



Cisco Embedded Service 6300 Series Software Configuration Guide

First Published: 2019-03-28

Last Modified: 2024-01-31

Americas Headquarters

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



CONTENTS

CHAPTER 1

Overview 1

- Introduction 1
- Accessing the CLI Using a Router Console 2
 - Using the Console Interface 4
- Accessing the CLI from a Remote Console 4
 - Preparing to Connect to the Router Console Using Telnet 4
 - Using Telnet to Access a Console Interface 5
- CLI Session Management 6
 - Changing the CLI Session Timeout 6
 - Locking a CLI Session 6

CHAPTER 2

New Features 9

- New Features for Cisco IOS XE 17.14.1a 9
- New Features for Cisco IOS XE 17.13.1 9
- New Features for Cisco IOS XE 17.12.1a 10
- New Features for Cisco IOS XE 17.11.1a 10
- New Features for Cisco IOS XE 17.10.1a 10
- New Features for Cisco IOS XE 17.9.1 10
- New Features for Cisco IOS-XE 17.8.1 11
 - Cellular Serviceability Enhancements 11
 - GNMI Broker (GNMIB) Update 11
 - gRPC Network Operations Interface Update 12
 - Raw Socket Feature Enhancement 12
 - SCADA Enhancement for TNB 12
 - DLEP and Credit Based Radio Aware Routing Support 12
- New Features for Cisco IOS-XE 17.7.1 13

LTE Support for ESR6300	13
Support 1G SFPs	13
New Features for Cisco IOS-XE 17.6.1	14
Additional SFF Support	14
VXLAN support	14
New Features for Cisco IOS-XE 17.5.1	14
RFC4884 ICMPv6 and MPLSv6	14
Command Example	15
Limitations	15
Netboot Support	15
Alarm port Support on the ESR6300	15
Alarm Port Configuration Examples	17
New Features for Cisco IOS-XE 17.4.1	20
Plug and Play (PnP) Support	20
PnP Overview	20
New Features for Cisco IOS-XE 17.3.1	20
Support for Security-Enhanced Linux (SELinux)	20
Command Examples	21
Syslog Message Reference	22
SD-WAN on the ESR6300	23
New Features for Cisco IOS-XE 17.2.1	23
Serial Port Support	23
Boot from the USB	23
Booting from IOS	23
Booting from ROMMON	24
Booting from the USB Feature Summary	25

CHAPTER 3**Web User Interface 27**

Web User Interface Management Overview	27
Using Web User Interface for Day One Setup	27
Configure LAN Settings	28
Configure Primary WAN Settings	29
Configure Secondary WAN Settings	29
Configure Security Settings	30

GPS Mode Enabled By Default	31
Cisco WebUI Access Point Name (APN)	31
Summary Screen	34

CHAPTER 4
Secure Shell 37

Information About Secure Shell	37
Prerequisites for Configuring Secure Shell	37
Restrictions for Configuring Secure Shell	37
SSH And Router Access	38
SSH Servers, Integrated Clients, and Supported Versions	38
SSH Configuration Guidelines	39
How to Configure Secure Shell	39
Setting Up the Router to Run SSH	39
Configuring the SSH Server	41
Monitoring the SSH Configuration and Status	43
Configuring the Router for Local Authentication and Authorization	43
Information about Secure Copy	45
Prerequisites for Secure Copy	45
Restrictions for Configuring Secure Copy	45
Configuring Secure Copy	46
Additional References	47

CHAPTER 5
Using Cisco IOS XE Software 49

Understanding Command Modes	49
Using Keyboard Shortcuts	51
Using the no and default Forms of Commands	51
Using the History Buffer to Recall Commands	52
Managing Configuration Files	52
Saving Configuration Changes	52
Filtering Output from the show and more Commands	53
Using Cisco Feature Navigator	54
Finding Support Information for Platforms and Cisco Software Images	54
Getting Help	54
Finding Command Options: Example	55

Using Software Advisor	58
Using Software Release Notes	58

CHAPTER 6

Basic Router Configuration	59
ESR6300 Interface Naming	59
Basic Configuration	60
Configuring Global Parameters	65
Serial Port Support	66
Rawsocket Keepalive Configuration CLI	66
Configuring the Gigabit Ethernet Interface	67
Configuring a Loopback Interface	68
Enabling Cisco Discovery Protocol	69
Configuring Command-Line Access	69
Configuring Static Routes	71
Configuring Dynamic Routes	72
Configuring Routing Information Protocol	72
Configuring Enhanced Interior Gateway Routing Protocol	74
Configuring Open Shortest Path First (OSPF)	74
Configuring Integrated Intermediate System-to-Intermediate System (IS-IS) Routing Protocol	74
Modular QoS (MQC)	75

CHAPTER 7

Cisco IOS XE Installation Methods	77
Bundle Mode versus Install Mode	77
Installing the Software using install Commands	77
Restrictions for Installing the Software Using install Commands	78
Install Mode Support	78
Information About Installing the Software Using install Commands	79
Install Mode Process Flow	80
Booting the Platform in Install Mode	84
One-Step Installation OR Converting from Bundle Mode to Install Mode	85
Three-Step Installation	86
Upgrading in Install Mode	88
Downgrading in Install Mode	88
Terminating a Software Installation	88

Configuration Examples	88
One Step Installation	88
Three Step Installation	90
Showing the Installed Packages	92
Showing Committed and Uncommitted Packages	93
Removing Inactive Packages	93
Troubleshooting Software Installation Using install Commands	94

CHAPTER 8**Installing the Software 97**

Overview	97
Licensing	97
Cisco Software Licensing	98
Consolidated Packages	98
License Installation on the ESR6300	98
Network-Essentials	99
Network-Advantage	100
Feature Support Caveats	100
How to Install the Software for Cisco IOS XE	101
Booting from the USB Feature Summary	102
Booting from ROMMON	102
Upgrading the Cisco IOS XE Release	102
IOS XE Downgrade Warning	104
ROMMON Images	104
File Systems	105
Auto-generated File Directories and Files	105
Flash Storage	106
LED Indicators	106

CHAPTER 9**Smart Licensing Using Policy 107**

SLP Overview	107
License Enforcement Types	109
High Security (HSEC) License	109
SLP Architecture	111
Product Instance	111

- Cisco Smart Software Manager (CSSM) 111
- Cisco Smart Licensing Utility (CSLU) 112
- Customer Topologies 112
- License Installation Procedure - Full Offline Access Topology 113
 - Procedure to Register Product Instance in CSSM 113
 - Importing the ACK file from CSSM to your Device 116
 - Removing the Device from CSSM 118
- License Installation Procedure - CSLU has No Access to CSSM 118
 - Procedure when devices are connected to the CSLU 119
 - Exporting the AuthRequest File to CSSM 122
 - Uploading the Authorization Request Code file into CSLU 128
 - License Installation Process in the Router 129
 - HSEC Installation 131
- Change to Smart Licensing Packaging 132
- Uncapped License Implementation 135

CHAPTER 10

- Configuring Ethernet Switch Ports 137**
 - Configuring VLANs 137
 - VLAN Trunking Protocol (VTP) 138
 - Configuring 802.1x Authentication 138
 - Configuring Spanning Tree Protocol 140
 - Configuring MAC Address Table Manipulation 141
 - Configuring Switch Port Analyzer 142
 - Configuring IGMP Snooping 143

CHAPTER 11

- Gigabit Ethernet Combo Ports WAN 145**
 - Gigabit Ethernet Combo Ports WAN 145
 - Command Line Interface 146

CHAPTER 12

- SD-WAN Remote Access 149**
 - SD-WAN 149

CHAPTER 13

- CLI Output for the FN980 5G Modem 151**
 - Change in CLI Output for the FN980 5G Modem 151

CHAPTER 14	MAB 802-1x Support	153
	MAB 802.1x Support	153

CHAPTER 15	Enable Secure Data Wipe Capabilities	155
	Enable Secure Data Wipe Capabilities	155

CHAPTER 16	Implementing Multicast Service Reflection	157
	Multicast Service Reflection Overview	157
	Prerequisites for Implementing Multicast Service Reflection	157
	Restrictions for Implementing Multicast Service Reflection	157
	Information About Implementing Multicast Service Reflection	158
	Benefits of Implementing Multicast Service Reflection	158
	Rendezvous Point (RP)	158
	Vif1 Interface	159
	Multicast Service Reflection Application	159
	How to Implement Multicast Service Reflection	160
	Configuring Multicast Service Reflection	160
	Configuration Examples for Multicast Service Reflection	162
	Example Multicast-to-Multicast Destination Translation	162
	Example Multicast-to-Unicast Destination Translation	163
	Example Multicast-to-Multicast Destination Splitting	165
	Example Multicast-to-Unicast Destination Splitting	167

CHAPTER 17	Cellular Boot Time Improvements	171
	Cellular Boot Time Improvements	171

CHAPTER 18	Cellular Pluggable Interface Module Configuration Guide	173
-------------------	--	------------

CHAPTER 19	Radio Aware Routing and Dynamic Link Exchange Protocol	175
	Overview of Radio Aware Routing	176
	Benefits of Radio Aware Routing	177
	Restrictions and Limitations	178

Performance	178
System Components	178
Radio Aware Routing Topology	179
QoS Provisioning on PPPoE Extension Session	182
Example: Configuring the RAR Feature in Bypass Mode	183
Verifying RAR Session Details	184
Overview of DLEP	190
DLEP Topology and Packet Flow	190
License Requirements	192
Configuring DLEP with OSPFv3	192
Configuring the Virtual Multipoint Interface	193
Configuring the Virtual Template	194
Configuring the Physical Interface	195
DLEP Configuration Modes	196
Configure DLEP Client/Server Based On Port Number	197
Configure DLEP with Dynamic Port on Server (Router)	197
Attach DLEP Template in Discovery Mode	199
Using a DLEP Template with a Well-Known IP Address	200
DLEP Configuration with GTSM	202
Configuring DLEP with OSPFv3	202
Configuring DLEP with EIGRP	204
DLEP with Quality of Service (QoS)	205
Edit the Virtual-Template	209
Configuring DLEP on a Sub-Interface	210
Removing the DLEP Configuration	212
Configuring DLEP using the Web User Interface (WebUI)	213
DLEP Validation Commands	217
Optional Configurations for DLEP	219
DLEP IPv6 Unicast	220
IPv4 and IPv6 Multicast Over DLEP	221
IPv6 Control Plane for DLEP	222
Clearing DLEP Clients and Neighbors	222
Troubleshooting with show commands	223
Troubleshooting with debug commands	226

Additional Debug Commands	233
SNMP MIB Support for DLEP	234
Related Documentation	239

CHAPTER 20

IPv6 Multicast Over PPPoE	241
PPPoE in MANET	241
Feature Requirements	244
Enabling IPv6 Routing	245
Creating a Subscriber Profile	245
Configuring License Level	246
Configuring PPPoE Service Policy	246
Configuring QoS Provisioning	247
Configuring PPPoE Service Selection	247
Configuring PPPoE on an Ethernet Interface	248
Configuring a Virtual Template Interface	248
Configuring VMI interface and Enabling Multicast Support	250
Configuring the Loopback Interface	251
Configuring the OSPFv3 IPv4 Address Family Process	252
Configuring the OSPFv3 IPv6 Address Family Process	253
Configuring IPv6 PIM Bootstrap Router (BSR)	254
Configuring IPv6 Multicast Group	254
Verifying Virtual Template Interface	255
Verifying PPPoE Session Details	256
Verifying BSR Election	257
IPv6 Multicast Routing Table	258
IPv6 Multicast over PPPoE	259
Verifying VMI Neighbors	259
Verifying OSPF Neighbor	261
Sample Running Configuration	261
Debug Commands	265

CHAPTER 21

Implementation Options	267
SFP Overview	267
SFP Command Line	268

Power over Ethernet 268

 Device Detection and Power Allocation 269

 CLI for PoE 269

Working with External USB3.0 271

CHAPTER 22 **ROM Monitor Overview and Basic Procedures 273**

 ROM Monitor Overview 273

 Access ROM Monitor Mode 274

 Checking the Current ROMMON Version 274

 Commonly Used ROM Monitor Commands 275

 ROMMON Command Examples 276

 Changing the ROM Monitor Prompt 276

 Displaying the Configuration Register Setting 276

 Environment Variable Settings 277

 Frequently Used Environmental Variables 277

 Displaying Environment Variable Settings 277

 Entering Environment Variable Settings 277

 Saving Environment Variable Settings 278

 Exiting ROM Monitor Mode 278

 Configuration Example 278

 Upgrading the ROMMON for a Router 279

CHAPTER 23 **Device Zeroization 281**

 Push Button 281

 Microcontroller Unit (MCU) 282

 Device Zeroization 282

 Zeroization Trigger 283

 Command Line Interface 284

 Zeroization Support in bootloader 285

 Troubleshooting Zeroization 285

CHAPTER 24 **Call Manager Express 287**

 Call Manager Express Overview 287

 SCCP Configuration Example 287

SCCP Show Command Example 288

SIP Configuration Example 289

Debug Commands 290

SIP Show Command Example 290

CHAPTER 25

Troubleshooting 293

Getting Started with Troubleshooting 293

Understanding Diagnostic Mode 293

Before Contacting Cisco or Your Reseller 294

show interfaces Troubleshooting Command 294

Software Upgrade Methods 294

Recovering a Lost Password 295

 Change the Configuration Register 295

 Configuring the Configuration Register for Autoboot 296

 Reset the Router 296

 Reset the Password and Save Your Changes 297

 Reset the Configuration Register Value 298

 Configuring a Console Port Transport Map 299

 Viewing Console Port, SSH, and Telnet Handling Configurations 300

 Using the factory reset Commands 302

CHAPTER 26

System Messages 303

Information About Process Management 303

How to Find Error Message Details 303

CHAPTER 27

Process Health Monitoring 309

Monitoring Control Plane Resources 309

 Avoiding Problems Through Regular Monitoring 309

 Cisco IOS XE Process Resources 309

 Overall Control Plane Resources 313

Monitoring Hardware Using Alarms 314

 Router Design and Monitoring Hardware 315

 BootFlash Disk Monitoring 315

Approaches for Monitoring Hardware Alarms 315

Viewing the Console or Syslog for Alarm Messages 315

Enabling the logging alarm Command 315

Network Management System Alerts a Network Administrator when an Alarm is Reported Through
SNMP 315

CHAPTER 28

Environmental Monitoring 317

Environmental Monitoring 317

Environmental Monitoring 317

Environmental Monitoring and Reporting Functions 318

Environmental Monitoring Functions 318

Environmental Reporting Functions 319

SNMP Polling of Temperature OID 325

Technical Assistance 326

Additional References 326

CHAPTER 29

Additional Information 327

Where to find Additional Information 327

Communications, Services, and Additional Information 327

Cisco Bug Search Tool 327

Documentation Feedback 328



CHAPTER 1

Overview

This section contains the following topics:

- [Introduction, on page 1](#)
- [Accessing the CLI Using a Router Console, on page 2](#)
- [Accessing the CLI from a Remote Console, on page 4](#)
- [CLI Session Management, on page 6](#)

Introduction

The ESR6300 is a compact form factor embedded router module with a board size of 3.0" x 3.75". This module may fit in an enclosure that is originally designed for PC/104 modules with some additional adaptation. The more compact design simplifies integration and offers system integrators the ability to use the Cisco ESR6300 in a wide variety of embedded applications. The ESR card is available in two options. The first is a Cisco-designed cooling plate customized to the ESR (ESR-6300-CON-K9). The second is without the cooling plate for system integrators who want to design their own custom thermal solution (ESR-6300-NCP-K9).

The ESR6300 runs IOS-XE, which is a Linux-based OS that comes with many enhancements and more features compared to the classic IOS version.



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.



Note IOx development is not supported on the ESR6300. While this is platform independent code, it is unsupported and untested on this device.

Complete details on the ESR6300 are found in the product data sheet that is located here:

<https://www.cisco.com/c/dam/en/us/products/routers/cisco-embedded-series-router-c78-742901.pdf>

Accessing the CLI Using a Router Console

The ESR6300 router provides access to a console port through USB and RS232 support.

If your laptop or PC warns you that you do not have the proper drivers to communicate with the router, you can obtain them from your computers manufacturer, or go here: <https://www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers>

On a device fresh from the factory, you are greeted with a System Configuration Dialog where you respond to basic configuration questions. If the router was ordered for the use of Cisco PnP connect services, in the case of centralized provisioning, the router skips the initial dialog. The following is an example:

```

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Router]: <your-host-name>

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: <your-password>

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: <your-password>

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: <your-password>
Setup account for accessing HTTP server? [yes]: <return>
  Username [admin]: <your-username>
  Password [cisco]: <your-password>
  Password is UNENCRYPTED.
  Configure SNMP Network Management? [no]: <return>

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0/0    172.27.168.161  YES NVRAM up             up
GigabitEthernet0/0/1    15.0.0.1        YES NVRAM administratively down  down
GigabitEthernet0/1/0    unassigned      YES unset administratively down  down
GigabitEthernet0/1/1    unassigned      YES unset administratively down  down
GigabitEthernet0/1/2    unassigned      YES unset administratively down  down
GigabitEthernet0/1/3    unassigned      YES unset administratively down  down
Async0/2/0              unassigned      YES unset up             down

```



```
VirtualPortGroup0    192.168.0.1      YES NVRAM up          up
Vlan1                unassigned      YES unset administratively down down
vmil                 unassigned      YES unset down        down
```

Names and IP addresses in this next section are shown as examples.

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface Vlan1:

```
Configure IP on this interface? [no]: yes
IP address for this interface: 192.168.1.1
Subnet mask for this interface [255.255.255.0] : <return>
Class C network is 192.168.1.0, 24 subnet bits; mask is /24
```

Would you like to configure DHCP? [yes/no]: **yes**

```
Enter DHCP pool name: wDHCPool
Enter DHCP network: 192.168.1.0
Enter DHCP netmask: 255.255.255.0
Enter Default router: 192.168.1.1
```

The following configuration command script was created:

```
hostname <your-hostname>
enable secret 9 $9$Z6f174fvoEdMgU$XZYs8l4phbqpXsb48l9bzCng3u4Bc2khlSTsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
no snmp-server
!
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!interface GigabitEthernet0/0/1
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2

interface GigabitEthernet0/1/3
!
interface Vlan1
no shutdown
ip address 192.168.1.1 255.255.255.0
no mop enabled
ip dhcp pool wDHCPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
end
```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

Enter your selection [2]: **2**
Building configuration...

[OK]
Use the enabled mode 'configure' command to modify this configuration.

```
Press RETURN to get started! <return>
```

```
*Jul 27 21:35:24.369: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-3211716068
has been generated or imported by crypto-engine
*Jul 27 21:35:24.372: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 27 21:35:24.448: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
*Jul 27 21:35:24.532: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named
TP-self-signed-3211716068.server has been generated or imported by crypto-engine
hostname>
```

The device now has a basic configuration that you can build upon.

Using the Console Interface

Step 1 Enter the following command:

```
Router > enable
```

Step 2 (Go to Step 3 if the enable password has not been configured.) At the password prompt, enter your system password:

```
Password: enablepass
```

When your password is accepted, the privileged EXEC mode prompt is displayed.

```
Router#
```

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

Step 3 To exit the console session, enter the **quit** command:

```
Router# quit
```

Accessing the CLI from a Remote Console

The remote console of the ESR6300 can be accessed through Telnet or the more secure SSH. Details on telnet access follow in this chapter. For details on SSH access see the SSH chapter located here: [Secure Shell, on page 37](#)

The following topics describe the procedure to access the CLI from a remote console:

Preparing to Connect to the Router Console Using Telnet

See the Cisco IOS-XE Device hardening guide at <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html> for details.

Configuring the diagnostic and wait banners is optional, but recommended. The banners are especially useful as indicators to users about the status of their Telnet or SSH attempts.

To access the router remotely using Telnet from a TCP/IP network, configure the router to support virtual terminal lines using the **line vty** global configuration command. Configure the virtual terminal lines to require users to log in and specify a password.

See the [Cisco IOS Terminal Services Command Reference](#) document for more information about the **line vty global** configuration command.

To prevent disabling login on a line, specify a password with the **password** command when you configure the **login** command.

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a 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: Secure Connectivity](#) and the [Cisco IOS Security Command Reference](#) documents. For more information about the **login line-configuration** command, see the [Cisco IOS Terminal Services Command Reference](#) document.

In addition, before you make a Telnet connection to the router, you must have a valid hostname for the router or have an IP address configured on the router. For more information about the 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

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

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

Here, *host* is the router hostname or IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information about these commands, see the [Cisco IOS Terminal Services Command Reference](#) document.

Note If you are using an access server, 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 how to use the **telnet** command to connect to a router named **router**:

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

Step 2 Enter your login password:

```
User Access Verification
Password: mypassword
```

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

Step 3 From user EXEC mode, enter the **enable** command:

```
Router> enable
```

- Step 4** At the password prompt, enter your system password:
Password: **enablepass**
- Step 5** When the **enable** password is accepted, the privileged EXEC mode prompt is displayed:
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.
Router# **logout**
-

CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

Changing the CLI Session Timeout

- Step 1** `configure terminal`
Enters global configuration mode
- Step 2** `line console 0`
- Step 3** `session-timeout minutes`
The value of *minutes* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *minutes* to disable session timeout.
- Step 4** `show line console 0`
Verifies the value to which the session timeout has been set, which is shown as the value for " Idle Session ".
-

Locking a CLI Session

Before you begin

To configure a temporary password on a CLI session, use the **lock** command in EXEC mode. Before you can use the **lock** command, you need to configure the line using the **lockable** command. In this example the line is configured as **lockable**, and then the **lock** command is used and a temporary password is assigned.

- Step 1** Router# `configure terminal`
Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the **lock** command.

```
Router(config)# line console 0
```

Step 3 Router(config)# lockable

Enables the line to be locked.

Step 4 Router(config)# exit

Step 5 Router# lock

The system prompts you for a password, which you must enter twice.

```
Password: <password>
```

```
Again: <password>
```

```
Locked
```



CHAPTER 2

New Features

- [New Features for Cisco IOS XE 17.14.1a, on page 9](#)
- [New Features for Cisco IOS XE 17.13.1, on page 9](#)
- [New Features for Cisco IOS XE 17.12.1a, on page 10](#)
- [New Features for Cisco IOS XE 17.11.1a, on page 10](#)
- [New Features for Cisco IOS XE 17.10.1a, on page 10](#)
- [New Features for Cisco IOS XE 17.9.1, on page 10](#)
- [New Features for Cisco IOS-XE 17.8.1, on page 11](#)
- [New Features for Cisco IOS-XE 17.7.1, on page 13](#)
- [New Features for Cisco IOS-XE 17.6.1, on page 14](#)
- [New Features for Cisco IOS-XE 17.5.1, on page 14](#)
- [New Features for Cisco IOS-XE 17.4.1, on page 20](#)
- [New Features for Cisco IOS-XE 17.3.1, on page 20](#)
- [New Features for Cisco IOS-XE 17.2.1, on page 23](#)

New Features for Cisco IOS XE 17.14.1a

New features in this release are listed below:

- [SNMP MIB Support for DLEP](#)

New Features for Cisco IOS XE 17.13.1

This chapter contains the following sections:

- [IPv4 and IPv6 Multicast Over DLEP](#)
- [IPv6 Control Plane for DLEP](#)
- [SD-WAN](#)
- [Change in CLI Output for the FN980 5G Modem](#)

New Features for Cisco IOS XE 17.12.1a

This chapter contains the following sections:

- [DLEP IPv6 Unicast](#)
- [Uncapped License Implementation](#)

New Features for Cisco IOS XE 17.11.1a

This chapter contains the following sections:

- [Change to Smart Licensing Packaging](#)
- [Galileo Support on the LTE Pluggable Modules](#)

New Features for Cisco IOS XE 17.10.1a

This chapter contains the following sections:

- [Support for the P-5GS6-GL Pluggable Module on the ESR6300](#)
- [MAB 802.1x Support](#)
- [Enable Secure Data Wipe Capabilities](#)
- [Rawsocket Keepalive Configuration CLI](#)

New Features for Cisco IOS XE 17.9.1

This chapter contains the following sections:

- [Install Mode Support](#)
- [Cellular Boot Time Improvements](#)
- [IOS XE Downgrade Warning](#)
- [SNMP Polling of Temperature OID](#)
- [GPS Mode Enabled By Default](#)
- [Cisco WebUI Access Point Name \(APN\)](#)
- [IPv6 Multicast over PPPoE](#)

New Features for Cisco IOS-XE 17.8.1

Cellular Serviceability Enhancements

Enhancements have been made for cellular and GPS features as follows:

Trigger points and debug code can be enabled via controller cellular CLIs for generating and trap the debug data automatically without manual intervention. The following CLI options are available:

```
(config-controller)#lte modem serviceability ?
gps                GPS debugging
interface-resets   Interface resets/Bearer deletion
modem-crash        Modem-crash debugging
modem-resets       IOS initiated unknown modem-resets
```

The debug data includes the following:

- Context Based debug logs (tracebacks, and GPS locations).
- Well formatted debug messages.
- Vendor specific debug data at a broader range.

The debug logs are located in the following location of flash:

```
router#dir flash:servelogs
Directory of bootflash:/servelogs/

259340  -rw-                122   Sep 7 2021 17:40:44 +00:00  gpslog-slot5-20210907-174044
259339  -rw-                1734  Sep 7 2021 12:14:07 +00:00  celllog-slot5-20210905-164628
```

GPS and cellular log files are created separately with file names using the timestamp at the time of the creation. These files are created as follows:

- If the existing file has reached 10Mb, a new file will be created.
- A new file will be created if the feature (GPS, or cellular) is completely disabled, and then re-enabled.

GNMI Broker (GNMIB) Update

The GNMI Broker (GNMIB) has been extended to support the gRPC Network Operations Interface (gNOI) reset.proto service. This service provides functionality for restoring the device to its factory defaults via gRPC.

When the service is executed, it behaves similarly to the 'factory-reset all' command, and subsequently triggering a reload. Additionally, the service will maintain the current booted image. The additional steps below will be taken to comply with the reset.proto service:

- Set the rommon BOOT variable to the current booted image and maintain it through reload following factory-reset
- Enable autoboot to bring the device up on the current booted image following factory-reset.

gRPC Network Operations Interface Update

gNOI is the gRPC Network Operations Interface. gNOI defines a set of gRPC-based microservices for executing operational commands and procedure on network devices, such as OS Install, Activate, and Verification.

