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar
```

```
Installing package
'https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar'
for 'tel1000'.
```

Use 'show app-hosting list' for progress.

```
*Jun 29 23:43:29.244: %IOSXE-6-PLATFORM: R0/0: IOx: App verification successful
*Jun 29 23:45:00.449: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: tel1000
installed successfully Current state is DEPLOYED
*Jun 29 23:45:01.801: %IOSXE-6-PLATFORM: R0/0: IOx: App verification successful
*Jun 29 23:45:51.054: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: tel1000 started
successfully Current state is RUNNING
```

```
Device#show app-hosting detail appid tel1000 (Details of Application)
```

```
App id          : tel1000
Owner           : iox
State           : RUNNING
Application
  Type          : docker
  Name          : ThousandEyes Enterprise Agent
  Version       : 4.0
  Author        : ThousandEyes <support@thousandeyes.com>
  Path          : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory        : 500 MB
  Disk          : 1 MB
  CPU           : 1500 units
  CPU-percent   : 70 %
```

- b) If the device has a proxy server, copy the image manually to *bootflash:/apps*.
- c) Download the Cisco ThousandEyes application package from the [software downloads](#) page and ensure that you use the agent version 4.0.2.
- d) Create an application directory in the *bootflash:* to copy the image:

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

- e) Copy the Cisco ThousandEyes image to the *bootflash:apps* directory.
- f) Validate the image using the **verify** command:

```
verify /md5 bootflash:apps/<file name>
```

Connecting the Cisco ThousandEyes Agent with the Controller

Before you begin

Ensure that you have an Internet connection before you connect the agent with the controller.

After the Cisco ThousandEyes application is up and running, the agent (ThousandEyes-agent) process connects to the controller that is running on the cloud environment.

Note If you have issues related to connectivity, the application logs the relevant error messages in the application-specific logs (*/var/logs*).

Modifying the Agent Parameters

To modify the agent parameters, perform these actions:

-
- Step 1** Stop the application using the **app-hosting stop appid appid** command.
 - Step 2** Deactivate the application using the **app-hosting deactivate appid appid** command.
 - Step 3** Make the required changes to app-hosting configuration.
 - Step 4** Activate the application using the **app-hosting activate appid appid** command.
 - Step 5** Start the application using the **app-hosting start appid appid** command.
-

Uninstalling the Application

To uninstall the application, perform these steps:

-
- Step 1** Stop the application using the **app-hosting stop appid te** command.
 - Step 2** Check if the application is in active state using the **show app-hosting list** command.
 - Step 3** Deactivate the application using the **app-hosting deactivate appid te** command.
 - Step 4** Ensure that the application is not in active state. Use the **show app-hosting list** command to check status of the application.
 - Step 5** Uninstall the application using the **app-hosting uninstall appid te** command.
 - Step 6** After the uninstallation process is complete, use the **show app-hosting list** command to check if the application is uninstalled successfully.
-

Troubleshooting the Cisco ThousandEyes Application

To troubleshoot the Cisco ThousandEyes application, perform these steps:

1. Connect to Cisco ThousandEyes agent application using the **app-hosting connect appid appid session /bin/bash** command.
2. Verify the configuration applied to the application at the following path */etc/te-agent.cfg*.
3. View the logs at the following path */var/log/agent/te-agent.log*. You can use these logs to troubleshoot the configuration.

Checking the ThousandEyes Application Status

When the Cisco ThousandEyes application is in running state, it is registered on the ThousandEyes portal. If the application does not show up in a few minutes after the agent is in running state, check the following using the **app-hosting connect appid thousandeyes_enterprise_agent session** command:

```
Device#app-hosting connect appid thousandeyes_enterprise_agent session
Device# cat /var/log/agent/te-agent.log
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.AptPackageInterface] {} Initialized APT
package interface
2021-02-04 08:59:29.642 INFO [e4736a40] [te.agent.main] {} Agent version 1.103.0 starting.
Max core size is 0 and max open files is 1024
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.db] {} Vacuuming database
2021-02-04 08:59:29.643 INFO [e4736a40] [te.agent.db] {} Found version 0, expected version
50
2021-02-04 08:59:29.672 INFO [e4708700] [te.probe.ServerTaskExecutor] {} ProbeTaskExecutor
started with 2 threads.
2021-02-04 08:59:29.673 INFO [e2f05700] [te.probe.ProbeTaskExecutor.bandwidth] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO [e2704700] [te.probe.ProbeTaskExecutor.realtime] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO [e1f03700] [te.probe.ProbeTaskExecutor.throughput] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.agent.DnssecTaskProceessor] {} Agent is not
running bind
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised SNMP++
session
2021-02-04 08:59:29.674 INFO [e4736a40] [te.agent.main] {} Agent starting up
2021-02-04 08:59:29.675 INFO [e4736a40] [te.agent.main] {} No agent id found, attempting
to obtain one
2021-02-04 08:59:29.675 INFO [e4736a40] [te.agent.ClusterMasterAdapter] {} Attempting to
get agent id from scl.thousandeyes.com
2021-02-04 08:59:29.679 ERROR [e4736a40] [te.agent.main] {} Error calling create_agent:
Curl error - Couldn't resolve host name
2021-02-04 08:59:29.680 INFO [e4736a40] [te.agent.main] {} Sleeping for 30 seconds
Note :
```



Note Check the DNS server connection. If the Cisco ThousandEyes agent is assigned to a private IP address, check the NAT configuration.