Through gNOI `os.proto` will be possible to perform operating system related tasks such as OS activation, install, detailed overview, internal OS commands, and finally to output a summary of OS operations.

Furthermore, gNOI `os.proto` can also be used to display the gnmib detailed state, check the gnmib operational statistics, and also to output modifiers.

Raw Socket Feature Enhancement

This enhancement allows the user to input the maximum number of retries available to the write socket. The range of the number of retries goes from 1 to 1000. The default number of retries is 10. To accommodate this feature, a new CLI has been created, **raw-socket tcp max-retries <1-1000>**. <1-1000> is the maximum number of retries.

SCADA Enhancement for TNB

This enhancement provides compatibility with TNB's WG RTUs, including the following:

- TNB RTUs require Reset-Link message to be sent out along with Link-Status message to ensure correct initialization of the serial. The feature can be selectively turned on using the new configuration CLI **scada-gw protocol force reset-link**.
- When clock passthru is enabled and if the router hasn't received the timestamp from the DNP3-IP master, the router's hardware time will be sent downstream to RTU. Upon receiving a new timestamp from DNP3-IP master, the router will start sending the new timestamp sourced from DNP3-IP master to RTU.
- The number of bufferable DNP3 events in memory will be increased from 600 to 10000.
- The **scada-gw protocol interlock** command will be supported for DNP3. Previously, the support only existed for T101/T104. With this new enhancement, the router will disconnect Serial link if the DNP3-IP master is down or unreachable. Similarly, when the Serial link to RTU is down, the TCP connection to DNP3-IP master will be untethered.
- Custom "requests" will be automatically ordered based on priority so that the user can specify them in any order that they would like to.

DLEP and Credit Based Radio Aware Routing Support

DLEP Support

DLEP addresses the challenges faced when merging IP routing and radio frequency (RF) communications. Cisco provides capabilities that enable:

- Optimal route selection based on feedback from radios
- Faster convergence when nodes join and leave the network
- Efficient integration of point-to-point, point-to-multipoint and broadcast multi-access radio topologies with multi-hop routing

- Flow-controlled communications between the radio and its partner router using rate-based Quality of Service (QoS) policies
- Dynamic shaping of fluctuating RF bandwidth in near real time to provide optimized use of actual RF bandwidth

Credit Based Radio Aware Routing Support

Radio-Aware Routing (RAR) is a mechanism that uses radios to interact with the routing protocol OSPFv3 to signal the appearance, disappearance, and link conditions of one-hop routing neighbors.

In a large mobile networks, connections to the routing neighbors are often interrupted due to distance and radio obstructions. When these signals do not reach the routing protocols, protocol timers are used to update the status of a neighbor. Routing protocols have lengthy timer, which is not recommended in mobile networks.

PPPoE extensions are used when the router communicates with the radio. In the Cisco IOS implementation of PPPoE, each individual session is represented by virtual access interface (connectivity to a radio neighbor) on which, QoS can be applied with these PPPoE extensions.

RFC5578 provides extensions to PPPoE to support credit-based flow control and session-based real time link metrics, which are very useful for connections with variable bandwidth and limited buffering capabilities (such as radio links).

Complete details can be found in [Radio Aware Routing and Dynamic Link Exchange Protocol](#)

New Features for Cisco IOS-XE 17.7.1

LTE Support for ESR6300

Cisco IOS-XE Release 17.7.1 adds support for LTE modules on the ESR6300 platform in slot 3. The related interface is Cellular 0/3/0.

ESR6300 will only support the following LTE modules:

- P-LTE-MNA (WP7610 modem)
- P-LTEA-LA (EM7430 modem)
- P-LTEA-EA (EM7455 modem)
- P-LTEAP18-GL (LM960 modem)

The cellular interface/module configuration will follow the same as on any other Polaris IOS-XE based platform and LTE modem.

Support 1G SFPs

Release 17.7.1 will add support for the following SFPs:

GLC-T-RGD

CWDM-SFP-1470=

CWDM-SFP-1610=

CWDM-SFP-1530=
DWDM-SFP-3033=
DWDM-SFP-3112=
GLC-BX-D-I=
GLC-BX-U-I=
GLC-TE

New Features for Cisco IOS-XE 17.6.1

Additional SFF Support

A Small Form Factor (SFF) transceiver is an optical transceiver that is soldered onto the PCB. It tends to be smaller in size than traditional SFPs.

There was a need for the ESR6300 to support SFFs in order to meet high vibration and shock requirements that can't be met with traditional SFPs. Therefore, support was added in 17.6.1 for the Finisar FTE8501K1LTN.

Since, this is not a Cisco transceiver, the end-user will need to use the **service unsupported-transceiver** CLI in order to get the router to accept and initialize the SFF.

Functionally, an SFF operates in the same way as an SFP.

VXLAN support

This feature functions the same as it does on the IR1101 running 17.5.1

See the section on VXLAN in the [IR1101 Software Configuration Guide](#).

New Features for Cisco IOS-XE 17.5.1

RFC4884 ICMPv6 and MPLSv6

RFC 4884 redefines selected ICMP error messages to support multi-part operation.

A multi-part ICMP message carries all of the information that ICMP messages carried previously, as well as additional information that applications may require.

RFC 4884 feature introduces an 8-bit length attribute to the following ICMPv6 messages with extensions.

- Destination Unreachable (type = 1)
- Time Exceeded (type = 3)

As part of RFC 4884 feature, for applications like MPLS/trace route which add extensions to type 1 and type 3 ICMPv6 error messages, original datagram length will be added in ICMPv6 header.

Also, infra is added as part of RFC 4884 support. If any new application is adding extensions it has to call defined registries to be compliant with RFC 4884.

Backward compatibility is also taken care of as part of this feature.

This feature is enabled by default and a CLI *[no]* **ipv6 icmp od-length enable** is provided which is enabled by default.

Command Example

```
ipv6 icmp od-length enable
```

Limitations

RFC4884 ICMP v4 and MPLS v4 extensions will be supported in the IOS-XE 17.6.1 release.

Netboot Support

The Netboot (TFTP boot) feature is now supported on the ESR6300. The ESR6300 has two Combo ports, Copper and Fiber ports (SFP) ports that support TFTP boot.

The Netboot (TFTP boot) feature allows the user to recover their router in the case that there is no image in the bootflash or USB.

The following configuration needs to be in place in ROMMON:

- WAN port Gigabit-Ethernet 0/0/0 or 0/0/1 should be connected to a TFTP network
- Path to image should be in a TFTP directory
- set IP_ADDRESS=<IP address of router>
- set IP_SUBNET_MASK=<mask>
- set DEFAULT_GATEWAY=<IP address of gateway>
- boot tftp://<server IP address>/<path to image>

Alarm port Support on the ESR6300

There is one alarm port available on the ESR6300. The IOS name for the alarm port is Alarm Contact 0.

The following configuration commands are available in IOS:

- alarm contact 0 enable
- alarm contact 0 description
- alarm contact 0 severity
- alarm contact 0 trigger

The configuration commands also have their equivalent **no** prefaces.

Alarm Contact Command

The ESR6300 supports only one alarm contact, which is Alarm Contact 0. Options are described in the following table:

description	The description string is up to 80 alphanumeric characters in length and is included in any generated system messages.
severity	For severity, enter critical, major, minor or none. If you do not configure a severity, the default is minor.
trigger	For trigger, enter open or closed. If you do not configure a trigger, the alarm is triggered when the circuit is closed.
enable	Provides a mechanism for you to enable or disable alarm conditions for a port.

Alarm Trigger Command

The **trigger** command has two options as shown below:

closed	Assert alarm when contact is closed. Closed means that no current flows through the contact (normally open contact). The alarm is generated when current does flow.
open	Assert alarm when contact is open. Open means that the normal condition has current flowing through the contact (normally closed contact). The alarm is generated when the current stops flowing.



Note See the [Alarm Port Configuration Examples](#), on page 17 for command examples.

Alarm LEDs

The alarm LED behavior is described in the following table:

Severity	LED Status
Critical	Flashing Red
Major	Flashing Red
Minor	Red



Note The LED behavior depends on both the trigger configuration as well as the severity configuration. The LED behavior does not differentiate between the Critical and Major severity.

Alarm Port Configuration Examples

To configure the feature, the alarm contact 0 needs to be enabled first. Perform the following:

```
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#alarm contact 0 enable
Router(config)#alarm contact 0 description test
Router(config)#alarm contact 0 severity critical
```

Alarm Enable/Disable

The alarm needs to be enabled to configure the severity and trigger. The following example shows the errors when the alarm is not enabled:

```
Router(config)#alarm contact 0 trigger open
Alarm / Digital IO Port 0 is not enabled.

Router(config)#alarm contact 0 severity major
Alarm / Digital IO Port 0 is not enabled.
```

Enabling the Alarm and Setting the Severity

See the following example:

```
Router(config)#alarm contact 0 enable

Router(config)#alarm contact 0 severity ?
  critical  Critical alarm severity
  major    Major alarm severity
  minor    Minor alarm severity
  none     No alarm severity

Router(config)#alarm contact 0 severity major
Router(config)#end
Router#
*Oct 16 14:54:54.518: %IIOT_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External
alarm/digital IO port (External alarm contact on Motherboard) asserted

*Oct 16 14:54:54.518: %IIOT_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External
alarm/digital IO port (ASSERT) asserted
ha
*Oct 16 14:54:54.733: %SYS-5-CONFIG_I: Configured from console by cons
```

Viewing The Configuration

To view the configuration:

```
Router#show alarm
Alarm contact 0:
Description: External alarm contact on Motherboard
Status: Not Asserted
Application: Dry
Severity: major
Trigger: Open
Mode: Input
Router#

Router#show facility-alarm status
System Totals  Critical: 0  Major: 1  Minor: 0
```

Source -----	Time -----	Severity -----	Description [Index] -----
External alarm contact Motherboard [0]	Oct 16 2023 14:46:14	MAJOR	External alarm contact on
Async0/2/0 State Down [2]	Oct 15 2023 18:58:08	INFO	Physical Port Administrative
GigabitEthernet0/0/0 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/0/1 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/1/0 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/1 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/2 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/3 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
Cellular0/3/0 State Down [2]	Oct 15 2023 18:58:22	INFO	Physical Port Administrative
Cellular0/3/1 State Down [2]	Oct 15 2023 18:58:22	INFO	Physical Port Administrative

```
Router#
Router#show facility-alarm status major
System Totals Critical: 0 Major: 1 Minor: 0
```

Source -----	Time -----	Severity -----	Description [Index] -----
External alarm contact Motherboard [0]	Oct 16 2023 14:46:14	MAJOR	External alarm contact on

Alarm Trigger Commands

See the following example:

```
Router#show run | sec alarm
alarm contact 0 enable
alarm contact 0 trigger Open
logging alarm informational
Router#
Router#show alarm
Alarm contact 0:
  Description: External alarm contact on Motherboard
  Status:      Asserted
  Application: Dry
  Severity:    minor
  Trigger:     Open
  Mode:        Input
Router#
Router#show facility-alarm status
System Totals Critical: 0 Major: 0 Minor: 1
```


Source -----	Time -----	Severity -----	Description [Index] -----
External alarm contact Motherboard [0]	Oct 16 2023 14:54:54	MINOR	External alarm contact on
Async0/2/0 State Down [2]	Oct 15 2023 18:58:08	INFO	Physical Port Administrative
GigabitEthernet0/0/0 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/0/1 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/1/0 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/1 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/2 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/3 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
Cellular0/3/0 State Down [2]	Oct 15 2023 18:58:22	INFO	Physical Port Administrative
Cellular0/3/1 State Down [2]	Oct 15 2023 18:58:22	INFO	Physical Port Administrative

Router#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**alarm contact 0 trigger closed**

Router(config)#

*Oct 16 14:58:19.548: %IIOT_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External alarm/digital IO port (External alarm contact on Motherboard) cleared

*Oct 16 14:58:19.549: %IIOT_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External alarm/digital IO port (CLEAR) cleared

Router#**sh facility-alarm status**

System Totals Critical: 0 Major: 0 Minor: 0

Source -----	Time -----	Severity -----	Description [Index] -----
Async0/2/0 State Down [2]	Oct 15 2023 18:58:08	INFO	Physical Port Administrative
GigabitEthernet0/0/0 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/0/1 State Down [2]	Oct 15 2023 18:58:21	INFO	Physical Port Administrative
GigabitEthernet0/1/0 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative
GigabitEthernet0/1/1 State Down [2]	Oct 15 2023 18:58:20	INFO	Physical Port Administrative

```

GigabitEthernet0/1/2      Oct 15 2023 18:58:20   INFO      Physical Port Administrative
State Down [2]

GigabitEthernet0/1/3      Oct 15 2023 18:58:20   INFO      Physical Port Administrative
State Down [2]

Cellular0/3/0             Oct 15 2023 18:58:22   INFO      Physical Port Administrative
State Down [2]

Cellular0/3/1             Oct 15 2023 18:58:22   INFO      Physical Port Administrative
State Down [2]

Router#

Router#show alarm
Alarm contact 0:
  Description: External alarm contact on Motherboard
  Status:      Not Asserted
  Application: Dry
  Severity:    minor
  Trigger:     Closed
  Mode:        Input

```

New Features for Cisco IOS-XE 17.4.1

Plug and Play (PnP) Support

This release enables PnP to work the same as on the IR1101. See the [IR1101 Software Configuration Guide](#).

PnP Overview

The out of box configuration boots the platform up to the configuration wizard. The control stops at a prompt where the user is given an option to enter the startup configuration wizard or not. If the user does not have access to the router, or does not enter any options, PnP discovery kicks in. If the PnP agent successfully establishes a connection to the PnP Server, the device configurations are pushed from the Server. The platform gets configured according to the user preference.

If PnP is not setup for the Router, the WebUI is accessible without having to access the platform console.

New Features for Cisco IOS-XE 17.3.1

Support for Security-Enhanced Linux (SELinux)

Security-Enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. SELinux provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

SELinux enforces mandatory access control policies that confine user programs and system servers to the minimum amount of privilege they require to do their jobs. This reduces or eliminates the ability of these

programs and daemons to cause harm when compromised (for example, via buffer overflows or mis-configurations). This confinement mechanism operates independently of the traditional Linux access control mechanisms.

There are no additional requirements or configuration steps required to enable or operate the SELinux feature. The solution is enabled/operational by default as part of the base IOS-XE software on supported platforms.

The following are enhanced show commands that have been defined for viewing SELinux related audit logs.

show platform software audit all

show platform software audit summary

show platform software audit switch <<1-8> | active | standby> <FRU identifier from a drop-down list>

Command Examples

The following is a sample output of the **show software platform software audit summary** command:

```
Device# show platform software audit summary
=====
AUDIT LOG ON switch 1
-----
AVC Denial count: 58
=====
```

The following is a sample output of the **show software platform software audit all** command:

```
Device# show platform software audit all
=====
AUDIT LOG ON switch 1
-----
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
===== END =====
```

(output omitted for brevity)

The following is a sample output of the **show software platform software audit switch** command:

```
Device# show platform software audit switch active R0
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
```

```

scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====

```

Syslog Message Reference

Facility-Severity-Mnemonic

- %SELINUX-3-MISMATCH

Severity-Meaning

- ERROR LEVEL Log

Message Explanation

- A resource access was made by the process for which a resource access policy is not defined. The operation was flagged but not denied.

- The operation continued successfully and was not disrupted. A system log has been generated about the missing policy for resource access by the process as denied operation.

Recommended Action

- Please contact CISCO TAC with the following relevant information as attachments:
 - The message exactly as it appears on the console or in the system log.
 - Output of "show tech-support" (text file)
 - Archive of Btrace files from the box using the following command ("request platform software trace archive target <URL>") For Example: Device#**request platform software trace archive target flash:selinux_btrace_logs**

SD-WAN on the ESR6300

The ESR6300 supports SDWAN with release 17.3.1 or later. This release brings the ESR6300 into feature parity with the IR1101. The ESR6300 will require controller version 20.2 or later.

All of the available SDWAN documentation can be found here:

<https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html>

New Features for Cisco IOS-XE 17.2.1

Serial Port Support

Additional protocol capabilities have been added to the ESR6300 to bring it into feature compatibility with the IR1101. These include:

- SCADA Gateway functionality (IEC10x and DNP3)
- Raw Socket (TCP and UDP)
- Line Relay
- Reverse Telnet

All of the configuration and show commands will be the same as are available on the IR1101 platform.

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config.html

Boot from the USB

Support has been added in order to boot the device from configuration files located on the pluggable USB. Customized startup configuration files can be booted from IOS or from ROMMON.

Booting from IOS

The following configuration steps need to be taken in order to boot from the USB.

To display the boot options:

```
Router(config)#boot config ?
 bootflash:  URL of the config file
 flash:      URL of the config file
 nvram:      URL of the config file
 usbflash0:  URL of the config file
 webui:      URL of the config file
```

The syntax for the boot command is:

boot config usbflash0:*<file name>*

For example:

```
Router(config)#boot config usbflash0:startup-config
Router(config)#
Router#write memory
Building configuration...
[OK]
*Feb 10 10:20:11.990: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
```

The environment variable CONFIG_FILE in the following example confirms that the startup-config is set to boot from usbflash0.

```
Router#show boot
BOOT variable =
CONFIG_FILE variable = usbflash0:startup-config
BOOTLDR variable does not exist
Configuration register is 0x1820
Standby not ready to show bootvar
```

Booting from ROMMON

The following configuration steps need to be taken in order to boot from the USB.

From the ROMMON prompt, execute **set CONFIG_FILE=usbflash0:** *<filename>*

For example:

```
rommon 2 > set CONFIG_FILE=usbflash0:my_startuppcfg
rommon 3 > sync
rommon 4 > set
PS1=rommon ! >
MCU_UPGRADE=SKIP
THRPUT=
LICENSE_BOOT_LEVEL=
RET_2_RTS=
MCP_STARTUP_TRACEFLAGS=00000000:00000000
BSI=0
RANDOM_NUM=1275114933
BOOT=flash:Jun5_1.SSA,12
RET_2_RCALTS=951454376
CONFIG_FILE=usbflash0:my_startuppcfg
```

Continue booting the IOS image as usual from the ROMMON prompt.

Booting from the USB Feature Summary

- Once the CONFIG_FILE is set to a non-default value, the **nvr_{am}:startup-config** command is aliased to this new location.
- Any change made to the config file in usbflash will be reflected in nvr_{am}:startup-config as well.
- The EXEC command **erase nvr_{am}:startup-config** erases the contents of NVRAM, and deletes the file referenced by CONFIG_FILE variable.
- If the USB is unplugged after setting the **boot config usbflash0: <filename>** variable, then the day 0 default configuration will take effect.
- When the configuration is saved using the **copy system:running-config nvr_{am}:startup-config** command, the device saves a complete version of the configuration file to the location specified by the CONFIG_FILE environment variable, and a distilled version to NVRAM. A distilled version is one that does not contain access list information.



CHAPTER 3

Web User Interface

This section contains the following:

- [Web User Interface Management Overview](#), on page 27
- [Using Web User Interface for Day One Setup](#), on page 27
- [Configure LAN Settings](#), on page 28
- [Configure Primary WAN Settings](#), on page 29
- [Configure Secondary WAN Settings](#), on page 29
- [Configure Security Settings](#), on page 30
- [GPS Mode Enabled By Default](#), on page 31
- [Cisco WebUI Access Point Name \(APN\)](#), on page 31
- [Summary Screen](#), on page 34

Web User Interface Management Overview

You can access your router using a web user interface. The web user interface allows you to monitor router performance using an easy-to-read graphical interface. Most aspects of your router can be monitored using the web user interface which enables you to perform the following functions:

Using Web User Interface for Day One Setup

To configure the Web user interface:

-
- Step 1** Configure the HTTP server. By default, the HTTP server configuration should be present on the device. Ensure the configuration by checking if the **ip http server** and **ip http secure-server** commands are present in the running configuration.

```
Device #configure terminal
Device (config)#ip http server
Device (config)#ip http secure-server
```

- Step 2** Set up the authentication options to log into Web UI. You can use one of these methods to authenticate:
- a) You can authenticate using local database. To use a local database for Web UI authentication, ensure to have the **ip http authentication local** command in the running configuration. This command is preconfigured on the device. If the command is not present, configure the device as shown in this example:

```
Device #configure terminal
Device (config)#ip http authentication local
```

Note You need a user with privilege 15 to access the configuration screens on Web UI. If the privilege is less than 15, you can access only the Dashboard and Monitoring screens on Web UI.

To create a user account, use the **username** <username> **privilege** <privilege> **password 0** <passwordtext>

```
Device #configure terminal
Device (config)# username <username> privilege <privilege> password 0 <passwordtext>
```

- b) Authenticate using AAA options. To use AAA authentication for Web UI, ensure to configure 'ip http authentication aaa' on the device. Also, ensure that the required AAA server configuration is present on the device.

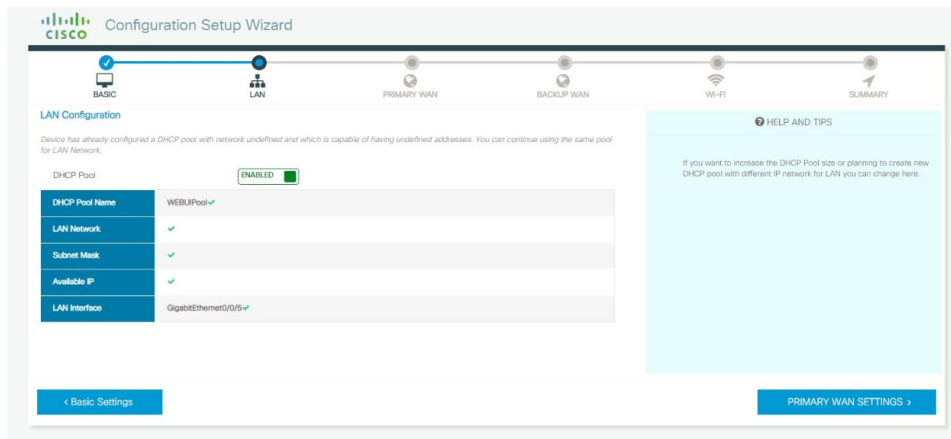
```
Device #configure terminal
Device (config)#ip http authentication local
```

- Step 3** Launch the browser. In the address bar, type the IP address of the device. For a secure connection, type `https://<your-ip-address>/webui/#/dayZeroRouting`
- Step 4** Enter the default username (cisco) and password provided with the device
- Step 5** Click **Log In**.

Configure LAN Settings

Refer to the following image for LAN Settings:

Figure 1: LAN Settings



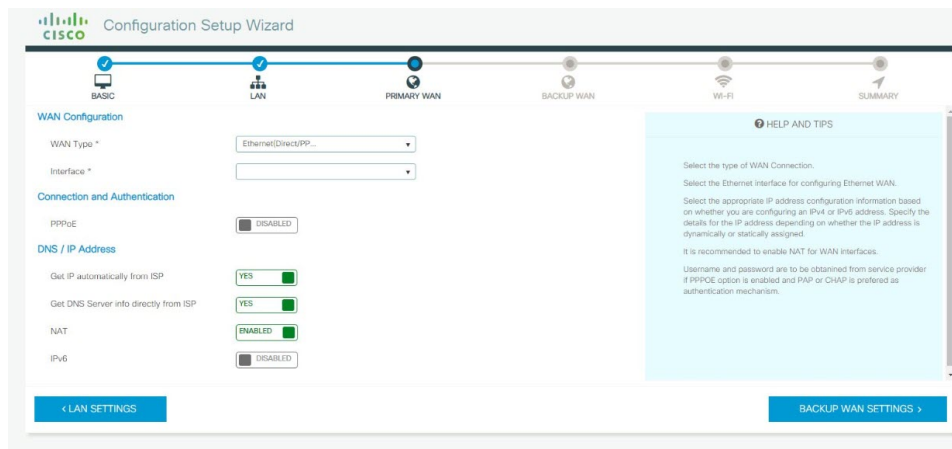
- Step 1** Select the interface from the drop-down list.
- Step 2** Enter the IP address and subnet mask.
- Step 3** **Note** Ensure that you do not use addresses that would conflict with what was previously created in the initial configuration dialog.

Check the **Use this as DHCP Server** check box, and enter the DHCP pool name and network address. Select the appropriate time zone from the drop-down list.

- Step 4** Check the **Configure Management Interface** check box, and enter the IP address of the management interface.
- Step 5** Click **Primary WAN Settings**.

Configure Primary WAN Settings

Refer to the following image for WAN Settings:

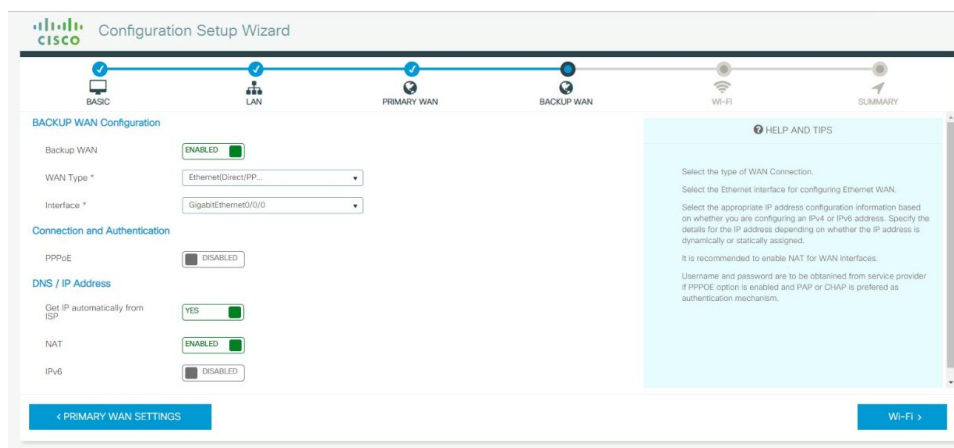


- Step 1** Select the primary WAN type for configuring the primary WAN connection. You can configure 3G/4G or Ethernet, as primary WAN depending on the WAN types supported by the router.
- Step 2** Select the interface from the drop-down list.
- Step 3** Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.
- Step 4** Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.
- Step 5** Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.
- Step 6** Enter the user name and password provided by the service provider.
- Step 7** Click **Security / APP Visibility WAN Settings**.

Configure Secondary WAN Settings

For advanced configuration, you should configure the secondary WAN connection. Refer to the following image for Backup WAN:

Figure 2: Backup WAN Settings



-
- Step 1** Select the secondary WAN type for configuring the secondary WAN connection. You can configure 3G/4G or Ethernet, as a secondary WAN depending on the WAN types supported by the router.
- Step 2** Select the interface from the drop-down list.
- Step 3** Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.
- Step 4** Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.
- Step 5** Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.
- Step 6** Enter the user name and password provided by the service provider.
-

Configure Security Settings

Before you begin

This screen only appears when Advanced Mode is selected at first launch.

-
- Step 1** Check the **Enable Cisco Recommended Security Settings** check box to ensure that all passwords are not shown in plain text. The passwords are encrypted.
- Step 2** Click **Day 0 Config Summary**.
- Step 3** To preview the configuration, click **CLI Preview**. After you preview the configuration, click **Finish** to complete the Day Zero setup.
-

GPS Mode Enabled By Default

In IOS XE versions prior to 17.9.1, GPS was enabled by default, however, GPS Mode was disabled by default. This required that the user perform an additional modem power-cycle after the router came up in order to use GPS.

Starting with IOS XE 17.9.1, GPS Mode will be enabled by default, and will be set to standalone mode. This will help reduce the cellular link up time.



Note This only applies to the cellular based GPS. This does not apply to the GPS/GNSS module in IR1800 (DR module), IR8140 (native GPS) and IR8340 (Timing module).

Use the following command to check cellular GPS status:

```
Router# show cellular <slot> gps
auto-reset Enable reset modem automatically after configuring GPS enable or mode
```

Cisco WebUI Access Point Name (APN)

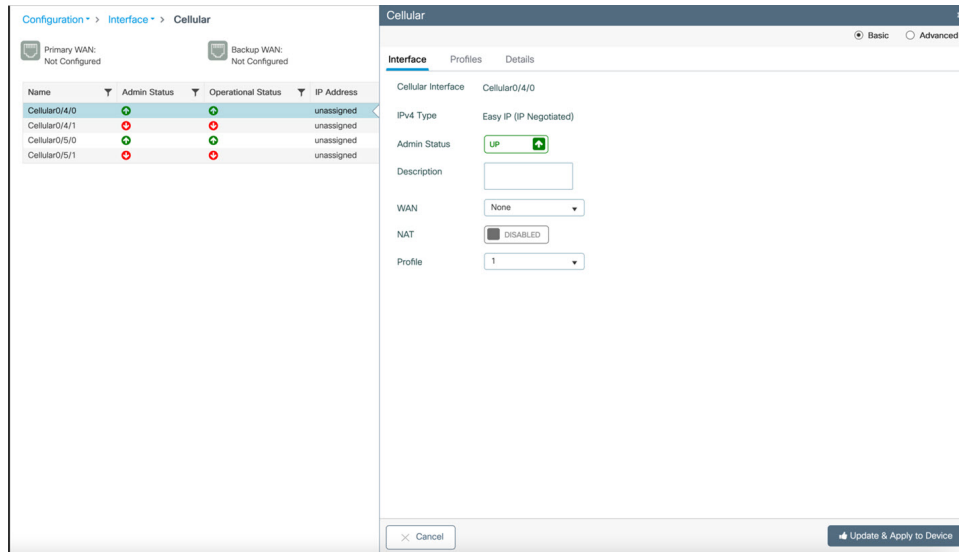
IOS XE 17.9.1 added the ability to add, edit, or delete the APN from the Cisco WebUI Interface. The following provides an overview of how to perform this function.



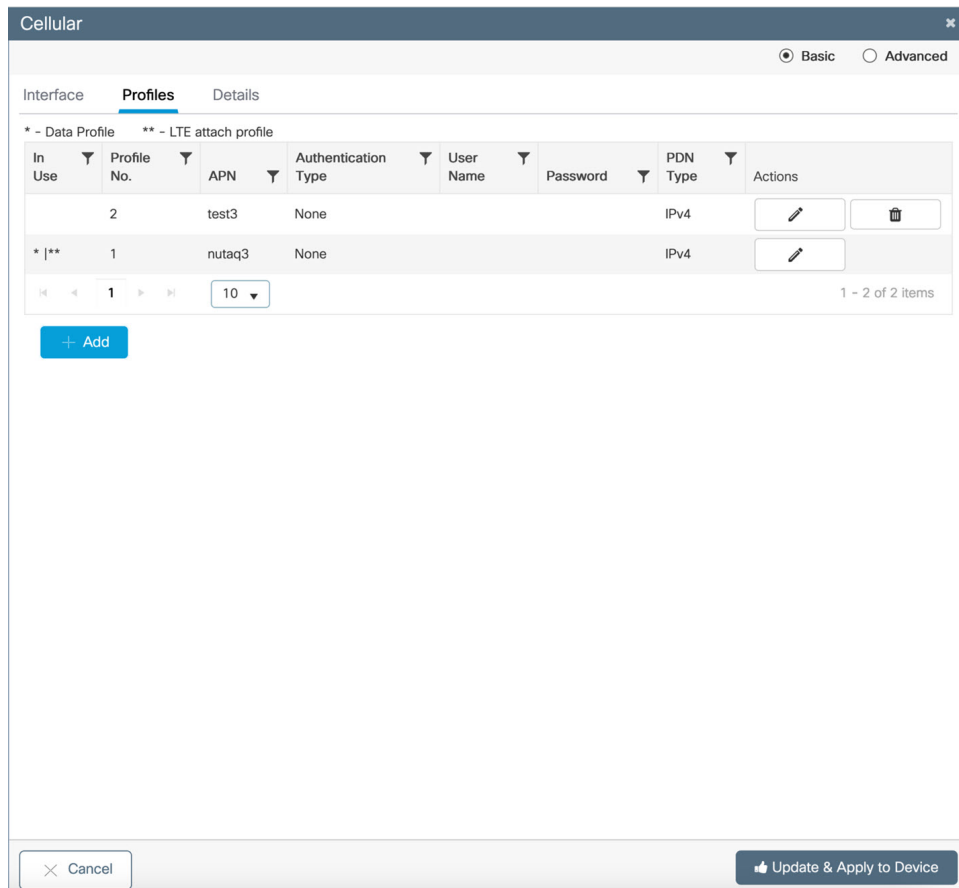
Note This section only describes new functionality and is not a complete overview of the WebUI.

Adding the APN

From the WebUI, navigate to **Configuration > Interface > Cellular**. Double click on the cellular interface based upon your platform.



On the Cellular window, click on the **Profiles** tab.



From the **Profiles** tab, you can Add, Delete, or Edit the APN. Once the profile is modified, click on **Update & Apply to Device** at the bottom of the window.

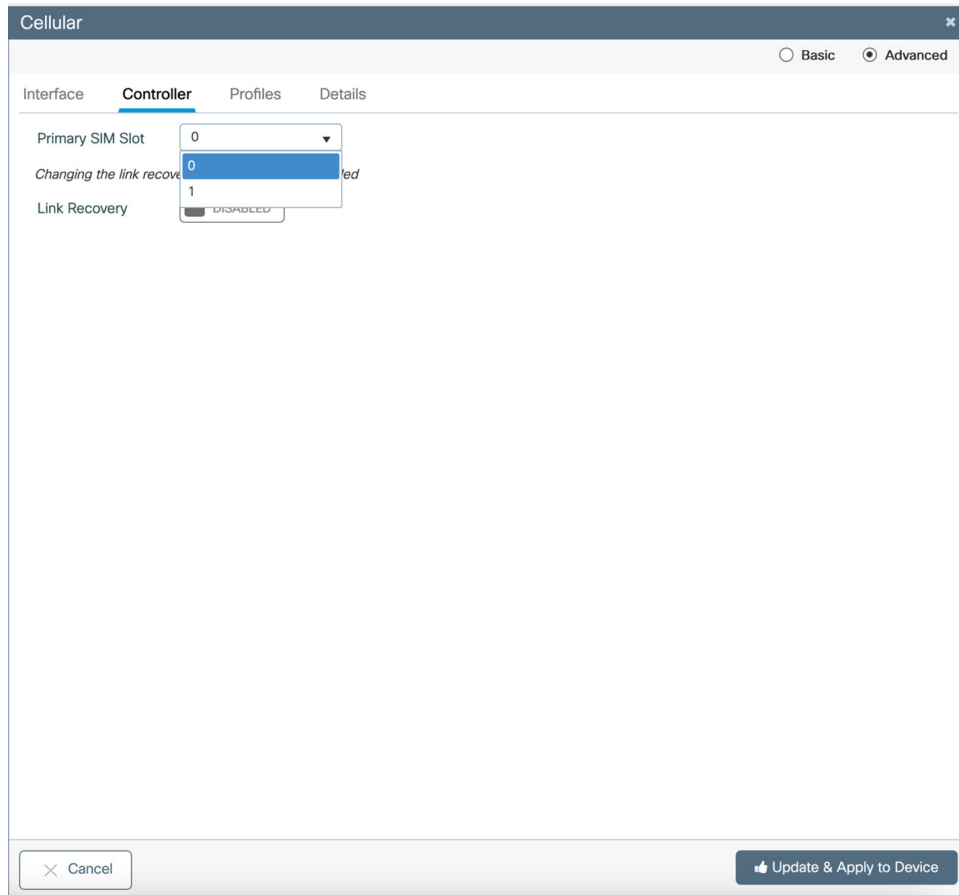
Changing the SIM Slot

By default, the APN is attached to SIM slot 0. You can change the APN to SIM slot 1 by using the WebUI. From the WebUI, navigate to **Configuration > Interface > Cellular**. Click on the **Advanced** radio button on the top of the window.

The screenshot shows the 'Cellular' configuration window in the 'Advanced' view. The 'Interface' tab is selected, showing configuration for 'Cellular0/4/0'. The 'Admin Status' is 'UP' and 'Dialer In-Band' is 'ENABLED'. The 'Data Profile' and 'Attach Profile' are both set to '1'. The 'Dialer Idle Timeout' is '0', 'Dialer Group' is '1', 'Pulse Time' is '1', and 'Load Interval' is '30'. The 'WAN' is set to 'None' and 'NAT' is 'DISABLED'. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

Parameter	Value
Cellular Interface	Cellular0/4/0
Data Profile	1
IPv4 Type	Easy IP (IP Negotiated)
Attach Profile	1
Admin Status	UP
Dialer In-Band	ENABLED
Description	
Dialer Idle Timeout	0
WAN	None
Dialer Group	1
NAT	DISABLED
Pulse Time	1
Load Interval	30

Click on the **Controller** tab at the top of the window.

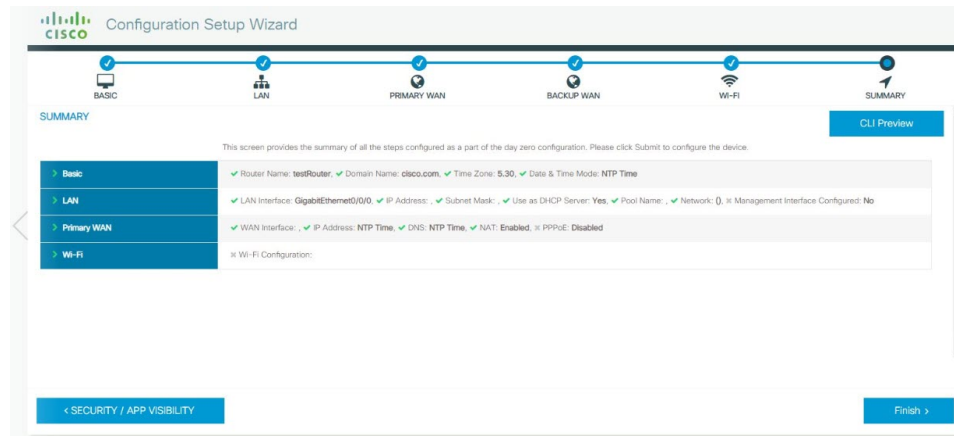


Click on the Primary SIM Slot pull-down and select slot 1. Click on **Update & Apply to Device** on the bottom of the window.

Summary Screen

Refer to the following image for the Router Summary:

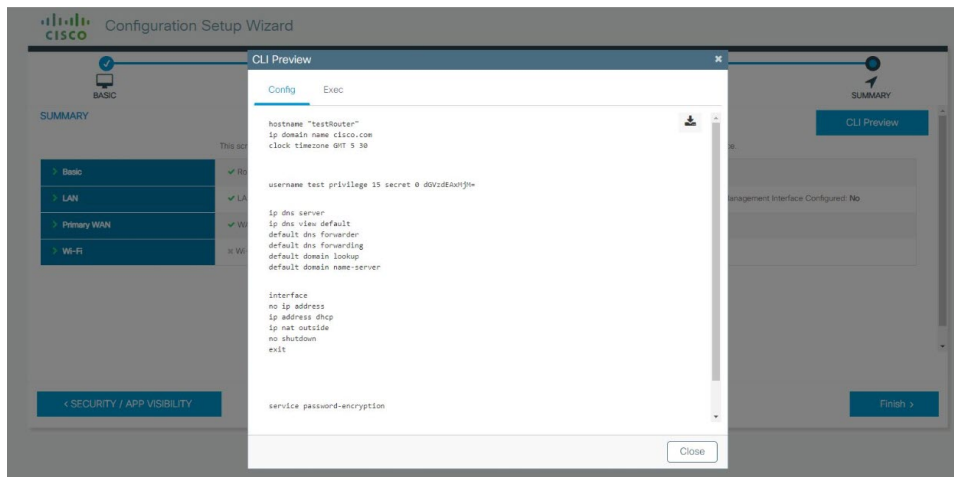
Figure 3: Summary Screen



Step 1 Review the settings that you have configured so far to verify they are accurate.

Step 2 If you wish to view the command line entries for your settings, you can click on **CLI Preview**. The following image shows an example:

Figure 4: CLI Settings



Step 3 Close the CLI Preview window.

Step 4 Click **Finish** to save all of your settings.



CHAPTER 4

Secure Shell

This section contains the following topics:

- [Information About Secure Shell, on page 37](#)
- [How to Configure Secure Shell, on page 39](#)
- [Information about Secure Copy, on page 45](#)
- [Additional References, on page 47](#)

Information About Secure Shell

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the device for secure shell (SSH):

- For SSH to work, the switch needs an RSA public/private key pair.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)
- Configure a hostname and host domain for your device by using the `hostname` and `ip domain-name` commands in global configuration mode. Use the **hostname** and **ip domain-name** commands in global configuration mode.

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the router for secure shell.

- The router supports RSA authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.



Note Cisco highly recommends the 3DES encryption as it is stronger. See the Cisco IOS-XE Device hardening guide at <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html> for details.

- This software release supports IP Security (IPSec).
- The router supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2, which Cisco recommends due to its better security.
- The `-l` keyword and `userid :{number} {ip-address}` delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

SSH And Router Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2). SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.



Note The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

SSH Configuration Guidelines

Follow these guidelines when configuring the device as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the **crypto key generate rsa global** configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command.
- When generating the RSA key pair, the message *No hostname specified* might appear. If it does, you must configure an IP hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message *No domain specified* might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

How to Configure Secure Shell

This section contains the following:

Setting Up the Router to Run SSH

Follow the procedure given below to set up your device to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *domain_name*
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	<code>router> enable</code>	
Step 2	configure terminal Example: <code>router# configure terminal</code>	Enters global configuration mode.
Step 3	hostname <i>hostname</i> Example: <code>router(config)# hostname your_hostname</code>	Configures a hostname and IP domain name for your device. Note Follow this procedure only if you are configuring the device as an SSH server.
Step 4	ip domain-name <i>domain_name</i> Example: <code>router(config)# ip domain-name your_domain_name</code>	Configures a host domain for your device.
Step 5	crypto key generate rsa Example: <code>router(config)# crypto key generate rsa</code>	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. Note Follow this procedure only if you are configuring the device as an SSH server.
Step 6	end Example: <code>router(config)# end</code>	Returns to privileged EXEC mode.
Step 7	show running-config Example: <code>router# show running-config</code>	Verifies your entries.
Step 8	copy running-config startup-config Example: <code>router# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuring the SSH Server

Follow these steps to configure the SSH server:



Note This procedure is only required if you are configuring the device as an SSH server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh version [2]**
4. **ip ssh {timeout *seconds* | authentication-retries *number*}**
5. Use one or both of the following:
 - **line vty *line_number* [ending line number]**
 - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

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	ip ssh version [2] Example: <pre>router(config)# ip ssh version 2</pre>	(Optional) Configures the device to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
Step 4	ip ssh {timeout <i>seconds</i> authentication-retries <i>number</i>} Example: <pre>router(config)# ip ssh timeout 90 ip ssh authentication-retries 2</pre>	Configures the SSH control parameters: <ul style="list-style-type: none"> • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After

	Command or Action	Purpose
		<p>the connection is established, the device uses the default time-out values of the CLI-based sessions.</p> <p>By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.</p> <ul style="list-style-type: none"> Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. <p>Repeat this step when configuring both parameters.</p>
Step 5	<p>Use one or both of the following:</p> <ul style="list-style-type: none"> line vty <i>line_number</i> [<i>ending line number</i>] transport input ssh <p>Example:</p> <pre>router(config)# line vty 1 10</pre> <p>or</p> <pre>router(config-line)# transport input ssh</pre>	<p>(Optional) Configures the virtual terminal line settings.</p> <ul style="list-style-type: none"> Enters line configuration mode to configure the virtual terminal line settings. For the <i>line_number</i> and <i>ending_line_number</i> arguments, the range is from 0 to 15. Specifies that the device prevents non-SSH Telnet connections, limiting the device to only SSH connections.
Step 6	<p>end</p> <p>Example:</p> <pre>router(config-line)# end</pre>	Exits line configuration mode and returns to privileged EXEC mode.
Step 7	<p>show running-config</p> <p>Example:</p> <pre>router# show running-config</pre>	Verifies your entries.
Step 8	<p>copy running-config startup-config</p> <p>Example:</p> <pre>router# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring the SSH Configuration and Status

Table 1: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

Configuring the Router for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The router then handles authentication and authorization. No accounting is available in this configuration.

Follow these steps to configure AAA to operate without a server by setting the router to implement AAA in local mode:



Note To secure the router for HTTP access by using AAA methods, you must configure the router with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the router for HTTP access by using AAA methods.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login default local`
5. `aaa authorization exec local`
6. `aaa authorization network local`
7. `username name privilege level password encryption-type password`
8. `end`
9. `show running-config`
10. `copy running-config startup-config`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example:	Enters global configuration mode.

	Command or Action	Purpose
	<code>router# configure terminal</code>	
Step 3	aaa new-model Example: <code>router(config)# aaa new-model</code>	Enables AAA
Step 4	aaa authentication login default local Example: <code>router(config)# aaa authentication login default local</code>	Sets the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports.
Step 5	aaa authorization exec local Example: <code>router(config-line)# aaa authorization exec local</code>	Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.
Step 6	aaa authorization network local Example: <code>router(config-line)# aaa authorization network local</code>	Configures user AAA authorization for all network-related service requests.
Step 7	username name privilege level password encryption-type password Example: <code>router(config-line)# username your_user_name privilege 1 password 7 secret567</code>	<p>Enters the local database, and establishes a username-based authentication system.</p> <p>Repeat this command for each user.</p> <ol style="list-style-type: none"> For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed. (Optional) For <i>level</i>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. For <i>encryption-type</i>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. For <i>password</i>, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
Step 8	end Example:	Exits line configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	<code>router(config-line)# end</code>	
Step 9	show running-config Example: <code>router# show running-config</code>	Verifies your entries.
Step 10	copy running-config startup-config Example: <code>router# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Information about Secure Copy

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provide a secure replacement for the Berkeley r-tools.

Prerequisites for Secure Copy

The following are the prerequisites for configuring the device for secure shell (SSH):

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an RSA key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.

Restrictions for Configuring Secure Copy

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.

Configuring Secure Copy

To configure the Cisco router for Secure Copy (SCP) server-side functionality, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {default | list-name} method1 [method2...]
5. **username** name [privilege level] **password** encryption-type encrypted-password
6. **ip scp server enable**
7. **exit**
8. **show running-config**
9. **debug ip scp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: router(config)# aaa new-model	Sets AAA authentication at login.
Step 4	aaa authentication login {default list-name} method1 [method2...] Example: router(config)# aaa authentication login default group tacacs+	Enables the AAA access control system.
Step 5	username name [privilege level] password encryption-type encrypted-password Example: router(config)# username superuser privilege 2 password 0 superpassword	Establishes a username-based authentication system. Note You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.

	Command or Action	Purpose
Step 6	ip scp server enable Example: <pre>router(config)# ip scp server enable</pre>	Enables SCP server-side functionality.
Step 7	exit Example: <pre>router(config)# exit</pre>	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	show running-config Example: <pre>router# show running-config</pre>	(Optional) Displays the SCP server-side functionality.
Step 9	debug ip scp Example: <pre>router# debug ip scp</pre>	(Optional) Troubleshoots SCP authentication problems.

Example

```
router# copy scp <somefile> your_username@remotehost:/<some/remote/directory>
```

Additional References

The following sections provide references related to the SSH feature.

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE: https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf
Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA.	Secure Shell Configuration Guide, Cisco IOS XE Gibraltar 16.11.x: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_secure_shell_ssh.html



CHAPTER 5

Using Cisco IOS XE Software

This chapter contains the following sections:

- [Understanding Command Modes, on page 49](#)
- [Using Keyboard Shortcuts, on page 51](#)
- [Using the no and default Forms of Commands, on page 51](#)
- [Using the History Buffer to Recall Commands, on page 52](#)
- [Managing Configuration Files, on page 52](#)
- [Saving Configuration Changes, on page 52](#)
- [Filtering Output from the show and more Commands, on page 53](#)
- [Using Cisco Feature Navigator, on page 54](#)
- [Finding Support Information for Platforms and Cisco Software Images, on page 54](#)
- [Getting Help, on page 54](#)
- [Finding Command Options: Example, on page 55](#)
- [Using Software Advisor, on page 58](#)
- [Using Software Release Notes, on page 58](#)

Understanding Command Modes

The command modes available in Cisco IOS XE are the same as those available in traditional Cisco IOS. 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 2: 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 command.	Router#	To return to user EXEC mode, use the disable command.
Global configuration	From privileged EXEC mode, use the configure terminal 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	The router boots up or accesses diagnostic mode in the following scenarios: <ul style="list-style-type: none"> • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy is configured using the transport-map command that directs a user into diagnostic mode. • A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) is entered and the router is configured to go to diagnostic mode when the break signal is received. 	Router (diag) #	If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI.

Command Mode	Access Method	Prompt	Exit Method
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.	rommon#>	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

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 3: Keyboard Shortcuts

Key Name	Purpose
Ctrl-B or the Left Arrow key	Move the cursor back one character.
Ctrl-F or the Right Arrow key	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.

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 from a **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.

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 4: History Substitution Commands

Command	Purpose
Ctrl-P or the Up Arrow key	Recalls 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	Returns 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, lists the last few commands you entered.

Managing Configuration Files

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 also used on several other Cisco router platforms.

IOS XE provides encryption of the configuration file. Encryption is discussed in length in the IOS XE hardening device guide which can be found here: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

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

The **copy** command can be used to back up startup configuration files.

For more detailed information on managing configuration files, see the “Managing Configuration Files” section in the [Cisco IOS XE Configuration Fundamentals Configuration Guide](#).

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
Destination filename [startup-config]? enter
Building configuration...
[OK]
```

```
IR1101#
*Sep 24 08:50:26.666: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
file
```



Note It may take a few minutes to save the configuration.

This task saves the configuration to the NVRAM.

Filtering Output from 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.

Example

In this example, a modifier of the **show interface** command (**include protocol**) is used to provide only the output lines in which the expression **protocol** is displayed:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
GigabitEthernet0/1/0 is down, line protocol is down (notconnect)
0 unknown protocol drops
GigabitEthernet0/1/1 is down, line protocol is down (notconnect)
0 unknown protocol drops
GigabitEthernet0/1/2 is down, line protocol is down (notconnect)
0 unknown protocol drops
GigabitEthernet0/1/3 is down, line protocol is down (notconnect)
0 unknown protocol drops
GigabitEthernet0/0/5 is up, line protocol is up (connected)
0 unknown protocol drops
Cellular0/4/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/4/1 is administratively down, line protocol is down
0 unknown protocol drops
Cellular0/5/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/5/1 is administratively down, line protocol is down
0 unknown protocol drops
Async0/2/0 is up, line protocol is down
0 unknown protocol drops
Vlan1 is up, line protocol is up , Autostate Enabled
0 unknown protocol drops
Vlan172 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
Vlan175 is down, line protocol is down , Autostate Enabled
0 unknown protocol drops
IR1800#
```

Using Cisco Feature Navigator

Use [Cisco Feature Navigator](#) to find information about platform support and software image support. Cisco Feature Navigator is a tool that enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To use the navigator tool, an account on Cisco.com is not required.

Finding Support Information for Platforms and Cisco Software Images

The Cisco IOS XE software is packaged in feature sets consisting of software images that support specific platforms.

All of the Cisco IOS-XE configuration guides can be found here: <https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html>.

The group of feature sets that are available for a specific platform depends 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 see the <https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html>.

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 that is specific to a command mode, a command, a keyword, or an argument, use one of the following commands.

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. Note There is no space between the command and the question mark.
abbreviated-command-entry <Tab>	Completes a partial command name.
?	Lists all the commands that are available for a particular command mode.

Command	Purpose
<code>command ?</code>	Lists the keywords or arguments that you must enter next on the command line. Note There is a space between the command and the question mark.

Finding Command Options: Example

This section provides information about how to display the 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 a part of a command followed by a space. The Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the **arap** command, you should 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 using the question mark (?) to assist you in entering commands.

Table 5: Finding Command Options

Command	Comment
<pre>Router> enable Password: <password> Router#</pre>	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#
<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	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)#
<pre>Router(config)# interface GigabitEthernet ? <0-0> GigabitEthernet interface number Router(config)# interface GigabitEthernet 0/? <0-5> Port Adapter number</pre>	Enter interface configuration mode by specifying the interface that you want to configure, using the interface GigabitEthernet global configuration command.
<pre>Router (config)# interface GigabitEthernet 0/0/? <0-63> GigabitEthernet interface number</pre>	Enter ? to display what you must enter next on the command line.
<pre>Router (config)# interface GigabitEthernet 0/0/0? . <0-71> Router(config-if)#</pre>	When the <cr> symbol is displayed, you can press Enter to complete the command. You are in interface configuration mode when the prompt changes to Router(config-if)#

Command	Comment
<pre> Router(config-if)# ? Interface configuration commands: . . . ip Interface Internet Protocol config commands Enable keepalive keepalive LAN Name command lan-name 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 interface. This example shows only some of the available interface configuration commands.</p>

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 cgmpp 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><cr> is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</p>

Command	Comment
<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><cr> is displayed. Press Enter to complete the command, or enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>Press Enter to complete the command.</p>

Using Software Advisor

Cisco maintains the Software Advisor tool. See [Tools and Resources](#). Use the Software Advisor tool to see if a feature is supported in 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. You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

See the release notes for information about the following:

- Product overview
- Open and resolved severity 1 and 2 caveats
- Software image names
- New features
- Known limitations

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. For cumulative feature information, refer to the Cisco Feature Navigator at:

<http://www.cisco.com/go/cfn/>.



CHAPTER 6

Basic Router Configuration

This chapter contains the following sections:

- [ESR6300 Interface Naming, on page 59](#)
- [Basic Configuration, on page 60](#)
- [Configuring Global Parameters, on page 65](#)
- [Serial Port Support, on page 66](#)
- [Rawsocket Keepalive Configuration CLI, on page 66](#)
- [Configuring the Gigabit Ethernet Interface, on page 67](#)
- [Configuring a Loopback Interface, on page 68](#)
- [Enabling Cisco Discovery Protocol, on page 69](#)
- [Configuring Command-Line Access, on page 69](#)
- [Configuring Static Routes, on page 71](#)
- [Configuring Dynamic Routes, on page 72](#)
- [Modular QoS \(MQC\), on page 75](#)

ESR6300 Interface Naming

The supported hardware interfaces and their naming conventions are in the following table:

Hardware Interface	IOS-XE Naming Convention
Gigabit Ethernet combo port WAN/Layer3	gigabitEthernet 0/0/0 gigabitEthernet 0/0/1
Gigabit Ethernet LAN/Layer 2 ports	gigabitEthernet 0/1/0 gigabitEthernet 0/1/1 gigabitEthernet 0/1/2 gigabitEthernet 0/1/3
Console Port	Line console 0
USB Port	usbflash0: (IOS and rommon)

Basic Configuration

The basic configuration is a result of the entries you made during the initial configuration dialog. This means the router has at least one interface set with an IP address to be reachable, either through WebUI or to allow the PnP process to work. Use the **show running-config** command to view the initial configuration, as shown in the following example:

```
Router# show running-config
Building configuration...

Current configuration : 13001 bytes
!
! Last configuration change at 12:17:45 UTC Wed Sep 25 2019
!
version 17.1
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform hardware throughput level 2G
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot system bootflash:c6300-universalk9.2019-09-23_04.57_gpollepa.SSA.bin
boot-end-marker
!
!
no logging monitor
!
aaa new-model
--More--
*Sep 25 23:53:59.524: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:!ex! e
!
aaa authentication enable default none
aaa authorization exec default local
!
aaa session-id common
clock timezone UTC -8 0
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
! address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
!
login on-success log
ipv6 unicast-routing
!
subscriber templating
!
multilink bundle-name authenticated
!
flow exporter 10.10.10.11
destination 10.10.10.11
!
crypto pki trustpoint SLA-TrustPoint
```

```

revocation-check crl
!
crypto pki trustpoint DNAC-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
!
crypto pki trustpoint TP-self-signed-2633875772
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2633875772
revocation-check none
rsaakeypair TP-self-signed-2633875772
!
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
crypto pki certificate chain DNAC-CA
crypto pki certificate chain TP-self-signed-2633875772
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 32363333 38373537 3732301E 170D3139 30393235 30303034
35305A17 0D333030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 36333338
37353737 32308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100E848 4E2F3B31 0FA018F3 32D29A16 D8FDD1E1 14820D00 1D9A0AEF
994283C8 938803DA 3344AF4E BB4E94CD A8FDD1B8 AE35DC14 97BB8EC6 DC475C5F
438D80A9 6EC125BE 77246D7C 7D3F15DA CA340EDE 238595C5 CE70A762 315934B4
CA08037A 83E31EFB 5D070986 3C2553C0 C5B63A45 3A1FE935 EF0F74E2 2D5AC8C8
F21408A8 6AE6C799 D0F882D1 A2CA684D 29DA01A3 A31527F1 C613FF3F 547CEC2F
82ADF5E5 9461AA9A 546448AC BB3D82B6 449D3BC0 C844C92B 9D951423 7869250E
936E1147 AF8C5367 D34ECCA7 833AF8D1 CAC6F0CD 8A41BDD3 AE68CBD7 FA0794FF
D984763C 33E7F772 13A0E35B C9FA823E F6262FA1 269407B1 68BE318D EB3E13E2
2C32B3DF FC9D0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 14F5FA3B 95F59783 28BF5857 1EF8C95B CC6F758C
98301D06 03551D0E 04160414 F5FA3B95 F5978328 BF58571E F8C95BCC 6F758C98

```

```

300D0609 2A864886 F70D0101 05050003 82010100 31F5A7B6 DA464923 BFB45830
24FB2D90 D044B831 EDF45EB8 7671C54B 9F309AC9 1BE168EB C4AE8142 CE939520
4633531E 8DFFA22A A46373F5 9AEFFBDC A33DC696 C8606AEB 0771B923 E3731049
CE802EE9 825A93AD EA304F4B DE495E02 25142F57 4B50CBF7 08480E62 BF9587E4
0303DB1E 5B524CA9 0AAFF669 7319074B CE560D90 409F0976 60DE6299 12F360EC
36D50FB1 8471FF91 5C613CDE 836C1CD0 DB876E34 60BA6FF8 8DBE4F76 180F0A36
DAEB023C C3672AB6 F3CA2792 6585700A E9B3F173 08D02311 8FBECDD5 0B4D459E
5352D388 7414DED9 964AB488 68F6B3D7 0EB39A46 2351DBCD 8FD97D24 DFA4C9E1
02A312DF 31E49F1F F10F9D39 D9A7B12A 62F7875A
quit
!
no license feature hseck9
license udi pid ESR-6300-NCP-K9 sn FOC23032UUN
license boot level network-advantage addon dna-advantage
archive
log config
logging enable
logging size 1000
notify syslog contenttype plaintext
path bootflash:saved-config
maximum 5
memory free low-watermark processor 49965
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
username cisco privilege 15 password 0 cisco
!
redundancy
mode none
!
vlan internal allocation policy ascending
!
lldp run
!
bridge irb
!
interface VirtualPortGroup0
ip address 192.168.0.1 255.255.255.0
ip nat inside
ipv6 address autoconfig
ipv6 enable
no mop enabled
no mop sysid
!
interface GigabitEthernet0/0/0
ip address 172.27.168.161 255.255.255.128
media-type rj45
negotiation auto
!
interface GigabitEthernet0/0/1
ip address 15.0.0.1 255.255.255.0
ip nat inside
shutdown
media-type sfp
negotiation auto
ipv6 enable
!
interface GigabitEthernet0/1/0
shutdown
!
interface GigabitEthernet0/1/1
shutdown

```

```

!
interface GigabitEthernet0/1/2
shutdown
!
interface GigabitEthernet0/1/3
shutdown
!
interface Vlan1
no ip address
!
interface vml1
no ip address
!
iox (Note: Some protocols appear in the configuration although they are not supported)
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0 172.27.168.129
ip ssh rsa keypair-name sshkeys
ip ssh version 2
!
snmp-server group mac v3 priv read mac write mac notify maca
snmp-server group fips v3 priv read fips write fips notify fips
snmp-server group cgnms v3 priv
snmp-server group cg-nms-administrator v3 priv
snmp-server view mac mib-2 included
snmp-server view mac system included
snmp-server view mac sysUpTime included
snmp-server view fips mib-2 included
snmp-server view fips system included
snmp-server view fips sysUpTime included
snmp-server community public RO R0
snmp-server community private RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps dsl
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps ds3
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps casa
snmp-server enable traps xgcp
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid

```

```

snmp-server enable traps dhcp
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune
rp-mapping-change interface-election
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps ip local pool
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps pki
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps ether-oam
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps entity-state
snmp-server enable traps vdsl2line
snmp-server enable traps entity-sensor
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps srp
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps otn
snmp-server enable traps pw vc
snmp-server enable traps ipsla
snmp-server enable traps sonet
snmp-server enable traps dlsr
snmp-server enable traps resource-policy
snmp-server enable traps lisp
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps dial
snmp-server enable traps sbc adj-status
snmp-server enable traps sbc blacklist
snmp-server enable traps sbc congestion-alarm
snmp-server enable traps c3g
snmp-server enable traps LTE
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete

```

```

snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps gdoi ks-role-change
snmp-server enable traps gdoi ks-gm-deleted
snmp-server enable traps gdoi ks-peer-reachable
snmp-server enable traps gdoi ks-peer-unreachable
snmp-server enable traps firewall serverstatus
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps alarms informational
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
line con 0
stopbits 1
speed 115200
line vty 0 4
transport input all
transport output all
line vty 5 15
transport input all
transport output all
!
app-hosting system-resources
end

```

Configuring Global Parameters

To configure global parameters for your router, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router> enable	Enters global configuration mode when using the console port. Use the following to connect to the router with a remote terminal:

	Command or Action	Purpose
	Router# configure terminal Router(config)#	telnet router-name or address Login: login-id Password: ***** Router> enable
Step 2	hostname <i>name</i> Example: Router(config)# hostname ESR6300	Specifies the name for the router.
Step 3	enable password <i>password</i> Example: Router(config)# enable password cr1ny5ho	Specifies a password to prevent unauthorized access to the router. Note In this form of the command, password is not encrypted. To encrypt the password use enable secret password as noted in the previously mentioned Device Hardening Guide.

Serial Port Support

Additional protocol capabilities have been added to the ESR6300 to bring it into feature compatibility with the IR1101. These include:

- SCADA Gateway functionality (IEC10x and DNP3)
- Raw Socket (TCP and UDP)
- Line Relay
- Reverse Telnet

All of the configuration and show commands will be the same as are available on the IR1101 platform.

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config.html

Rawsocket Keepalive Configuration CLI

Rawsocket keepalive for async interfaces is a feature that existed in classic IOS platforms. As part of 17.10.1a, the feature will be extended to IOS-XE based platforms. A new CLI with the following syntax will be added under rawsocket.

```
Router(config-line)#raw-socket tcp keepalive interval
```

CLI Changes

On IOS-XE platforms starting from 17.10.1a, there is a CLI correction and an additional CLI was added as part of raw-socket.

The correction is for the **raw-socket idle timeout** command. There is now an option to configure the timeout based on minutes and seconds, whereas the previous configuration used only minutes.


```
Router(config-line)# raw-socket tcp idle-timeout [0-1440] [<0-59> | cr]
```

The additional CLI is for clearing the raw-socket TCP clients. The command syntax is **clear raw-socket line** [1-145/tty/x/y/z] for example:

```
Router# clear raw-socket line 0/2/0
```



Note When initiating clear raw-socket line, raw-socket sessions will be cleared for raw-socket clients from the **show raw-socket tcp sessions** command. Connections will be re-established after a TCP hand-shake, which can be done by doing shut/no shut on TCP connection interface.

Configuring the Gigabit Ethernet Interface

The default configuration for the Gigabit Ethernet Interface (GI0/0/0 and GI0/0/1) on the ESR6300 are only Layer 3 (L3). The Gigabit Ethernet Interface on the ESR6300 is a combo port, which means it is a RJ45+SFP connector. These interfaces are combo ports, which means you can connect either through the RJ45 or SFP port by configuring the "media-type" to either auto-select, rj45 or sfp

To manually define the Gigabit Ethernet interface, follow these steps, beginning from global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	interface GigabitEthernet <i>slot/bay/port</i> Example: Router(config)# interface GigabitEthernet 0/0/0	Enters the configuration mode for an interface on the router.
Step 2	ip address <i>ip-address mask</i> Example: Router(config-if)# ip address 192.168.12.2 255.255.255.0	Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.
Step 3	ipv6 address <i>ipv6-address/prefix</i> Example: Router(config-if)# ipv6 address 2001.db8::ffff:1/128	Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address. IPv6 unicast-routing needs to be set-up as well, see further information in the IPv6 Addressing and Basic Connectivity Configuration Guide located here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xr-16-10/ipv6-xr-16-10-book/read-me-first.html
Step 4	ipv6 unicast-routing Example: Router (config)# ipv6 unicast-routing	Enables forwarding of IPv6 unicast data packets.

	Command or Action	Purpose
Step 5	no shutdown Example: Router(config-if)# no shutdown	Enables the interface and changes its state from administratively down to administratively up.
Step 6	exit Example: Router(config-if)# exit	Exits the configuration mode of interface and returns to the global configuration mode.

Configuring a Loopback Interface

Before you begin

The loopback interface acts as a placeholder for the static IP address and provides default routing information.

To configure a loopback interface, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	interface <i>type number</i> Example: Router(config)# interface Loopback 0	Enters configuration mode on the loopback interface.
Step 2	(Option 1) ip address <i>ip-address mask</i> Example: Router(config-if)# ip address 10.108.1.1 255.255.255.0	Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the ipv6 address <i>ipv6-address/prefix</i> command described below.
Step 3	(Option 2) ipv6 address <i>ipv6-address/prefix</i> Example: Router(config-if)# ipv6 address 2001:db8::ffff:1/128	Sets the IPv6 address and prefix on the loopback interface.
Step 4	exit Example: Router(config-if)# exit	Exits configuration mode for the loopback interface and returns to global configuration mode.

Example

Verifying Loopback Interface Configuration

Enter the **show interface loopback** command. You should see an output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.0.2.0/16
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Alternatively, use the **ping** command to verify the loopback interface, as shown in the following example:

```
Router# ping 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router. It may be disabled if needed for security purposes.

For more information on using CDP, see [Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S](#).

Configuring Command-Line Access

To configure parameters to control access to the router, follow these steps.



Note Transport input must be set as explained in the previous Telnet and SSH sections of the guide.

Procedure

	Command or Action	Purpose
Step 1	line [aux console tty vty] <i>line-number</i> Example: Router(config)# line console 0	Enters line configuration mode, and specifies the type of line. The example provided here specifies a console terminal for access.
Step 2	password <i>password</i> Example: Router(config-line)# password 5dr4Hepw3	Specifies a unique password for the console terminal line.
Step 3	login Example: Router(config-line)# login	Enables password checking at terminal session login.
Step 4	exec-timeout <i>minutes</i> [<i>seconds</i>] Example: Router(config-line)# exec-timeout 5 30 Router(config-line)#	Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value. The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of 0 0 specifies never to time out.
Step 5	exit Example: Router(config-line)# exit	Exits line configuration mode to re-enter global configuration mode.
Step 6	line [aux console tty vty] <i>line-number</i> Example: Router(config)# line vty 0 4 Router(config-line)#	Specifies a virtual terminal for remote console access.
Step 7	password <i>password</i> Example: Router(config-line)# password aldf2ad1	Specifies a unique password for the virtual terminal line.
Step 8	login Example: Router(config-line)# login	Enables password checking at the virtual terminal session login.
Step 9	end Example:	Exits line configuration mode, and returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-line)# end	

Configuring Static Routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	(Option 1) ip route <i>prefix mask {ip-address interface-type interface-number [ip-address]}</i> Example: Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2	Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the ipv6 route command described below.)
Step 2	(Option 2) ipv6 route <i>prefix/mask {ipv6-address interface-type interface-number [ipv6-address]}</i> Example: Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0	Specifies a static route for the IP packets. See additional information for IPv6 here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ipv6b-xe-16-10-book/read-me-first.html
Step 3	end Example: Router(config)# end	Exits global configuration mode and enters privileged EXEC mode.

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Gigabit Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not have to enter the command marked **default**. This command appears automatically in the configuration file generated when you use the **running-config** command.

```
!
ip classless (default)
ip route 2001:db8:2::/64 2001:db8:3::0
```

Verifying Configuration

To verify that you have configured static routing correctly, enter the **show ip route** command (or **show ipv6 route** command) and look for static routes marked with the letter S.

When you use an IPv4 address, you should see verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S*     0.0.0.0/0 is directly connected, FastEthernet0
```

When you use an IPv6 address, you should see verification output similar to the following:

```
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
Ndr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
ls - LISP site, ld - LISP dyn-EID, a - Application

C     2001:DB8:3::/64 [0/0]
      via GigabitEthernet0/0/2, directly connected
S     2001:DB8:2::/64 [1/0]
      via 2001:DB8:3::1
```

Configuring Dynamic Routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.

All of the Cisco IOS-XE configuration guides can be found here: <https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-gibraltar-16-10-1/model.html#ConfigurationGuides>

Configuring Routing Information Protocol

To configure the RIP on a router, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	router rip Example: Router(config)# router rip	Enters router configuration mode, and enables RIP on the router.
Step 2	version {1 2} Example: Router(config-router)# version 2	Specifies use of RIP version 1 or 2.
Step 3	network ip-address Example: Router(config-router)# network 192.168.1.1 Router(config-router)# network 10.10.7.1	Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.
Step 4	no auto-summary Example: Router(config-router)# no auto-summary	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.
Step 5	end Example: Router(config-router)# end	Exits router configuration mode, and enters privileged EXEC mode.

Example

Verifying Configuration

To verify that you have configured RIP correctly, enter the **show ip route** command and look for RIP routes marked with the letter R. You should see an output similar to the one shown in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R       3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0/0
```

Configuring Enhanced Interior Gateway Routing Protocol

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the Interior Gateway Routing Protocol (IGRP) developed by Cisco. The convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP, and IGRP is now obsolete.

The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations.

Details on configuring Enhanced Interior Gateway Routing Protocol (EIGRP), are found in the following guide: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xs-16-10/ire-xe-16-10-book/ire-enhanced-igrp.html

Configuring Open Shortest Path First (OSPF)

OSPF is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). OSPF was designed expressly for IP networks and it supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Cisco supports RFC 1253, *OSPF Version 2 Management Information Base*, August 1991. The OSPF MIB defines an IP routing protocol that provides management information related to OSPF and is supported by Cisco routers.

Details on configuring OSPF are found in the following guide: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xs-16-12/iro-xe-16-12-book.html

Configuring Integrated Intermediate System-to-Intermediate System (IS-IS) Routing Protocol

IS-IS is a link-state Interior Gateway Protocol (IGP). Link-state protocols are characterized by the propagation of the information required to build a complete network connectivity map on each participating device. That map is then used to calculate the shortest path to destinations.

The IS-IS protocol was developed in the late 1980s by Digital Equipment Corporation (DEC) and was standardized by the International Standards Organization (ISO) in ISO/IEC 10589. The current version of this standard is ISO/IEC 10589:2002.

ISO/IEC 10589 defines support for the ISO Connectionless Network Protocol (CLNP) as defined in ISO 8473. However, the protocol was designed to be extensible to other network protocols. RFC 1195 defined IS-IS support for IP, and additional IETF extensions have defined IS-IS support for IPv6. Integration of support for multiple network layer protocols has led to the term Integrated IS-IS. The Cisco IOS IS-IS implementation supports CLNP, IPv4, and IPv6. This module and its related modules use the term IS-IS to refer to the Integrated IS-IS that is implemented by Cisco IOS software.

For details on configuring IS-IS, see the following guide:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xs-16-12/irs-xe-16-12-book.html

Modular QoS (MQC)

This section provides an overview of Modular QoS CLI (MQC), which is how all QoS features are configured on the IoT Integrated Services Router. MQC is a standardized approach to enabling QoS on Cisco routing and switching platforms.

Follow the procedures that are in the [QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE 17 guide](#).



CHAPTER 7

Cisco IOS XE Installation Methods

This chapter contains the following sections:

- [Bundle Mode versus Install Mode, on page 77](#)
- [Installing the Software using install Commands, on page 77](#)
- [Restrictions for Installing the Software Using install Commands, on page 78](#)
- [Install Mode Support, on page 78](#)
- [Information About Installing the Software Using install Commands, on page 79](#)
- [Configuration Examples, on page 88](#)
- [Troubleshooting Software Installation Using install Commands, on page 94](#)

Bundle Mode versus Install Mode

Cisco IOS XE running on IoT routers has typically made use of the Bundle boot mode. Bundle boot mode is also known as Consolidated boot, and uses a single compressed image. The typical naming convention is <product>-universalk9.<release>.SPA.bin.

This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image. Booting via a .bin image means that the router would first have to uncompress the image before booting from it. This led to a longer period of time for the router to boot.

To upgrade the router to a new version of IOS XE, you would point the "boot system" to a new software image. This method is well known and details are available in your products configuration guide.

Starting with IOS XE release 17.9.1, a new boot mode called Install mode has been added to the IoT routers. Install mode uses packages loaded into bootflash, which are read by a packages.conf file. This method provides more control over the software installation process.

Install mode requires more room in bootflash: for the files. The packages are slightly larger than the .bin images, and they vary per product in size.

Installing the Software using install Commands

From Cisco IOS XE 17.9.1, Cisco IoT routers 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

- Install mode requires a reboot of the system.
- SMU installation was supported in both bundle boot and install mode. From Cisco IOS XE Release 17.9.x, SMU installation will be stopped if the router is booted up in bundle mode. If the router is booted up in install mode, SMU installation will keep working as it is in previous releases.

Install Mode Support

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

Cisco IOS XE running on IoT routers has typically made use of the Bundle boot mode. Bundle boot mode is also known as Consolidated boot, and uses a single compressed image. The typical naming convention is <product>-universalk9.<release>.SPA.bin.

This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image. Booting via a .bin image means that the router would first have to uncompress the image before booting from it. This led to a longer period of time for the router to boot.

To upgrade the router to a new version of IOS XE, you would point the "boot system" to a new software image. This method is well known and details are available in your products configuration guide.

Starting with IOS XE release 17.9.1, a new boot mode called Install mode has been added to the IoT routers. Install mode uses packages loaded into bootflash, which are read by a packages.conf file. This method provides more control over the software installation process.



Note SMU installation was supported in both bundle boot and install mode. From Cisco IOS XE Release 17.9.x, SMU installation will be stopped if the router is booted up in bundle mode. If the router is booted up in install mode, SMU installation will keep working as it is in previous releases.

Table 6: 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: Router(config)#boot system bootflash:<filename>	CLI: #install add file bootflash: [activate commit]
To upgrade in this mode, point the boot system to the new image.	To upgrade in this mode, use the install commands.

Bundle Mode	Install Mode
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.

For additional information, please see [Cisco IOS XE Installation Methods](#).

Information About Installing the Software Using install Commands

From the Cisco IOS XE 17.9.1 release, IoT routers will be shipped in install mode instead of bundle mode. So any new router from the factory will boot up in install mode.

Existing installations using previous releases of IOS XE have the option to continue to use their device in Bundle mode if they wish to. Or they can convert their device to Install mode.

Install mode is applicable to both autonomous mode and controller mode.

A new release can be installed in Install mode using vManage.

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

Table 7: Bundle Mode vs Install Mode

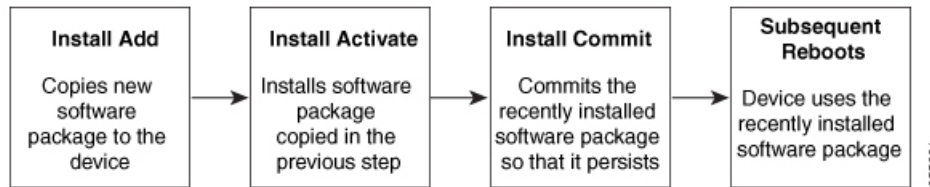
Bundle Mode	Install Mode
This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image.	This mode uses the local (bootflash) packages.conf file for the boot process.
This mode uses a single .bin file.	.bin file is replaced with expanded .pkg files in this mode.
CLI: <code>Router(config)#boot system bootflash:<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 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 location of the software package can be in several places, as shown in the output of the following command:

```

IR1831#install add file ?
bootflash: Package name
crashinfo: Package name
flash: Package name
ftp: Package name
http: Package name
https: Package name
pram: Package name
rcp: Package name
scp: Package name
sftp: Package name
tftp: Package name
webui: Package name
  
```

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 8: 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.
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.

Command	Syntax	Purpose
(install activate) auto abort-timer	install activate auto-abort timer <30-1200>	<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.
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.

Command	Syntax	Purpose
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.
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>

Command	Syntax	Purpose
install deactivate	install deactivate file <filename>	Removes a package from the platform repository. This command is supported only for SMUs. <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 9: 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.
show install summary	show install summary	Provides an overview of the image versions and their corresponding install states.
show install active	show install active	Provides information about the active packages.
show install inactive	show install inactive	Provides information about the inactive packages.
show install committed	show install committed	Provides information about the committed packages.
show install uncommitted	show install uncommitted	Provides information about uncommitted packages.
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.

You can see how your device is set up to boot by using the **show romvar** and **show bootvar** commands.

```
Router#show romvar
ROMMON variables:
PS1 = rommon ! >
CM = IR1100
DEVICE_MANAGED_MODE = autonomous
LICENSE_SUITE =
RET_2_RTS =
THRPUT = 250
BOOT = flash:packages.conf,12;
LICENSE_BOOT_LEVEL = network-advantage,all:IR1101;
BSI = 0
RET_2_RCALTS =
RANDOM_NUM = 212626522
Router#

Router#show bootvar
BOOT variable = flash:packages.conf,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby not ready to show bootvar

Router#
```

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.
- 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.

Procedure

	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:<router_image>.SSA.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.
- 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.

Procedure

	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:	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.

	Command or Action	Purpose
	<pre>Device#install add file bootflash:<router_image>.SSA.bin</pre>	
Step 3	<p>show install summary</p> <p>Example:</p> <pre>Device#show install summary</pre>	(Optional) Provides an overview of the image versions and their corresponding install state.
Step 4	<p>install activate auto-abort-timer <time></p> <p>Example:</p> <pre>Device# install activate auto-abort-timer 120</pre>	<p>Activates the previously added package and reloads the platform.</p> <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	<p>install abort</p> <p>Example:</p> <pre>Device#install abort</pre>	<p>(Optional) Terminates the software install activation and returns the platform to the last committed version.</p> <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	<p>install commit</p> <p>Example:</p> <pre>Device#install commit</pre>	Commits the new package installation and makes the changes persistent over reloads.
Step 7	<p>install rollback to committed</p> <p>Example:</p> <pre>Device#install rollback to committed</pre>	(Optional) Rolls back the platform to the last committed state.
Step 8	<p>install remove {file filesystem: filename inactive}</p> <p>Example:</p> <pre>Device#install remove inactive</pre>	<p>(Optional) Deletes software installation files.</p> <ul style="list-style-type: none"> file: Deletes a specific file inactive: Deletes all the unused and inactive installation files.
Step 9	<p>show install summary</p> <p>Example:</p> <pre>Device#show install summary</pre>	(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	<p>exit</p> <p>Example:</p> <pre>Device#exit</pre>	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

This section shows examples of using install commands.

One Step Installation

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

```
Router# install add file flash:ir1101-universalk9.SSA.bin activate commit
install_add_activate_commit: START Mon May 30 20:45:11 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:ir1101-universalk9.SSA.bin from R0 to R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Finished Add package(s) on R0
Checking status of Add on [R0]
```

```

Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.157857

install_activate: Activating IMG
Following packages shall be activated:
/flash/ir1101-mono-universalk9.SSA.pkg
/flash/ir1101-rpboot.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
Building configuration...
[OK] [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 all members
[1] Commit package(s) on R0
[1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Mon May 30 20:48:01 UTC 2022
%PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action requested
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system

System Bootstrap, Version 3.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

IR1101-K9 platform with 4169728 Kbytes of main memory

MCU Version - Bootloader: 4, App: 6
MCU is in application mode.

.....

Loading: bootflash:packages.conf
#

#####
#####
#####

%BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode
Press RETURN to get started!

Router# 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   17.09.01.0.157857
-----
```

```
-----
Auto abort timer: inactive
-----
```

Three Step Installation

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

Install Add

```
Router# install add file flash:ir1101-universalk9.17.09.01.SPA.bin
install_add: START Tue May 31 01:35:40 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:ir1101-universalk9.17.09.01.SPA.bin from R0 to R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
 [1] Finished Add package(s) on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.1

SUCCESS: install_add /flash1/ir1101-universalk9.17.09.01.SPA.bin Tue May 31 01:37:10 UTC
2022
Router#
```

```
Router# 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   I   17.09.01.0.1
-----
```

```
-----
Auto abort timer: inactive
-----
```

Install Activate

```
Router#install activate
install_activate: START Tue May 31 01:37:14 UTC 2022
install_activate: Activating IMG
Following packages shall be activated:
/flash/ir1101-mono-universalk9_iot.17.09.01.SPA.pkg
/flash/ir1101-rpboot.17.09.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
```

```
--- Starting Activate ---
```



```

Performing Activate on all members
  [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Tue May 31 01:41:03 UTC 2022
Router#
May 31 01:41:08.684: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
  reload action requested

watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system

System Bootstrap, Version 3.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

IR1101-K9 platform with 4169728 Kbytes of main memory

MCU Version - Bootloader: 4, App: 6
MCU is in application mode.

.....

Loading: bootflash:packages.conf
#

#####
#####
#####

Press RETURN to get started!

Router# 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   U    17.09.01.0.1
-----
Auto abort timer: inactive
-----

Install Commit

Router#install commit
install_commit: START Tue May 31 01:47:56 UTC 2022
--- Starting Commit ---
Performing Commit on all members
  [1] Commit packages(s) on R0
  [1] Finished Commit packages(s) on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Tue May 31 01:48:04 UTC 2022

Router# 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    17.09.01.0.1
-----
```

```
Auto abort timer: inactive
-----
```

Showing the Installed Packages

```
Router# show install package flash:ir1101-universalk9.17.09.01.SPA.bin
```

```
Package: ir1101-universalk9.17.09.01.SPA.bin
Size: 674114352
Timestamp:
Canonical path: /flash1/ir1101-universalk9.17.09.01.SPA.bin
```

```
Raw disk-file SHA1sum:
e54ba5a59824156af7515eaf4367ebe51b920316
Header size: 1148 bytes
Package type: 30000
Package flags: 0
Header version: 3
```

```
Internal package information:
Name: rp_super
BuildTime: 2022-04-27_00.47
ReleaseDate: 2022-04-27_07.05
BootArchitecture: arm64
RouteProcessor: IR1101
Platform: IR1101
User: mcpre
PackageName: universalk9
Build: 17.09.01
CardTypes:
```

```
Package is bootable from media and tftp.
Package contents:
```

```
Package: ir1101-mono-universalk9_iot.17.09.01.SPA.pkg
Size: 673776700
Timestamp:
```

```
Raw disk-file SHA1sum:

Header size: 1084 bytes
Package type: 30000
Package flags: 0
Header version: 3
```

```
Internal package information:
Name: mono
BuildTime: 2022-04-27_00.47
ReleaseDate: 2022-04-27_07.05
BootArchitecture: arm64
RouteProcessor: IR1101
Platform: IR1101
User: mcpre
PackageName: mono-universalk9_iot
Build: 17.09.01
```

```
CardTypes:
```

```
Package is bootable from media and tftp.
Package contents:
```

You can determine which package is active using the **show install active** command.

```
Router#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 17.09.01.0.1193
-----
Auto abort timer: inactive
-----
```

Showing Committed and Uncommitted Packages

These two show commands provide information on which packages are committed and uncommitted.

```
Router# 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   17.09.01.0.1
-----
Auto abort timer: inactive
-----

Router#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
```

Removing Inactive Packages

This command will remove unused installation files (.conf/.pkg/.bin) from installation media.



Note This command is used to clean up the boot directory of unused installation files. This will not remove the bootable image.

```
Router#install remove inactive
install_remove: START Tue May 31 01:49:10 UTC 2022
install_remove: Removing IMG
Cleaning up unnecessary package files
No path specified, will use booted path /bootflash/packages.conf
```

```

Cleaning /flash
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
  [R0]: /flash/packages.conf File is in use, will not delete.
  [R0]: /flash/irl101-mono-universalk9_iot.17.09.01.SPA.pkg File is in use, will not
delete.
  [R0]: /flash/irl101-universalk9.17.09.01.SPA.conf File is in use, will not delete.
  [R0]: /flash/irl101-rpboot.17.09.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:
[R0]: /flash/irl101-universalk9.17.09.01.SPA.bin
[R0]: /flash/irl101-mono-universalk9_iot.SSA.pkg
[R0]: /flash/irl101-universalk9.SSA.conf
[R0]: /flash/irl101-rpboot.SSA.pkg

Do you want to remove the above files? [y/n]y

Deleting file /flash/irl101-universalk9.17.09.01.SPA.bin ... done.
Deleting file /flash/irl101-mono-universalk9_iot.SSA.pkg ... done.
Deleting file /flash/irl101-universalk9.SSA.conf ... done.
Deleting file /flash/irl101-rpboot.SSA.pkg ... done.
Deleting /bootflash/.images/17.09.01.0.1.1651045630 ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Tue May 31 01:49:14 UTC 2022

Router#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

```

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 8

Installing the Software

This chapter contains the following sections:

- [Overview, on page 97](#)
- [Licensing, on page 97](#)
- [How to Install the Software for Cisco IOS XE , on page 101](#)
- [IOS XE Downgrade Warning, on page 104](#)
- [ROMMON Images, on page 104](#)
- [File Systems, on page 105](#)
- [Auto-generated File Directories and Files, on page 105](#)
- [Flash Storage, on page 106](#)
- [LED Indicators, on page 106](#)

Overview

Installing software on the router involves installing a consolidated package (bootable image). This consists of a bundle of subpackages (modular software units), with each subpackage controlling a different set of functions.

These are the two main methods to install the software:

- **Managing and Configuring a Router to Run Using Consolidated Packages** —This method allows for individual upgrade of subpackages and generally has reduced boot times compared to the method below. Use this method if you want to individually upgrade a module's software.
- **Managing and Configuring a Router to Run Using Individual Packages** —This simple method is similar to a typical Cisco router image installation and management that is supported across Cisco routers.

It is better to upgrade software in a planned period of maintenance when an interruption in service is acceptable. The router needs to be rebooted for a software upgrade to take effect.

There are different types of licenses for the device that are discussed in the next sections.

Licensing

This section contains the following:

Cisco Software Licensing

Cisco software licensing consists of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.

You can enable licensed features and store license files in the bootflash of your router. Licenses pertain to consolidated packages, technology packages, or individual features.

The ESR6300 does not support the Right to Use licenses, and supports only the Specific License Reservation (SLR)

Consolidated Packages

To obtain software images for the router, go to: <http://software.cisco.com/download/navigator.html>



Note All of the IOS-XE feature set may not apply to the ESR6300. Some features may not have been implemented yet, or are not appropriate for this platform.

An image-based license is used to help bring up all the subsystems that correspond to a license. This license is enforced only at boot time.

One of the following image-based licenses can be pre-installed on the ESR6300 router:

- Network-Essentials
- Network-Advantage
- HSecK9

To configure the license level, for example the network-advantage, use the following CLI:

```
Router#config terminal
Router (config)#license boot level network-advantage
Do you want to accept terms? Y
```



Note Network-Essentials and Network-Advantage licenses are mutually exclusive. To configure one, remove the other using **no license boot level <>** option in the privileged exec mode. The router will need to be reloaded for the configuration to take effect.

License Installation on the ESR6300

The ESR6300 license consists of two required parts:

- Feature License
- Throughput License

The feature license is either Network-Essentials or Network-Advantage. The throughput license can be either 50Mbps, 250Mbps or 2Gbps.



Note For the 2Gbps throughput level, an additional feature license, HSEck9 is required to comply with export restriction requirements.

Network-Essentials

The **Network-Essentials** technology package includes the baseline features. It also supports security features.

Features that are available in this license are:

- Traffic segmentation (VPN, VRF, VLAN)
- Crypto Tunnels
- IPSec
- IKEv2
- SSL-VPN
- DHCP
- QoS
- ACL
- EIGRP
- IGMP
- HTTP
- IP Multicast
- Radius
- TACACS
- OSPF
- RIP
- HSRP

The PIDs for the different levels of throughput for the Network-Essentials license are as follows.

- SL-6300-NE/DEF-K9 - Has a throughput level of 50Mbps.
- SL-6300-NE/PERF-K9 - Has a throughput level of 250Mbps
- SL-6300-NE/BOOS-K9 - Has a boosted throughput level of 2Gbps

The **Network-Essentials_npe** technology package (npe = No Payload Encryption) includes all the features in the Network-Essentials technology package without the payload encryption functionality. This is to fulfill export restriction requirements. The Network-Essentials_npe is available only in the Network-Essentials_npe image. The difference in features between the Network-Essentials package and the Network-Essentials_npe package is therefore the set of payload encryption features such as IPsec and Secure VPN.

Network-Advantage

The **Network-Advantage** technology package includes all crypto features.

The Network-Advantage license contains all of the features of the Network-Essentials license, plus the following.

- MPLS
- BFD
- RSVP
- RSRB
- SDLC
- IP SLA
- STUN
- TCP optimization
- App-aware QoS policies and troubleshooting

The PIDs for the different levels of throughput for the Network-Advantage license are as follows.

- SL-6300-NA/DEF-K9 - Has a throughput level of 50Mbps.
- SL-6300-NA/PERF-K9 - Has a throughput level of 250Mbps
- SL-6300-NA/BOOS-K9 - Has a boosted throughput level of 2Gbps

The **Network-Advantage_npe** package (npe = No Payload Encryption) includes all the features in the **Network-Advantage** technology package without the payload-encryption functionality. This is to fulfill export restriction requirements. The **Network-Advantage_npe** package is available only in the **Network-Advantage_npe** image. The difference in features between the **Network-Advantage** package and the **Network-Advantage_npe** package is therefore the set of payload-encryption-enabling features such as IPsec and Secure VPN.

Feature Support Caveats

The following features are not supported on the ESR6300:

- No support for MacSec or DLEP in the release.(MQC: modular quality of service command line).
- Layer2 COS to DSCP mapping does not work due to no ASIC chipset support for the feature.
- Copper FE SFPs are not supported on ESR6300.
- Copper GE SFPs are only supported in config terminal > service internal > service unsupported-transceiver mode.
- Cisco does not claim IP Mobility for Ethernet support on the ESR6300.
- Auto-negotiation for 10Mbps, 100Mbps, 1000Mbps in full-duplex mode is supported. For half duplex, support is only on 10Mbps and 100Mbps.

- Booting the golden configuration from a USB is NOT supported in 17.1.1, however it is available in 17.2.1.
- Refer to the Cisco approved vendor list [AVL] for Cisco USBs. Kingston USB 3.0 works as well. Ensure the USB has a single partition and ext2, fat16 or fat32 format only.
- There is no WebUI support for Day 0 or Day 1
- For Security: No support for TLS, TrustSec, MacSec , CWS [Cloud Web Security], IDS/IPS.

How to Install the Software for Cisco IOS XE

To install the software, use one of the following methods to use the software from a consolidated package or an individual package. Also see *Overview* section.

- *Managing and Configuring a Router to Run Using a Consolidated Package* section
- *Managing and Configuring a Router to Run Using Individual Packages* section
- *Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example* section

The device can be booted from a number of different resources, which can be found by using the following command:

```
Router(config)#boot config ?
bootflash:  URL of the config file
flash:      URL of the config file
nvram:      URL of the config file
usbflash0:  URL of the config file
webui:      URL of the config file
```

The following is an example of booting from a config file from flash:

```
Router(config)#boot config flash0:startup-config
```

Starting with IOS-XE Release 17.2.1, support has been added for booting from the USB.

The syntax for the boot command is:

```
boot config usbflash0:<file name>
```

For example:

```
Router(config)#boot config usbflash0:startup-config
Router(config)#
Router#write memory
Building configuration...
[OK]
*Feb 10 10:20:11.990: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
```

The environment variable CONFIG_FILE in the following example confirms that the startup-config is set to boot from usbflash0.

```
Router#show boot
BOOT variable =
CONFIG_FILE variable = usbflash0:startup-config
BOOTLDR variable does not exist
```

```
Configuration register is 0x1820
Standby not ready to show bootvar
```

Booting from the USB Feature Summary

- Once the CONFIG_FILE is set to a non-default value, the **nvr_{am}:startup-config** command is aliased to this new location.
- Any change made to the config file in usbflash will be reflected in nvr_{am}:startup-config as well.
- The EXEC command **erase nvr_{am}:startup-config** erases the contents of NVRAM, and deletes the file referenced by CONFIG_FILE variable.
- If the USB is unplugged after setting the **boot config usbflash0: <filename>** variable, then the day 0 default configuration will take effect.
- When the configuration is saved using the **copy system:running-config nvr_{am}:startup-config** command, the device saves a complete version of the configuration file to the location specified by the CONFIG_FILE environment variable, and a distilled version to NVRAM. A distilled version is one that does not contain access list information.

Booting from ROMMON

The following configuration steps need to be taken in order to boot from the USB.

From the ROMMON prompt, execute **set CONFIG_FILE=usbflash0: <filename>**

For example:

```
rommon 2 > set CONFIG_FILE=usbflash0:my_startupcfg
rommon 3 > sync
rommon 4 > set
PS1=rommon ! >
MCU_UPGRADE=SKIP
THRPUT=
LICENSE_BOOT_LEVEL=
RET_2_RTS=
MCP_STARTUP_TRACEFLAGS=00000000:00000000
BSI=0
RANDOM_NUM=1275114933
BOOT=flash:Jun5_1.SSA,12
RET_2_RCALTS=951454376
CONFIG_FILE=usbflash0:my_startupcfg
```

Continue booting the IOS image as usual from the ROMMON prompt.

Upgrading the Cisco IOS XE Release

When the device boots up with Cisco IOS XE image for the first time, the device checks the installed version of the ROMMON, and upgrades if the system is running an older version. During the upgrade, do not power cycle the device. The system automatically power cycles the device after the new ROMMON is installed.

Once ROMMON is upgraded, the device will check if the MCU is upgraded. Once that is complete, the device will boot up with the Cisco IOS XE image as normal.

After the installation, the system will boot up with the Cisco IOS XE image as normal.



Note When the device boots up for first time and if the device requires an upgrade, the entire boot process may take several minutes. This process will be longer than a normal boot due to the ROMMON and/or MCU upgrade.

The following example illustrates the boot process of a consolidated package:

```

Router# configure terminal
Router(config)#boot system bootflash:ESR 6300-universalk9.17.1.1.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router#
*Nov 7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#show run | inc license
license udi pid ESR 6300-K9 sn FCW2150TH0F
license boot level network-advantage
Router#
Router#reload ?
  /noverify Don't verify file signature before reload.
  /verify   Verify file signature before reload.
  at       Reload at a specific time/date
  cancel   Cancel pending reload
  in       Reload after a time interval
  pause    Pause during reload
  reason   Reload reason
  <cr>    <cr>

Router#reload /verify

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
*Nov 7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Verifying file integrity of bootflash:/ESR 6300-universalk9.16.10.01.SPA.bin.....
.....

Embedded Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Computed Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Starting image verification
Hash Computation: 100%Done!
Computed Hash   SHA2: 03febcc07fbeaded664f2f5ef87f6c3
                5b343e6f7aecdd70e50e5203909aec8f
                3d276529d2a6af6859d4c77237f812d5
                0da93678edc942c8874edca2d5224101

Embedded Hash   SHA2: 03febcc07fbeaded664f2f5ef87f6c3
                5b343e6f7aecdd70e50e5203909aec8f
                3d276529d2a6af6859d4c77237f812d5
                0da93678edc942c8874edca2d5224101

Digital signature successfully verified in file bootflash:/ESR
6300-universalk9.16.10.01.SPA.bin
Signature Verified

Proceed with reload? [confirm]

*Jul 9 06:43:37.910: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command. Jul 9 14:43:59.134: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
process exit with reload chassis code

```

```
watchdog watchdog0: watchdog did not stop!  
reboot: Restarting system
```

Press RETURN to get started!

IOS XE Downgrade Warning

This feature will present a warning when issuing a **boot system flash** command followed by a file name of an image which has a version number lower than the one of the running image. The downgrade operation will still be possible by ignoring the warning message presented to the user. Booting an image with the same or higher version of the running image is allowed without warning. The feature is only intended for images already loaded on the bootflash of the router, this means only for the **boot system flash** *<file_name>* CLI (excluding other sources/devices like ftp, mop, rpc, tftp, rom).

The following are examples of how the system compares versions:

When comparing two version numbers as follows:

- 17.7.1
- 17.7.1c

The version with the letter (17.7.1c) will be considered the most updated one.

When comparing two version numbers as follows:

- 17.7.3a
- 17.7.3f

The comparison will be made taking into consideration the alphabetical order. In the case above 17.7.3f will be considered the most updated one.

ROMMON Images

A ROMMON image is a software package used by ROM Monitor (ROMMON) software on a router. The software package is separate from the consolidated package normally used to boot the router.

An independent ROMMON image (software package) may occasionally be released and the router can be upgraded with the new ROMMON software. For detailed instructions, see the documentation that accompanies the ROMMON image.



Note A new version of the ROMMON image is not necessarily released at the same time as a consolidated package for a router.

File Systems

The following table provides a list of file systems that can be seen on the Cisco ESR6300 router.

Table 10: Router File Systems

File System	Description
bootflash:	Boot flash memory file system.
flash:	Alias to the boot flash memory file system above.
cns:	Cisco Networking Services file directory.
nvrnram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
obfl:	File system for Onboard Failure Logging (OBFL) files.
system:	System memory file system, which includes the running configuration.
tar:	Archive file system.
tmpsys:	Temporary system files file system.
usbflash0:	The Universal Serial Bus (USB) flash drive file systems. Note The USB flash drive file system is visible only if a USB drive is installed in the usb port.

Use the ? help option if you find a file system that is not listed in the table above.

Auto-generated File Directories and Files

This section discusses the auto-generated files and directories that can be created, and how the files in these directories can be managed.

Table 11: auto-generated Files

File or Directory	Description
crashinfo files	Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, 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
tracelogs directory	<p>The storage area for trace files.</p> <p>Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure.</p> <p>Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.</p>

Important Notes About auto-generated Directories

Important information about auto-generated directories include:

- auto-generated files on the bootflash: directory should not be deleted, renamed, moved, or altered in any way unless directed by Cisco customer support.



Note Altering auto-generating files on the bootflash: may have unpredictable consequences for system performance.

- Crashinfo files and files in the core and tracelogs directory can be deleted.

Flash Storage

Subpackages are installed to local media storage, such as flash. For flash storage, use the **dir bootflash:** command to list the file names.



Note Flash storage is required for successful operation of a router.

LED Indicators

For LED information on the router, see the LED section of the [ESR6300 Hardware Technical Manual](#).



CHAPTER 9

Smart Licensing Using Policy

This chapter contains the following sections:

- [SLP Overview, on page 107](#)
- [Customer Topologies, on page 112](#)
- [License Installation Procedure - Full Offline Access Topology, on page 113](#)
- [License Installation Procedure - CSLU has No Access to CSSM, on page 118](#)
- [Change to Smart Licensing Packaging, on page 132](#)
- [Uncapped License Implementation , on page 135](#)

SLP Overview

Smart Licensing Using Policy (SLP), previously known as Smart Licensing Enhanced (SLE), is the default mode for IoT routers. SLE replaced Smart Software Licensing.

This guide supports all IoT routers, and replaces individual chapters in each of the software configuration guides.

The following sections show the features and software differences between the IoT routers.

IR1800

The IR1800 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2
- An Authorization Code is required only for export control requirement
- Throughput greater than 250MB requires an HSEC license
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.

IR1101

The IR1100 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2

- An Authorization Code is required only for export control requirement
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.
- Throughput is defaulted and capped at 250MB.

IR8100

The IR8100 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2
- An Authorization Code is required only for export control requirement
- Throughput greater than 250 Mbps requires an HSEC license
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.

IR8300

The IR8300 series only supports SLP. Some of the feature differences are:

- Support started with IOS-XE release 17.3.2
- An Authorization Code is required only for export control requirement
- Throughput greater than 250 Mbps requires an HSEC license
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.

ESR6300

The ESR6300 embedded router operates slightly different than the other IoT routers. Some of the feature differences are:

- Support started with IOS-XE release 17.4.1
- An Authorization Code is required only for export control requirement
- Throughput greater than 250 Mbps requires an HSEC license
- No more EVAL licenses. Authorized status has changed to In Use or Not In Use with an Enforcement Type class.
- Cisco Smart Licensing Utility (CSLU) is a new tool interfacing between the devices and Cisco Smart Software Manager (CSSM) in specific customer topologies.

License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced

The vast majority of licenses belong to this enforcement type. Unenforced licenses do not require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

- Enforced

Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Industrial Ethernet Switches.

- Export-Controlled

Licenses that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

An example of an export-controlled license is the High Security (HSEC) license, which is available on certain Cisco Routers.

High Security (HSEC) License

HSEC (High Security) license is a feature license that can be configured in addition to the network license (NE/NA). An HSEC license provides export controls for strong levels of encryption. HSEC is available to customers in all currently non-embargoed countries as listed by the U.S. Department of Commerce. Without an HSEC license, SEC performance is limited to a total of 250 Mbps of IPsec throughput in each direction. An HSEC license removes this limitation.

Command Line Interface

The configuration mode CLI to enable HSEC on the IR1101 is the following:

```
IR1101(config)# license feature hsec9
```

To benefit from the HSEC license, a new bandwidth will be available. The new bandwidth is called **uncapped**, and it is available with the following CLI from configuration mode:

```
IR1101(config)# platform hardware throughput level ?  
250M throughput in bps  
uncapped throughput in bps  
IR1101# platform hardware throughput level uncapped
```

After performing the above commands, write mem and reload the router. The configuration will take effect when the router comes back up.

License Types

With this new feature, the IR1101 will support the following bandwidth/license types:

- Network-essentials 250 Mbps
- Network-advantage 250 Mbps
- Network-essentials uncapped
- Network-advantage uncapped
- HSEC

Ordering

The following is an example from the IR1101-K9. The license will be available on the IR1101-A-K9 as well. In the following example, select the SL-1101-NE/UNCP-K9 (Network Essentials Uncapped License):

IR1101-K9 > Software Licenses

[Expand All](#) | [Collapse All](#)

⊖ Software Licenses

SKU	Qty	Estimated Lead Time ⓘ
<input type="radio"/> SL-IR1101-NE SA Network Essentials License for Cisco IR1101 Industrial ISR More	1	3 days
<input type="radio"/> SL-IR1101-NE-NPE SA Network Essentials NPE for Cisco IR1101 Industrial ISR More	1	3 days
<input type="radio"/> SL-1101-NE/UNCP-K9 PLH SA Network Essentials Uncapped License for Cisco IR1101 More	1	21 days

The L-1101-HSEC-K9 license will get auto included when you select the uncapped license, as shown in the following:

OPTION SELECTION IR1101-K9 Global Price List in US Dollars (USD)

Configuration Summary [View Full Summary](#)

Category ⓘ	Qty	Extended List Price (USD)
SOFTWARE LICENSE		
Software Licenses		
HSEC License		
MODULES		
Base Module		
Expansion Module		
Expansion Module Placement		
ACCESSORIES		
Antennas		
Subtotal		1,182.89
Estimated Lead Time		206 days

Reset Configuration Cancel Done

Warnings (8):

- A Selection from Shipment Package is required. Please adjust your selection. (CE202343)
- A selection of IR1100-P-BLANK is required when no Base Module is selected. Please adjust the selections. (CE200440)

Option Search ⓘ Multiple Options Search ⓘ

IR1101-K9 > HSEC License [Key](#) ⌵

[Expand All](#) | [Collapse All](#)

⊖ HSEC License

SKU	Qty	Estimated Lead Time ⓘ	Unit List Price (USD)
<input type="radio"/> L-1101-HSEC-K9 PLH SA U.S. Export Restriction Compliance license for IR1101 More	Qty	21 days	--

Cisco Software Central

This guide provides information on how to order, activate, and manage your Cisco Smart Licenses.

https://software.cisco.com/software/cs/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

SLP Architecture

This section explains the various components that can be part of your SLP implementation.

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. The RUM reports and usage data are also stored securely in the product instance.

A Resource Utilization Measurement report (RUM report) is a license usage report, which fulfills reporting requirements as specified by the policy. RUM reports are generated by the product instance and consumed by CSSM. The product instance records license usage information and all license usage changes in an open RUM report. At system-determined intervals, open RUM reports are closed and new RUM reports are opened to continue recording license usage. A closed RUM report is ready to be sent to CSSM.

A RUM acknowledgement (RUM ACK or ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates that the corresponding RUM report is no longer required and can be deleted.

CSSM displays license usage information as per the last received RUM report.

Cisco Smart Software Manager (CSSM)

CSSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access CSSM at <https://software.cisco.com>. Under the License tab, click the Smart Software Licensing link.

In CSSM you can:

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

Prior to using CSSM, please view a short video about how to use the portal found here:

<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>

Click on the **View Video** button.

Cisco Smart Licensing Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing work-flows. It helps you administer all your licenses and their associated product instances from your premises instead of having to connect to CSSM.

This utility performs the following key functions:

- Provides the options relating to how work-flows are triggered. The work-flows can be triggered by CSLU or by the product instance,
- Collects usage reports from the product instance and upload these usage reports to the corresponding smart account or virtual account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and provided back to the product instance.
- Sends authorization code requests to CSSM and receives authorization codes¹ from CSSM.

CSLU can be part of your SLP topology in the following ways:

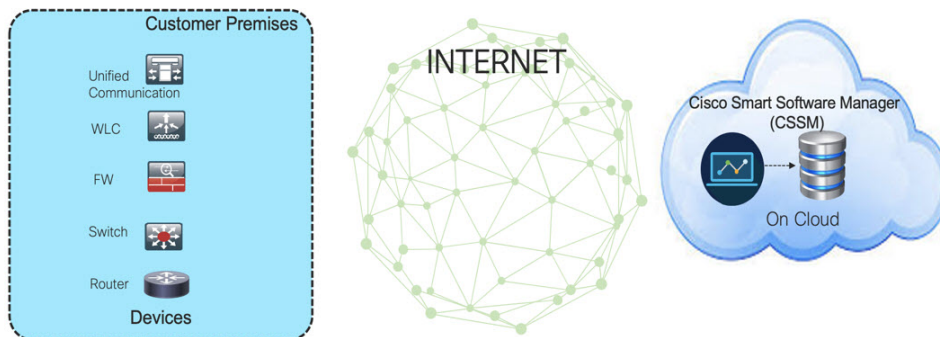
- Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.
- Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.
- Embed it in a controller such as Cisco DNA Center.

Customer Topologies

IoT Routing platforms use two different topologies.

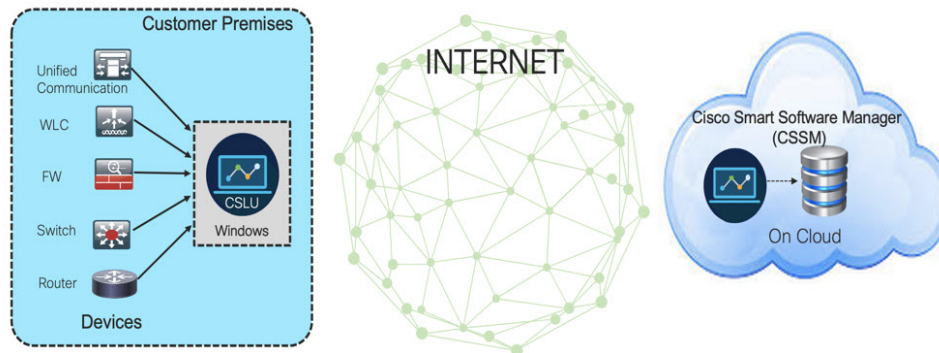
- Full Offline Access
- CSLU has No Access to CSSM

The following figure illustrates the Full Offline Access:



In this topology, devices do not have connectivity to CSSM (software.cisco.com). The user must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

The following figure illustrates the CSLU having No Access to CSSM:



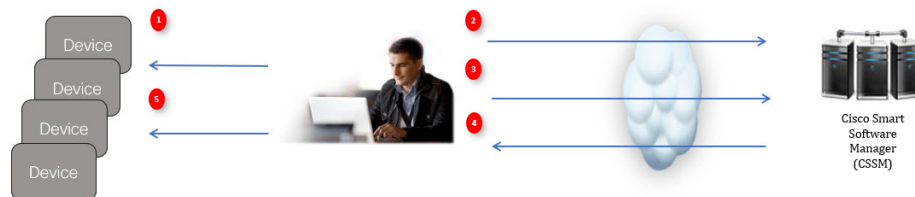
In this topology the devices are connected to the CSLU controller, but there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com).

Cisco devices will send usage information to a locally installed CSLU. The user must copy and paste information between the CSLU and CSSM to manually check-in and check-out licenses.

License Installation Procedure - Full Offline Access Topology

This procedure requires a manual exchange of required information between the router and CSSM.

Refer to the following graphic for the flow of information:



1. Generate a License Usage Data file or AuthCode Request
2. Export to CSSM
3. Upload License Usage Data or AuthCode Request
4. Export ACK/AuthRequest file to Router
5. Upload ACK file or AuthRequestAuthCode

This section contains the following topics:

Procedure to Register Product Instance in CSSM

Step 1 Generate a license usage file from the Router.

In exec mode, perform the following:

Example:

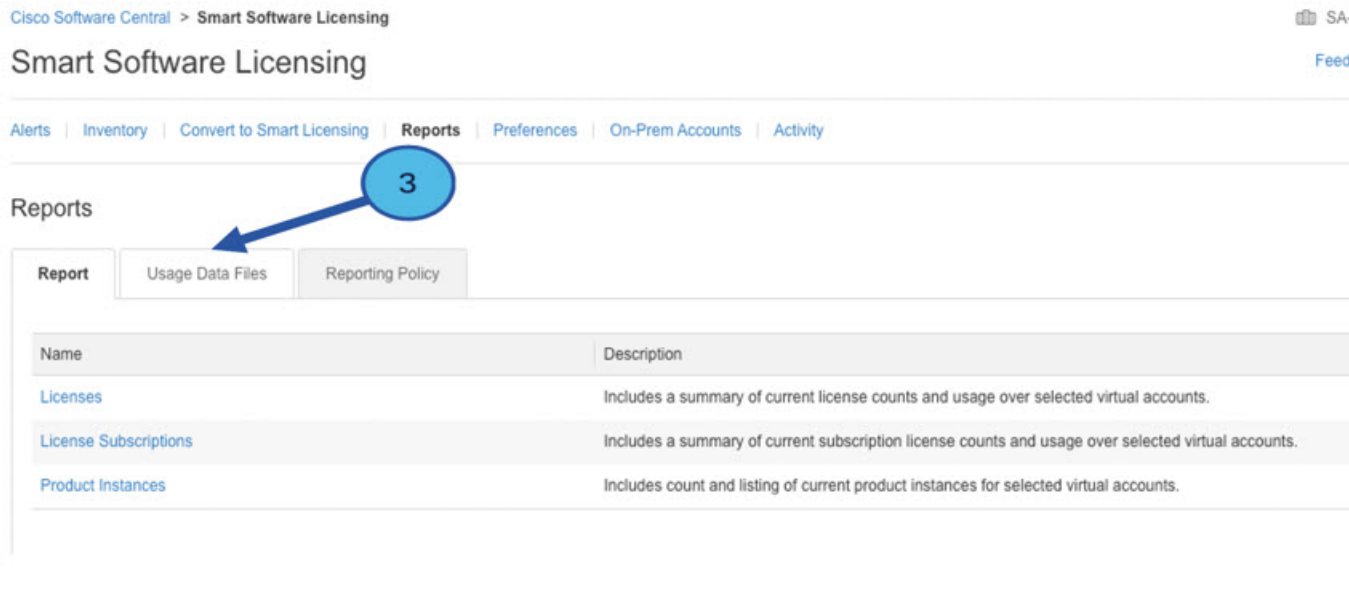
Procedure to Register Product Instance in CSSM

```
Router# license smart save usage all file flash:slp
```

Step 2 Export the license usage file (slp) to your host laptop/PC.

Step 3 Importing the license usage file to CSSM on Cloud. Click on the **Usage Data Files** tab.

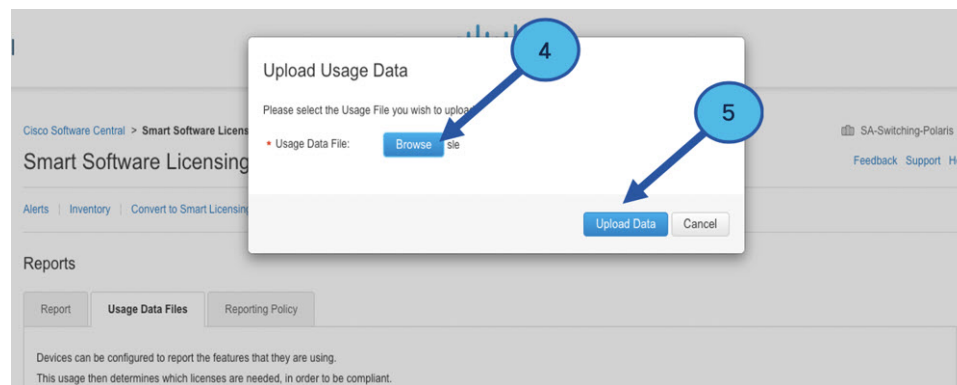
Figure 5: Usage Data File



Step 4 The **Upload Usage Data** window appears. Click **Browse**, and navigate to where the file is.

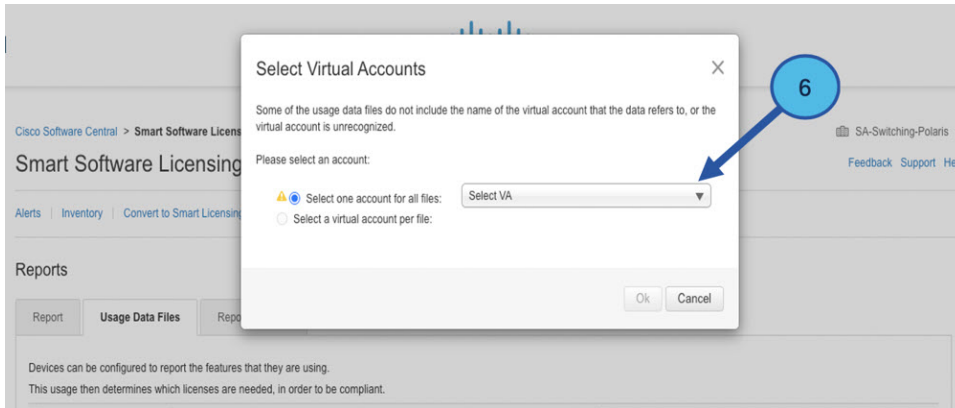
Step 5 Click on **Upload Data**.

Figure 6: Browse and Upload



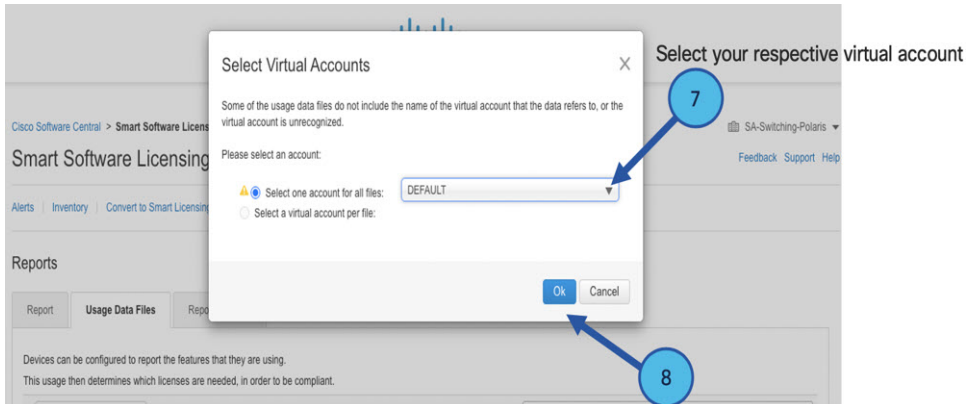
Step 6 Select the Virtual Account.

Figure 7: Select Account



Step 7 From the pull-down, select your respective virtual account.

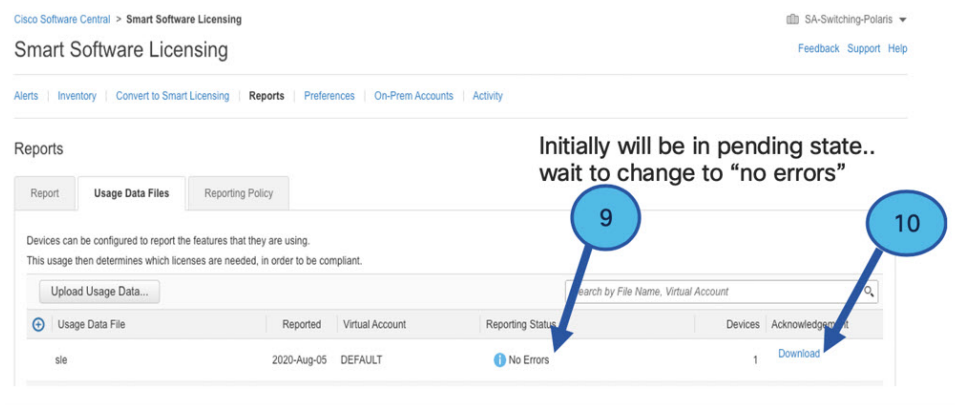
Figure 8: Select Your Account



Step 8 Click **Ok**.

Step 9 Observe the Smart Software Licensing window. Initially, the Reporting Status state will be **Pending**. Wait until the window reflects **No Errors** before continuing.

Figure 9: Reporting Status



Step 10 Click **Download** to download the ACK file.

Step 11 Check under the **Product Instances** tab to verify your device is listed.

Figure 10: Product Instances

Virtual Account: VA-Blackheart Minor Hide Alerts

General Licenses **Product Instances** Event Log

Authorize License-Enforced Features... Search by Name, Product Type

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:ESR-6300-CON-K9; UDI_SN:FOC23032UWF;	5900	2020-Sep-24 20:23:59 (Reserved Licenses)		Actions
UDI_PID:ESR-6300-CON-K9; UDI_SN:SJC19700415;	5900	2020-Sep-24 20:41:41 (Reserved Licenses)		Actions
UDI_PID:IR1101-K9; UDI_SN:FCW24150J0F;	IR1100	2020-Jul-30 02:22:04		Actions
UDI_PID:IR1833-K9; UDI_SN:FCW2420P0VB;	M2M800	2020-Jul-07 20:15:11 (Reserved Licenses)		Actions
UDI_PID:IR1835-K9; UDI_SN:PHH2416P00Z;	M2M800	2020-Sep-30 01:01:21		Actions
UDI_PID:IR8140H-P-K9; UDI_SN:FDO2420J7B6;	CGR1000	2020-Sep-08 18:37:24		Actions

Showing All 6 Records

Note This example shows an IR1835 highlighted. Your product name might be different.

Step 12 Import the ACK file from CSSM to your device using the command line interface.

Importing the ACK file from CSSM to your Device

Step 1 Copy the ACK file from CSSM to your host laptop or usbflash device. In exec mode on the device:

Example:

```
Router#license smart import <flash: | usbflash0:> ACK_slp
Import Data Successful
Router#
*Sep 1 21:12:58.576: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Sep 1 21:12:58.616: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully installed
```

Step 2 Verify Product Instance has imported the data.

a) The following example is from an IR1800:

Example:

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (IR1800_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
```

b) The following example is from an ESR6300:

Example:

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
```

Step 3

Verify the license is in use.

- a) The following example is from an IR1800:

Example:

```
Router# show license summary
License Usage:
  License                                     Entitlement tag          Count  Status
  -----
network-advantage_250M (IR1800_P_250M_A)    1      IN USE

Router#
Router#show license all | beg Usage Reporting:
Usage Reporting:
  Last ACK received: Sep 01 21:12:58 2020 UTC
  Next ACK deadline: <none>
  Reporting Interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: Sep 01 00:28:48 2020 UTC
```

- b) The following example is from an ESR6300:

Example:

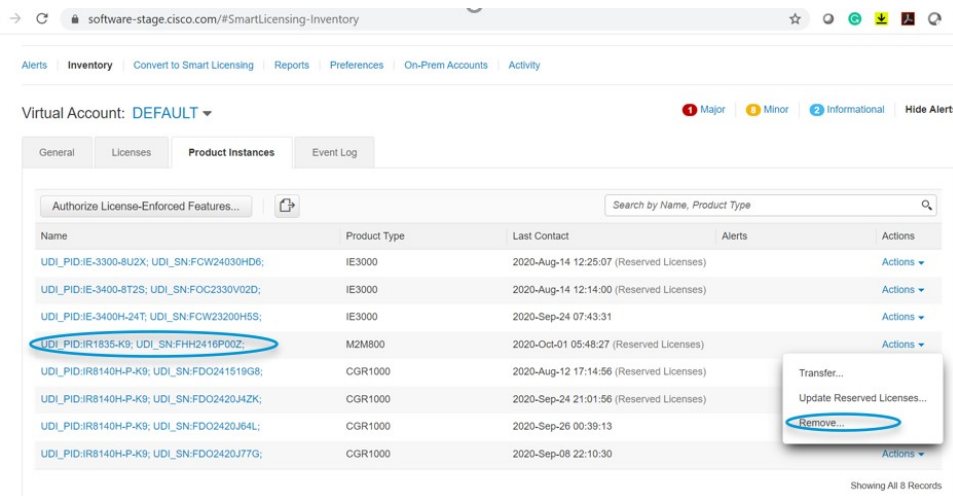
```
Router# show license summary
License Usage:
  License                                     Entitlement tag          Count  Status
  -----
network-advantage_250M (ESR6300_P_250M_A)    1      IN USE

Router#
Router#show license all | beg Usage Reporting:
Usage Reporting:
  Last ACK received: Sep 01 21:12:58 2020 UTC
  Next ACK deadline: <none>
  Reporting Interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: Sep 01 00:28:48 2020 UTC
```

Removing the Device from CSSM

Step 1 Navigate back to the product instances tab. Locate your device.

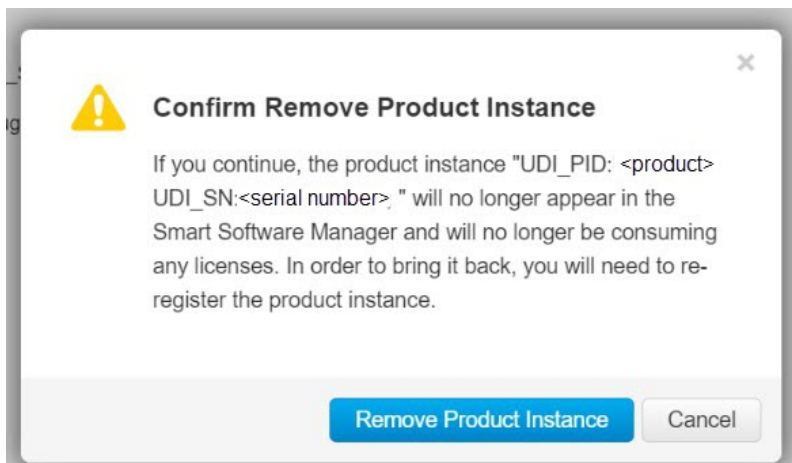
Figure 11: Product Instances



Step 2 Click on **Actions** beside your device, and from those options click **Remove**.

The Confirm Remove Product Instance window appears.

Figure 12: Confirm Remove Product Instance

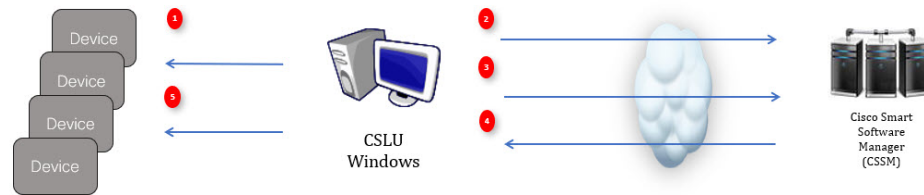


Step 3 Click **Remove Product Instance**.

License Installation Procedure - CSLU has No Access to CSSM

This procedure performs an online exchange of required information between the Router and CSLU.

Refer to the following graphic for the flow of information:



-
- Step 1** In CSLU, identify the devices that require an AuthCode, and initiate the request. An AuthCode file is created.
- Step 2** Export the AuthCode file to CSSM.
- Step 3** Upload the AuthCode to CSSM SA/VA account.
- Step 4** Export the AuthRequestAuthcode file to CSLU.
- Step 5** Upload ACK file or AuthRequestAuthCode.
-

What to do next

This section contains the following:

Procedure when devices are connected to the CSLU

First, perform these steps on the router using the CLI to get a license UDI:

Example from an IR1800:

```
Router#show license summary
License Reservation is ENABLED
License Usage:
License Entitlement tag Count Status
-----
network-essentials_250M (IR1800_P_250M_E) 1 IN USE
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!
Router(config)#end
```

```
Router#sh license udi
UDI: PID:IR1835-K9,SN:FHH2416P00Z
```

Example from an ESR6300:

```
Router#show license summary
License Reservation is ENABLED License Usage:
License Entitlement tag Count Status
-----
network-advantage_250M (ESR6300_P_250M_A) 1 IN USE
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!
```

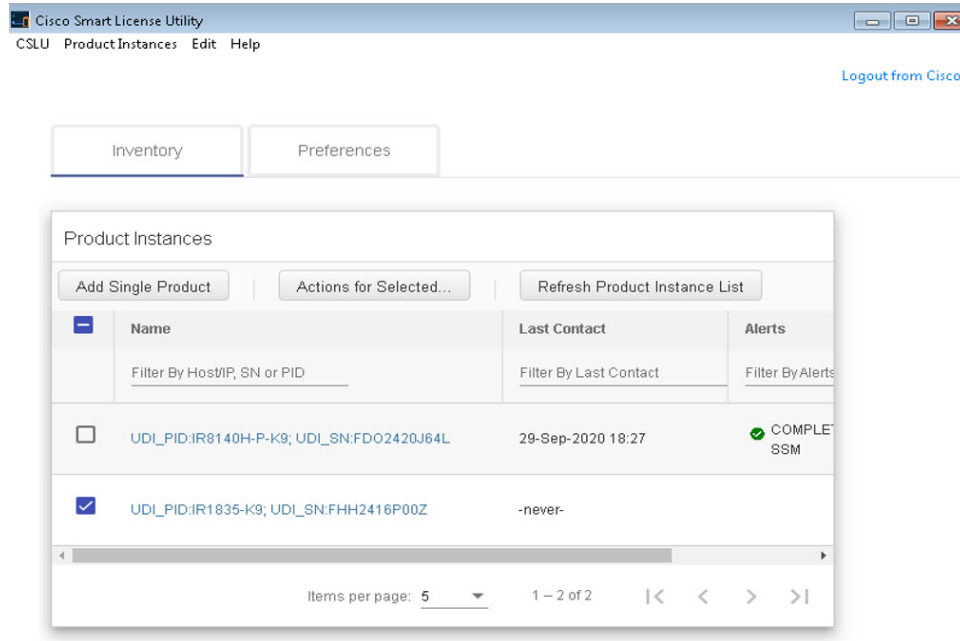
Procedure when devices are connected to the CSLU

```
Router(config)#end
Router#sh license udi
UDI: PID:ESR-6300-CON-K9,SN:FOC23032UVB
```

Step 1 Open the Cisco Smart License Utility (CSLU).

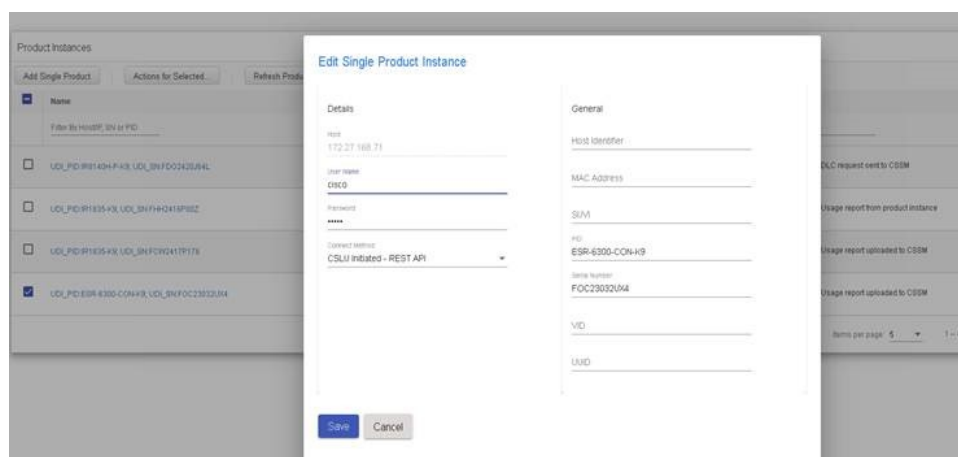
Step 2 Navigate to the **Product Instances** tab, then click on the UDI.

Figure 13: Select UDI - IR1835 Example



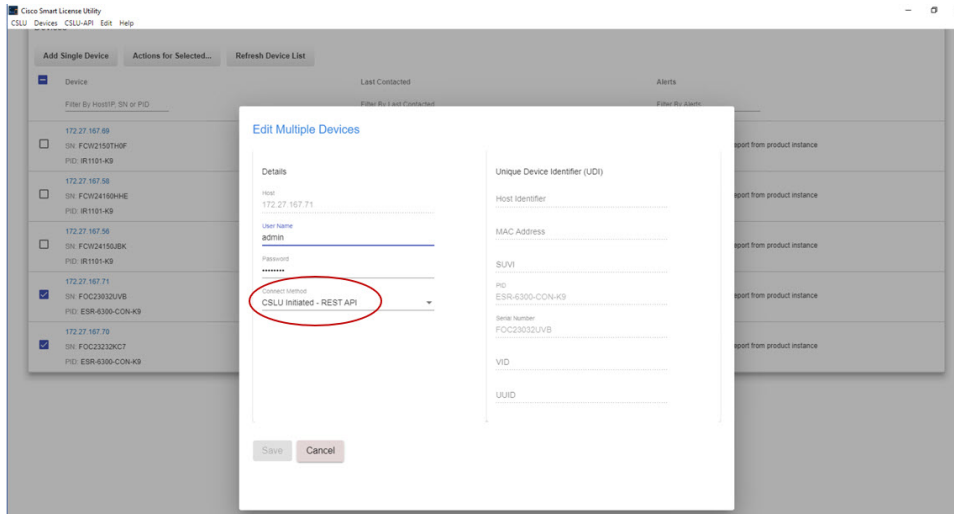
Step 3 The **Edit Single Product Instance** window appears.

Figure 14: Edit Single Product Instance



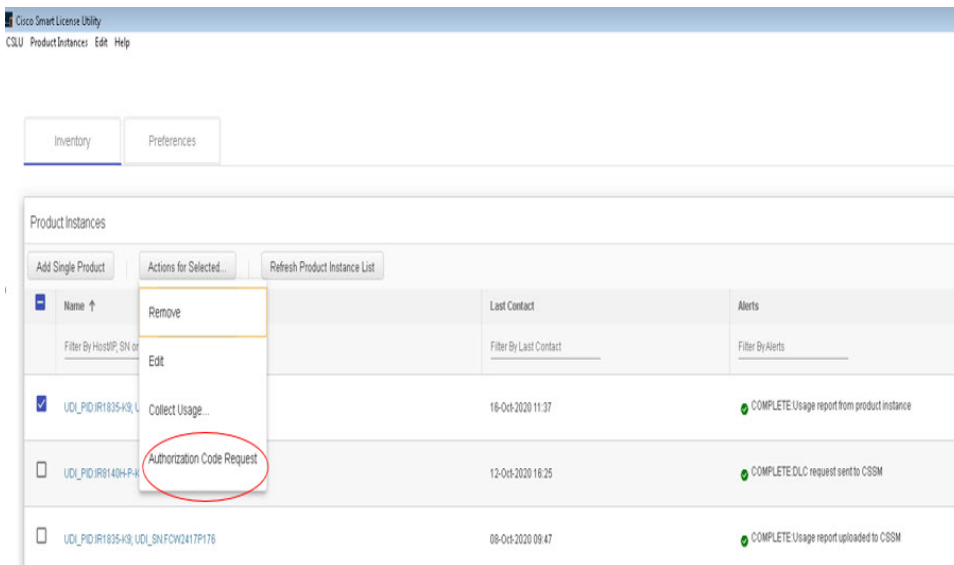
Step 4 The **Edit Multiple Devices** window appears. Supply your account password and click **Save**.

Figure 15: Edit Multiple Devices



Step 5 In the **Product Instances** window, click on the **Actions for Selected Devices** Tab.

Figure 16: Actions for Selected Devices



Step 6 Select **Authorization Code Request**.

Step 7 The **Authorization Request Information** window appears. Read the contents and then click **Accept**.

Figure 17: Authorization Request Information

Authorization Request Information

This operation will download an authorization request file for the devices that have been selected. Once this file is downloaded please:

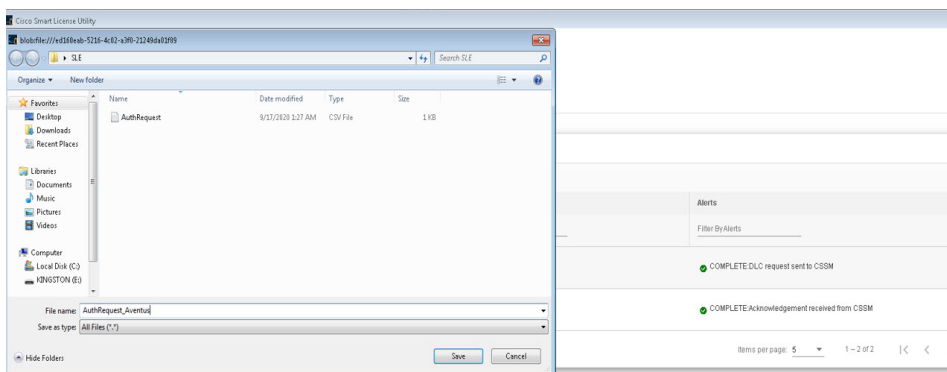
1. Upload the file to CSSM.
2. After uploading to CSSM you will be able to download the file containing the authorization codes for devices you selected.
3. Please upload this file using the "Upload From CSSM" menu option to apply the authorization codes for the devices.

Accept

Cancel

Step 8 The CSLU downloads a Authorization Request file to your laptop. Click **Save**.

Figure 18: Authorization Request File



Exporting the AuthRequest File to CSSM

The next step is to take the Authorization Request file you just saved, and export it into Cisco Smart Software Manager (CSSM).

Launch CSSM.

Click on the **Inventory** Tab, select your Virtual Account.

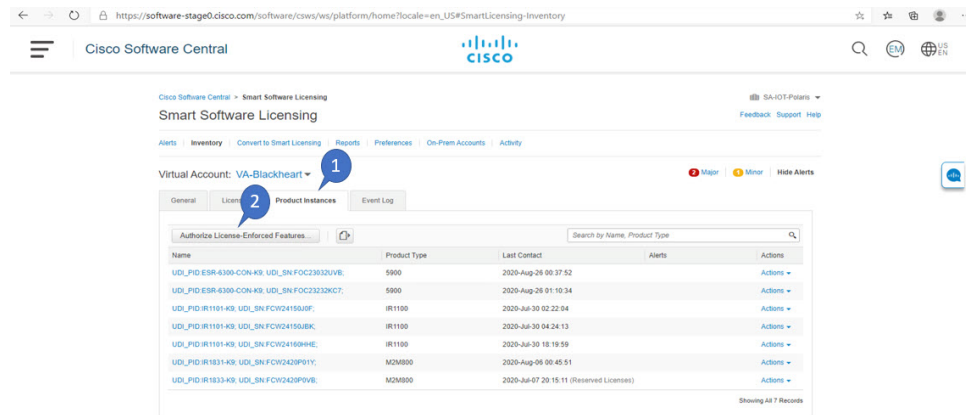
Step 1

Click on the **Product Instances** Tab.

Step 2

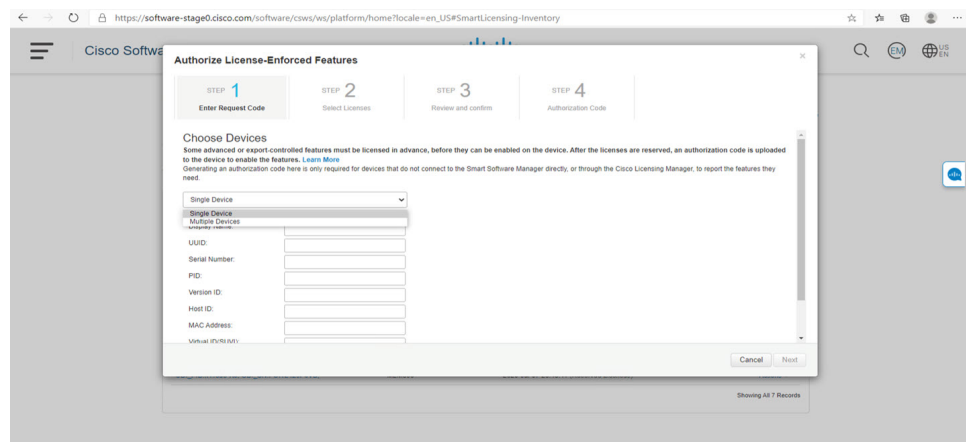
Click on **Authorize License-Enforced Features**.

Figure 19: Authorize License-Enforced Features



The **Authorize License-Enforced Features** window appears.

Figure 20: Authorize License-Enforced Features

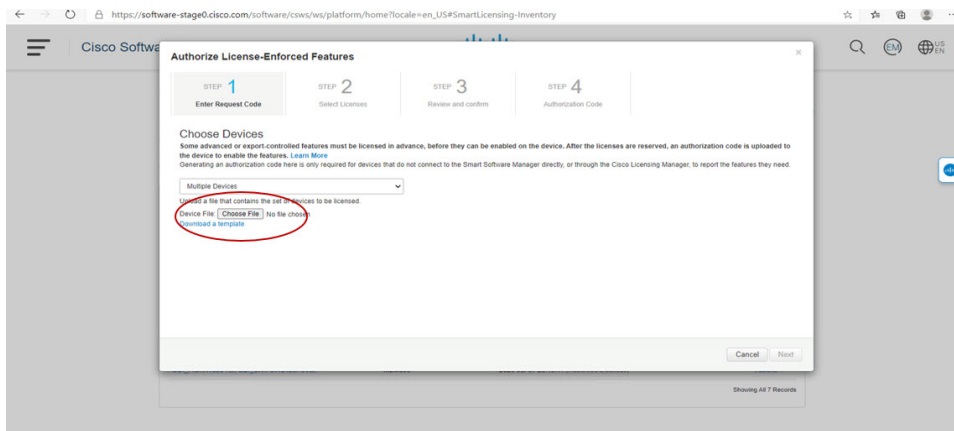


Step 3

Choose **Multiple** or **Single** devices from the pull-down.

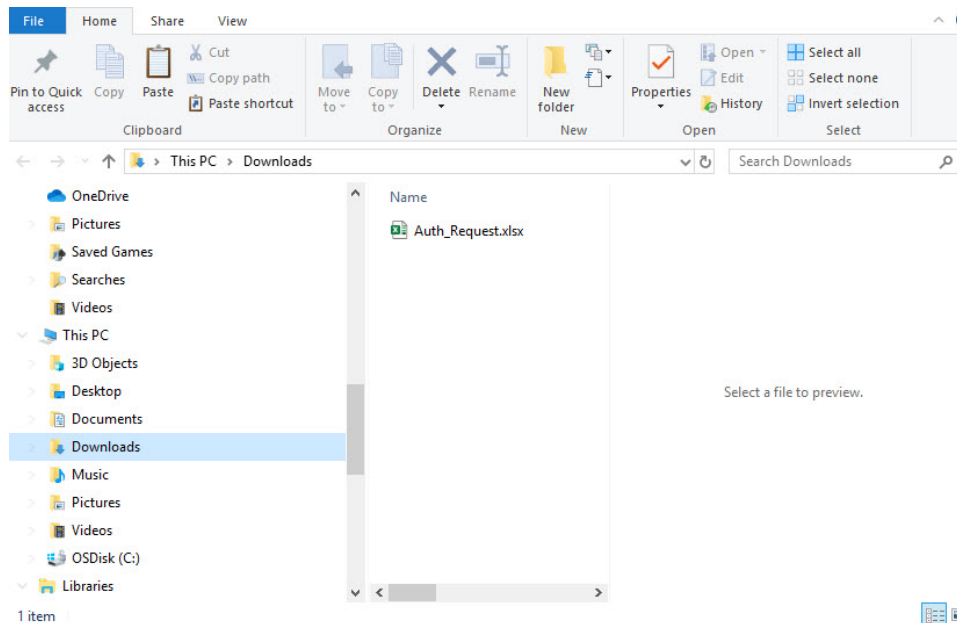
Step 4

The window changes to an option to select a device file. Click on **Choose File**.



Step 5 A popup window opens to navigate to where you saved your Authorization Request file on your laptop.

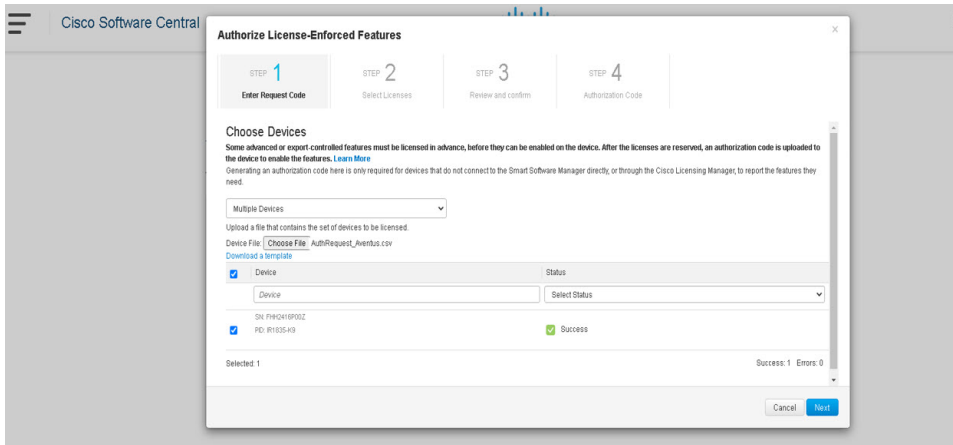
Figure 21: Open File Navigation Window



Step 6 Select your file, and then click **Open**.

Step 7 The authorization file loads, and the window changes to present your devices.

Figure 22: Present Devices



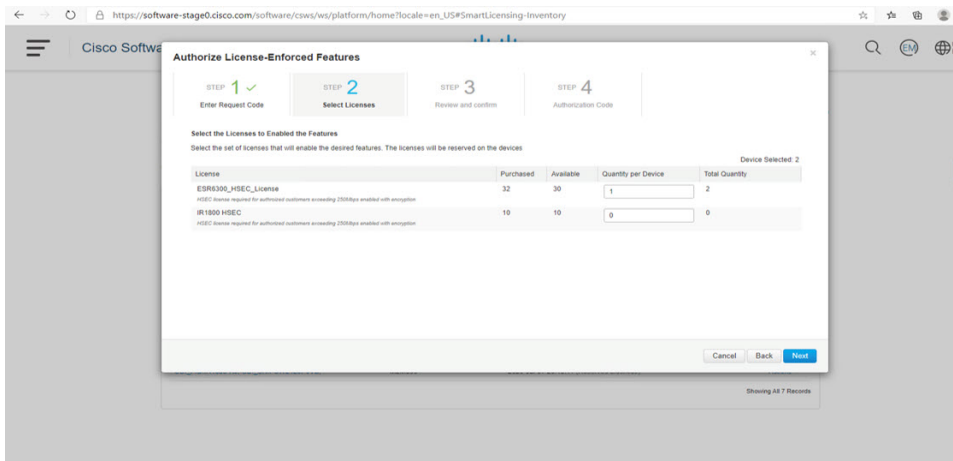
Step 8

When successful, click **Next**.

Step 9

The **Select Licenses** Tab opens.

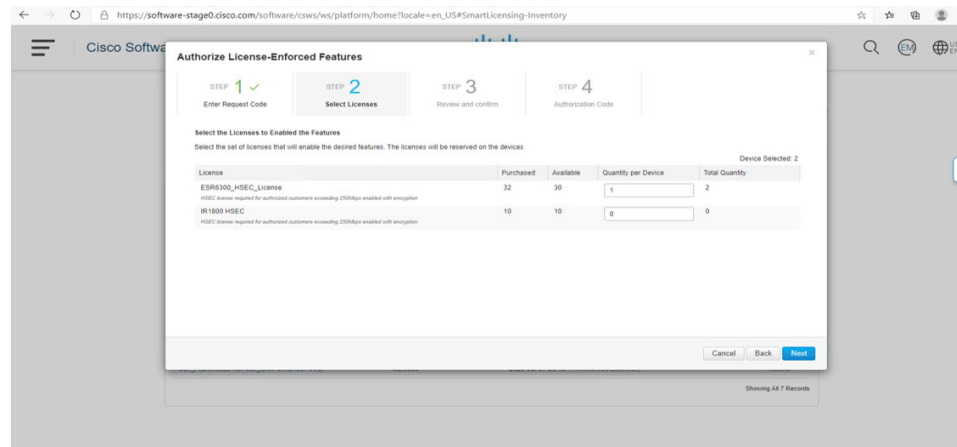
Figure 23: Select Licenses



Step 10

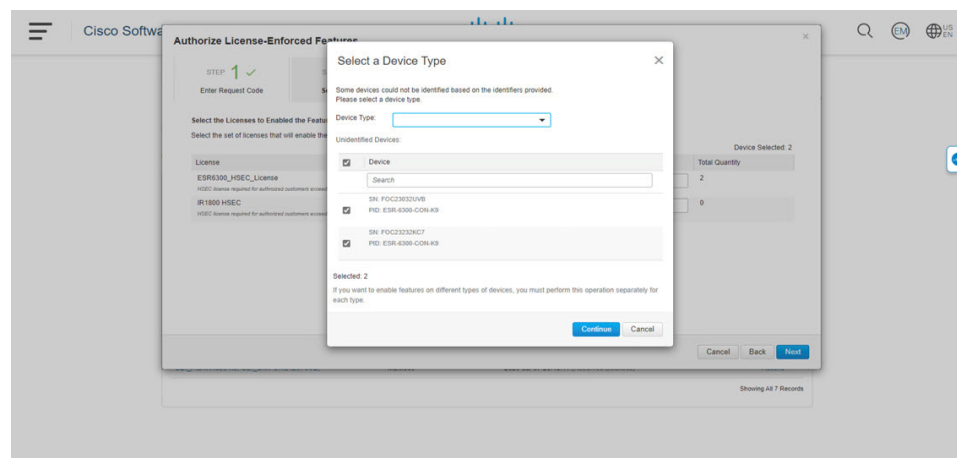
Under **Quantity per Device**, enter the number you wish.

Figure 24: Enter Number



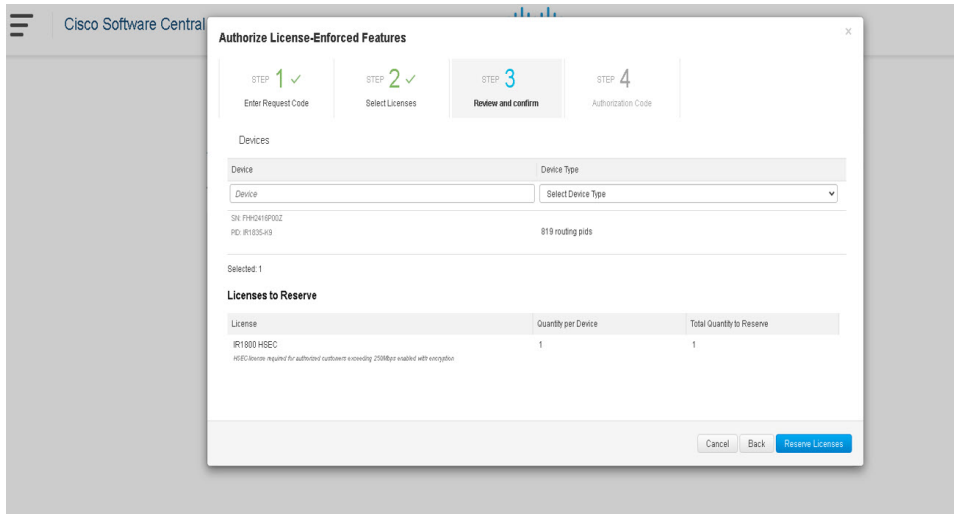
Step 11 If CSSM cannot identify your device from the identifying information, you can select it manually.

Figure 25: Select a Device Type



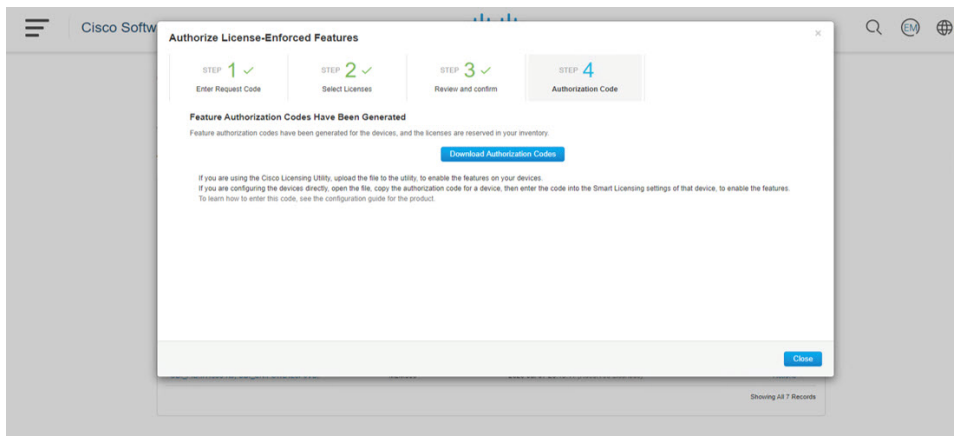
Step 12 Click **Continue**, and the window changes to **Review and Confirm**.

Figure 26: Review and Confirm



Step 13 Click on **Reserve Licenses**, and CSSM generates feature authorization codes.

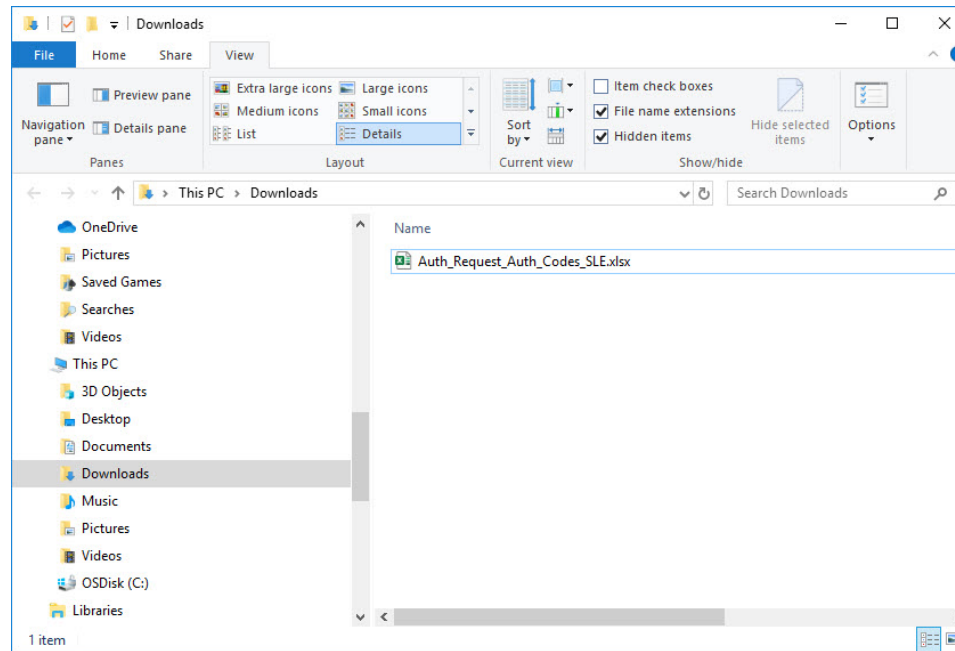
Figure 27: Feature Authorization Codes



Step 14 Click **Download Authorization Codes**, and a window opens to navigate to where you wish to save the codes.

Uploading the Authorization Request Code file into CSLU

Figure 28: Save Authorization Code



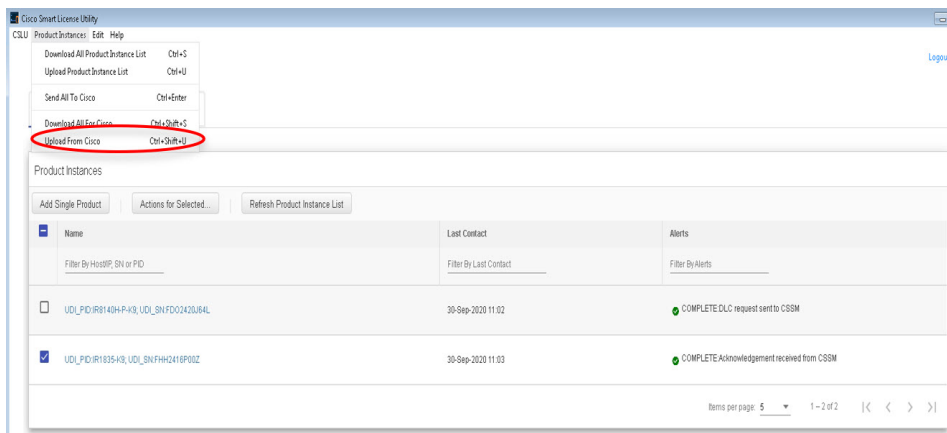
Step 15 Click **Ok**.

Uploading the Authorization Request Code file into CSLU

Step 1 Open the Cisco Smart License Utility (CSLU).

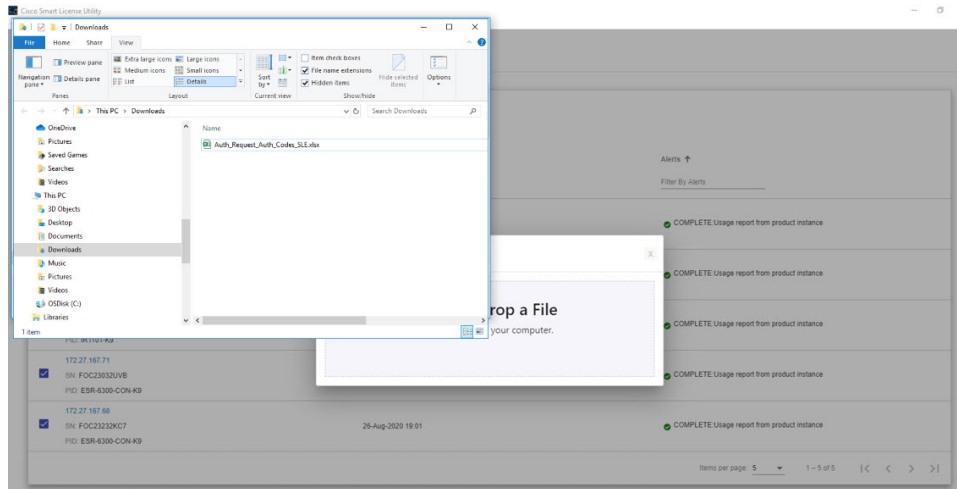
Step 2 Navigate to **Product Instances**, and then select **Upload From Cisco**.

Figure 29: Upload From Cisco



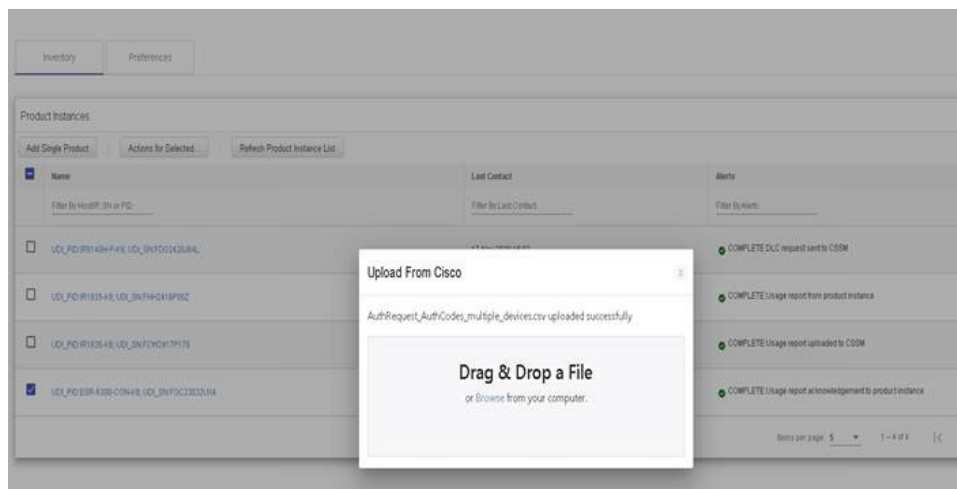
Step 3 There are two options to load your file. **Drag and Drop**, or **Browse** to where you saved your file. This example shows **Browse**.

Figure 30: Browse to File



Step 4 Select your authorization code file, and then click **Open**. The system uploads the authorization code file, then a successful upload message appears.

Figure 31: Successful Upload



License Installation Process in the Router

Perform the following from the command line interface.

IR1800 Example

Perform the following from the command line interface.

```
Router#show license summary
License Reservation is ENABLED
```

```

License Usage:
  License                               Entitlement tag                Count Status
  -----
  network-essentials_250M (IR1800_P_250M_E) 1 IN USE
  hseck9 (IR1800_HSEC) 1 IN USE
Router#show license usage
License Authorization:
  Status: Not Applicable
network-essentials_250M (IR1800_P_250M_E):
  Description: network-essentials_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-essentials_250M
  Feature Description: network-essentials_250M
  Enforcement type: NOT ENFORCED

hseck9 (IR1800_HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
Router(config)#end
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#show license summary
License Reservation is ENABLED
License Usage:
  License                               Entitlement tag                Count Status
  -----
  network-essentials_250M (IR1800_P_250M_E) 1 IN USE
  hseck9 (IR1800_HSEC) 1 IN USE
  network-essentials_2G (IR1800_P_2G_E) 1 IN USE

```

ESR6300 Example

Perform the following from the command line interface.

```

Router#show license summary
License Reservation is ENABLED
License Usage:
  License Entitlement tag Count Status
  network-advantage_250M (ESR6300_P_250M_E) 1 IN USE
  hseck9 (ESR6300_HSEC) 1 IN USE

Router#show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M

```



```

Feature Description: network-advantage_250M
Enforcement type: NOT ENFORCED
hseck9 (ESR6300_HSEC_License):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED

Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
Router(config)#end
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#show license summary
License Reservation is ENABLED License Usage:
  License                Entitlement tag          Count  Status
  network-advantage_250M (ESR6300_P_250M_A)      1      IN USE
  hseck9                  (ESR6300_HSEC_License) 1      IN USE
  network-advantage_2G    (ESR6300_P_2G_A)       1      IN USE

```

HSEC Installation

This example uses the IR8300 series router.

Perform the following from the command line interface.

```

Router#license smart authorization request add hseck9 local
Router#
Sep 23 05:29:37.894: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
  code was successfully installed on PID:IR8340-K9,SN:FDO2523J6N1
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#license feature hseck9
Router(config)#end
Router#show running-config | i license
license feature hseck9
license udi pid IR8340-K9 sn FDO2523J6N1
license boot level network-advantage
license smart url https://smartreceiver-stage.cisco.com/licservice/license
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
license smart transport smart
Router#
Router#show license summary
Account Information:
  Smart Account: SA-IOT-Polaris As of Sep 23 05:29:41 2021 UTC
  Virtual Account: Router

License Usage:
  License                Entitlement Tag          Count Status
  -----
  network-advantage_T1  (IR8300_NA_T1_PERF)      1 IN USE
  hseck9                 (IR8300_HSEC)            1 IN USE

Router#
Router#show license usage
License Authorization:
  Status: Not Applicable

```

```

.
.
.
hseck9 (IR8300_HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export

```

Change to Smart Licensing Packaging

This release brings the IoT routing products inline with other Integrated Service Routers (ISR).

Smart Licensing Overview

Cisco Smart Licensing is a flexible licensing model that provides users with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across their organization. And it's secure. With Smart Licensing users get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more Product Activation Keys (PAKs).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

Smart Licensing Using Policy (SLP), was previously referred to as Smart Licensing Enhanced (SLE), and is the default mode starting with Cisco IOS-XE release 17.3.2. SLE replaced Smart Software Licensing. This feature change for Cisco IOS XE release 17.11.1a focuses on the licensing packaging.

License Levels

The following are the license levels available for all Cisco IR devices.

Base Licenses

- Network Essentials
- Network Advantage (includes Network Essentials)



Note These licenses are ordered through Cisco Commerce Workspace (CCW), and are permanent.

Add-on Licenses — These can be subscribed for a fixed term of three, five, or seven years.

- Digital Networking Architecture (DNA) Essentials

- DNA Advantage (includes DNA Essentials)



Note These licenses are ordered through Cisco Commerce Workspace (CCW), and relate to DNA-C and SDWAN. For further information, see the [Cisco SD-WAN](#) and [Cisco DNA Center](#) web pages.

The following tables provide details on the licensing levels:

Table 12: Network Essentials (Perpetual License)

Essential Switch Capabilities	Layer 2, Routed Access(RIP, EIGRP Stub, OSPF (1000 routes)), PBR, PIM Stub Multicast (1000 routes) PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1x, Macsec-128, CoPP, SXP, IP SLA Responder SSO Note For the device to be compliant with the DNA Essential License it must not exceed 1000 routes in the routing table regardless of how the routes were learned.
DevOps Integration	<ul style="list-style-type: none"> • Netconf, Restconf, gRPC • Yang Data Models • GuestShell (On-Box Python) • PnP Agent, ZTP

Table 13: Network Advantage (Perpetual License) Contains all of the Network Essentials plus the following:

IoT & Mobility	CoAP
Full Routing Functionality	BGP, HSRP, OSPF, ISIS, GLBP
Flexible Network Segmentation	VRF, VXLAN, LISP, SGT, MPLS
High Availability & Resiliency	NSF, GIR, Stackwise Virtual*, ISSU/eFSU, Patching (CLI)
Optimize Bandwidth Utilization with Multicast	MSDP, mVPN, AutoRP, PIM-BIDIR

Table 14: DNA Essentials (3,5,7 year terms)

Basic Automation	<ul style="list-style-type: none"> • PnP Application • LAN Automation • Embedded Event Manager
Basic Assurance	<ul style="list-style-type: none"> • Health Dashboards – Network and Client • Basic Device & Wired Client Health Monitoring

Table 15: DNA Advantage (3,5,7 year terms) Contains all of the DNA Essentials plus the following:

Advanced Automation	<ul style="list-style-type: none"> • Encrypted Traffic Analytics • DNA Service for Bonjour
Assurance & Analytics	<ul style="list-style-type: none"> • Compliance, Custom Reports • Switch 360 & Wired Client 360

Licensing Throughput Levels

In addition to configuring the license level, it is also possible to configure the throughput level on the device. The throughput level determines the bandwidth limit which is applied to encrypted traffic. There is no limit applied to the non-encrypted (clear) traffic going through a device.



Important To comply with global export regulations, if more than 250Mbps of encrypted traffic is required, then an “uncapped” – platform dependent – selection must be done on CCW, as well as an HSEC license.

This limit is imposed bidirectionally. This means that if the throughput limit is set to 250Mbps then up to 250Mbps of encrypted traffic can flow through the device in either direction. For example, the device can both receive and transmit up to 250Mbps of encrypted traffic. There is no limit applied on unencrypted traffic.

When the throughput level on the device is set to ‘uncapped’ there are no limits imposed on both encrypted and unencrypted traffic flowing through it.



Note To avoid confusion on throughput limits and IOS XE software releases, please note the following:

Cisco IOS XE release 17.11.1a and earlier running on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses. These are configured using the **platform hardware throughput level 2G** CLI.

Future Cisco IOS XE release 17.12.1 and later running on the ESR6300, IR1800, and IR8140 support the same licenses, but will be configured using the **platform hardware throughput level uncapped** CLI.

With future Cisco IOS XE release 17.12.1 and later, the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will both provide the same throughput as the uncapped license.

The following table shows the throughput limits (also referred to as Tier license) supported on IoT devices as of Cisco IOS XE 17.11.1a release.

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR 6300	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR-6300-LIC-K9	N/A	Yes	N/A	N/A	N/A	Yes
IR1101	N/A	N/A	N/A	Yes	N/A	Supported starting with 17.10.1.
IR1800	N/A	Yes	N/A	Yes	Yes	To be supported starting with 17.12.1
IR8100	N/A	Yes	Yes	Yes	Yes	To be supported starting with 17.12.1
IR8300	Yes	N/A	Yes	N/A	N/A	Yes

Command Line Interface

The following commands are available:

```
license boot level <network-essentials/network-advantage>
```

The throughput level can be configured using the following CLI on all IR devices except IR8300:

```
platform hardware throughput level <limit>
```

On the IR8300, the throughput level can be configured using the following CLI:

```
platform hardware throughput crypto <limit>
```

To see the throughput configured on the device, use the following CLI:

```
show version | include throughput
```

```
The current crypto throughput level is: 50000 kbps
```

Uncapped License Implementation

The Cisco IOS XE 17.11.1 release introduced a new throughput level called "uncapped". This release extends the new throughput level to all of the Cisco IoT routing platforms. The following is a recap of the uncapped license implementation:

Licensing Throughput Levels

The throughput level determines the bandwidth limit which is applied to encrypted traffic. There is no limit applied to the non-encrypted (clear) traffic going through a device.



Important To comply with global export regulations, if more than 250Mbps of encrypted traffic is required, then an “uncapped” – platform dependent – selection must be done on CCW, as well as an HSEC license.

This limit is imposed bidirectionally. This means that if the throughput limit is set to 250Mbps then up to 250Mbps of encrypted traffic can flow through the device in either direction. For example, the device can both receive and transmit up to 250Mbps of encrypted traffic. There is no limit applied on unencrypted traffic.

When the throughput level on the device is set to "uncapped" there are no limits imposed on both encrypted and unencrypted traffic flowing through it.



Note To avoid confusion on throughput limits and IOS XE software releases, please note the following:

Cisco IOS XE release 17.11.1a and earlier running on the ESR6300, IR1800, and IR8140 platforms support boost, uncapped, and unlimited licenses. These are configured using the **platform hardware throughput level 2G** CLI.

Future Cisco IOS XE release 17.12.1a and later running on the ESR6300, IR1800, and IR8140 support the same licenses, but will be configured using the **platform hardware throughput level uncapped** CLI.

With Cisco IOS XE release 17.12.1a and later, the **platform hardware throughput level 2G** and the **platform hardware throughput level uncapped** CLIs will both provide the same throughput as the uncapped license.

The following table shows the throughput limits (also referred to as Tier license) supported on IoT devices.

Platform	25 Mbps bidirectional (Tier 0)	50 Mbps bidirectional	Up to 200 Mbps bidirectional (Tier 1)	250 Mbps bidirectional	2 Gbps	Uncapped (Tier 2)
ESR 6300	N/A	Yes	N/A	Yes	Yes	Supported starting with 17.12.1a
ESR-6300-LIC-K9	N/A	Yes	N/A	N/A	N/A	Yes
IR1101	N/A	N/A	N/A	Yes	N/A	Supported starting with 17.10.1.
IR1800	N/A	Yes	N/A	Yes	Yes	Supported starting with 17.12.1a
IR8100	N/A	Yes	Yes	Yes	Yes	Supported starting with 17.12.1a
IR8300	Yes	N/A	Yes	N/A	N/A	No



CHAPTER 10

Configuring Ethernet Switch Ports

This section contains the following:

- [Configuring VLANs, on page 137](#)
- [VLAN Trunking Protocol \(VTP\), on page 138](#)
- [Configuring 802.1x Authentication, on page 138](#)
- [Configuring Spanning Tree Protocol, on page 140](#)
- [Configuring MAC Address Table Manipulation, on page 141](#)
- [Configuring Switch Port Analyzer, on page 142](#)
- [Configuring IGMP Snooping, on page 143](#)

Configuring VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

On the ESR6300, all the Gigabit Ethernet LAN ports g0/1/0 through g0/1/4 are set up in vlan1, which does not need to be created.

The following is an example of a vlan configuration:

```
Router#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Gi0/1/0, Gi0/1/1, Gi0/1/2 Gi0/1/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Primary Secondary Type Ports
-----
```

```
Router#
```

You can assign a given port to a vlan by following these steps:

```
Router#conf t
Router(config)#int g 0/1/0
Router(config-if)#switchport access vlan 4
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#interface vlan 4
Router(config-if)#ipv4 address {ip} {mask}
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address autoconfig
Router(config-if)#no shut
Router(config-if)#end
```

To verify if the configuration took effect, use the **show run interface g0/1/0**, **show interface g0/1/0**, and **show vlan** commands.

IOS-XE supports Embedded Packet Capture (EPC), which provides an embedded systems management facility that helps in tracing and troubleshooting packets. This feature allows network administrators to capture data packets flowing through, to, and from a Cisco device. The network administrator may define the capture buffer size and type (circular, or linear), the maximum number of bytes of each packet to capture, and the direction of the traffic flow - ingress or egress, or both. The packet capture rate can be throttled using further administrative controls. For example, you can use the available options for filtering the packets to be captured using an Access Control List; and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval. For additional details see the guide located here: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xe-16-10/epc-xe-16-10-book/nm-packet-capture-xe.html>

VLAN Trunking Protocol (VTP)

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes mis-configurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

Further information about configuring VTP can be found here: http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

Configuring 802.1x Authentication

IEEE 802.1x port-based authentication defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication

server authenticates each client connected to a switch port before allowing access to any switch or LAN services. Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

With IEEE 802.1x authentication, the devices in the network have specific roles:

- **Supplicant**—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The supplicant is sometimes called the client.)
- **Authentication server**—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Authenticator**—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.



Note The ESR6300 supports authentication/authorization from TACACS+ server as well.

For detailed information on how to configure 802.1x port-based authentication, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

Example: Enabling IEEE 802.1x and AAA on a Switch Port

This example shows how to configure an ESR6300 router as 802.1x authenticator:

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# switchport mode access
Router(config-if)# access-session port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# access-session closed
Router(config-if)# access-session host-mode single-host
Router(config-if)# end
```

Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch. Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

For detailed configuration information on STP see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfid-1079138

Example: Spanning Tree Protocol Configuration

The following example shows configuring spanning-tree port priority of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses the port priority when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

The following example shows how to change the spanning-tree port cost of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

The following example shows configuring the bridge priority of VLAN 10 to 33792:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

The following example shows configuring the hello time for VLAN 10 being configured to 7 seconds. The hello time is the interval between the generation of configuration messages by the root switch.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 7
Router(config)# end
```

The following example shows configuring forward delay time. The forward delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

The following example shows configuring maximum age interval for the spanning tree. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

Configuring MAC Address Table Manipulation

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use. You can use the aging time setting to define how long the switch retains unseen addresses in the table.
- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port associated with the address and the type (static or dynamic).

See the “Example: MAC Address Table Manipulation” for sample configurations for enabling secure MAC address, creating a static entry, set the maximum number of secure MAC addresses and set the aging time.

For detailed configuration information on MAC address table manipulation see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

Example: MAC Address Table Manipulation

The following example shows creating a static entry in the MAC address table.

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface GigabitEthernet0/1/0 vlan
3
Router(config)# end
```

The following example shows setting the aging timer.

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

Configuring Switch Port Analyzer

The Cisco ESR6300 supports local SPAN only, and up to one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source can be monitored by using SPAN; traffic routed to a source cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another source cannot be monitored; however, traffic that is received on the source and routed to another can be monitored.

For detailed information on how to configure a switched port analyzer (SPAN) session, see the following web link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

Example: SPAN Configuration

The following example shows how to configure a SPAN session to monitor bidirectional traffic from an interface:

```
Router# configure terminal
Router(config)# monitor session 1 source GigabitEthernet0/1/0
Router(config)# end
```

The following example shows how to configure an interface as the destination for a SPAN session:

```
Router# configure terminal
Router(config)# monitor session 1 destination GigabitEthernet0/1/0
Router(config)# end
```

The following example shows how to remove the interface as a SPAN source for SPAN session 1:

```
Router# configure terminal  
Router(config)# no monitor session 1 source GigabitEthernet0/1/0  
Router(config)# end
```

Configuring IGMP Snooping

IGMP snooping constrains the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Use the **ip igmp snooping enable** command to configure IGMP Snooping on the ESR6300.

By default, IGMP snooping is globally enabled in the ESR6300.

MLD snooping is also supported on the ESR6300, and further information can be found in this documentation set: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/configuration_guide/b_161_consolidated_3850_cg/b_161_consolidated_3850_cg_chapter_01100.html



CHAPTER 11

Gigabit Ethernet Combo Ports WAN

This section contains the following topics:

- [Gigabit Ethernet Combo Ports WAN, on page 145](#)
- [Command Line Interface, on page 146](#)

Gigabit Ethernet Combo Ports WAN

Two Combo ports, Copper and Fiber ports (SFP) ports are available on the ESR6300. A combo port means that you can use either the RJ45 port or the SFP port. They are paired in two (which ports that are paired are usually indicated by arrows, lines or the like). Only one of the ports in the pair can be active at any given time. Usually the first port that gets a valid link will be the active one, but in some cases you need to specifically configure whether you want to use the RJ45 port or the SFP port.

The Copper ports support standard 3-speed, 10/100/1000Base-T protocol. The SFP supports standard 1000Base-X or 100Base-FX Ethernet over single-mode or multi-mode optics. A complete list of the supported SFPs can be found in the ESR6300 Hardware Technical Manual: <https://www.cisco.com/c/en/us/td/docs/routers/embedded/6300/hardware/tech-guide/ESR6300-tech-guide.html>

The interface names for the two combo ports are g0/0/0 and g0/0/1.



Note The GLC-T and GLC-TE are the only copper SFPs supported by Cisco, and the **service unsupported-transceiver** CLI must be mandatorily enabled if they are used.

Before you configure the combo ports, note the following:

- Copper FE SFPs are not supported on ESR6300
- Auto-negotiation for 10Mbps, 100Mbps, 1000Mbps in full-duplex and half-duplex mode is supported. For half duplex, support is only on 10Mbps and 100Mbps.
- Auto-select is supported. Whichever interface is detected first is selected. Typically fiber SFP bring-up is faster than RJ45 Copper is faster than Copper SFP.
- All Standard Cisco Layer 3 Routing Protocols are Supported on ESR6300 WAN interfaces.
- If running IOS-XE version 17.1.x and below, Jumbo MTU support is not available on the ESR6300. MTU >1500 packets will be fragmented. If running IOS-XE release 17.2.1 and above, MTU support is 64 - 9216 on the interface. If there are bursts of fragmented traffic expected beyond the device Non-drop

rate capability, IOS-XE implements a throttling mechanism and transmits MAC pause frames to other end to reduce rate of traffic. To resume normal operation, arp has to be sent again to re-negotiate. The default ip arp timeout is 14,000 seconds. In such corner case scenarios, it is recommended to have a much shorter arp timeout configuration.

- Auto-select is supported. Whichever interface is detected first is selected. Typically, fiber SFP bring-up is faster than RJ45 Copper, which is faster than Copper SFP.
- Auto-failover is supported as well between like GE Ethernet and GE SFP. In case one physical link goes down, the other mode will immediately kick-in.
- RJ45 to SFP mode conversion involves an interface reset (shut/no shut, interface DOWN/UP). The syslog can be observed accordingly.



Note For ARP, you must configure Ethernet II frames instead of 802.3 frames. If 802.3 frames are used, they may be recorded as SNAP encapsulation, which is currently not supported.

Command Line Interface

The following CLIs are available.

To configure a WAN port as RJ45 or SFP:

```
Router#config terminal
Router(config)#interface g0/0/{0|1}
Router(config-if)#media-type ?
  auto-select  Use whichever connector is attached
  rj45         Use RJ45 connector
  sfp          Use SFP connector
```

To configure auto-failover:

```
Router(config-if)#media-type {rj45|sfp} ?
  auto-failover  Automatic Fail over
```

To change the media type:

```
Router#conf t
Router(config)#int g 0/0/0
Router(config-if)#no shut
Router(config-if)#media-type sfp
GigabitEthernet0/0/0: Changing media to SFP
Router(config-if)#end
```

Other helpful commands to verify your configuration:

To verify if SFP is detected:

```
Router#show inventory
```

```
+++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++
```

```
NAME: "Chassis", DESCR: "Embedded Services Router with 2 Gigabit Ethernet routed ports,4
Gigabit Ethernet switched ports, no cooling plate"
PID: ESR-6300-NCP-K9 , VID: V00 , SN: FOC23032UUN
```



```
NAME: "Power Supply Module 0", DESCR: "External Power Supply Module"  
PID: PWR-12V , VID: , SN:
```

```
NAME: "module 0", DESCR: "Cisco ESR-6300-NCP-K9 Fixed and pluggable Interface Module  
controller"  
PID: ESR-6300-NCP-K9 , VID: , SN:
```

```
NAME: "NIM subslot 0/1", DESCR: "ESR-6300-ES-4"  
PID: ESR-6300-ES-4 , VID: V01 , SN:
```

```
NAME: "NIM subslot 0/0", DESCR: "Front Panel 2 port Gigabitethernet Module"  
PID: ESR-6300-2x1GE , VID: V01 , SN:
```

```
NAME: "module R0", DESCR: "Cisco ESR-6300-NCP-K9 Route Processor"  
PID: ESR-6300-NCP-K9 , VID: V00 , SN: FOC23032UUN
```

```
NAME: "module F0", DESCR: "Cisco ESR-6300-NCP-K9 Forwarding Processor"  
PID: ESR-6300-NCP-K9 , VID: , SN:
```

To verify if the configuration has taken effect:

```
Router#Conf t  
Router(config)#int g 0/0/0  
Router(config-if)#no shut  
Router(config-if)#media-type sfp  
GigabitEthernet0/0/0: Changing media to SFP  
Router(config-if)#end
```

To reload the Gigabit Ethernet module:

```
Router#hwmodule subslot 0/0 reload force
```




CHAPTER 12

SD-WAN Remote Access

- [SD-WAN, on page 149](#)

SD-WAN

SD-WAN RA is now supported on the IoT routers with IOS XE 17.13.1. SD-WAN RA is a combination of two features:

- IOS-XE SD-WAN
- IOS-XE FlexVPN Remote Access Server



Note All IoT devices only support the SD-WAN RA Client.

Information on SD-WAN Remote Access can be found in the following guide:

[Cisco Catalyst SD-WAN Remote Access](#)

Additional Documentation

Additional documentation for SDWAN/vManage is available at the following links:

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#)
- [Cisco Catalyst SD-WAN](#)
- [Cisco SD-WAN Support Information](#)
- [Cisco vManage Monitor Overview](#)
- [Managing the SD-Routing Device Using Cisco SD-WAN Manager](#)



CHAPTER 13

CLI Output for the FN980 5G Modem

- [Change in CLI Output for the FN980 5G Modem, on page 151](#)

Change in CLI Output for the FN980 5G Modem

This release has a different output to the **show cellular 0/x/0 radio band** command. The module will no longer display the 5G-SA band information by default. However, once the 5G-SA has been enabled, the band information will then be displayed.

See the following command examples using an IR1101 running IOS XE 17.13.1 with an FN980 modem:

```
IR1101#show cellular 0/1/0 radio band
```

```
LTE bands supported by modem:
```

```
- Bands 2 4 5 12 14 26 29 30 46 48 66.
```

```
LTE band Preference settings for the active sim(slot 1):
```

```
- Bands 2 4 5 12 14 26 29 30 46 48 66.
```

```
NR5G NSA bands supported by modem:
```

```
- Bands 2 5 12 66 77.
```

```
NR5G NSA band Preference settings for the active sim(slot 1):
```

```
- Bands 2 5 12 66 77.
```

```
3G bands supported by modem:
```

```
Index: <none>
```

```
3G band Preference settings for the active sim(slot 1):
```

```
Index: <none>
```

```
=====
```

```
Band index reference list:
```

```
For LTE and 5G, indices 1-128 correspond to bands 1-128.
```

```
For 3G, indices 1-64 maps to the 3G bands mentioned against each above.
```

```
IR1101#
```

```
IR1101#show cellular 0/1/0 hard
```

```
*Nov 8 12:13:31.969: Graphit 5G RSRP/RSRQ LTE modem:[1]
```

```
Modem Firmware Version = M0H.030202
```

```
Host Firmware Version = A0H.000302
```

```
Device Model ID = FN980
```

```
International Mobile Subscriber Identity (IMSI) = 001010123456789
```

```
International Mobile Equipment Identity (IMEI) = 359661100035795
```

```

Integrated Circuit Card ID (ICCID) = 89860000502000180722
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Modem Online
Current Modem Temperature = 40 deg C
PRI version = 1080-114, Carrier = Generic GCF
OEM PRI version = 1080-114
IR1101#

IR1101#show cellular 0/1/0 radio band

LTE bands supported by modem:
- Bands 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66
  71.
LTE band Preference settings for the active sim(slot 0):
- Bands 1 2 3 4 5 7 8 12 13 14 17 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66
  71.

NR5G NSA bands supported by modem:
- Bands 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79.
NR5G NSA band Preference settings for the active sim(slot 0):
- Bands 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79.

NR5G SA bands supported by modem:
- Bands <none>
NR5G SA band Preference settings for the active sim(slot 0):
- Bands <none>

3G bands supported by modem:
Index:
  23 - UMTS Band 1: 2100 MHz (IMT)
  24 - UMTS Band 2: 1900 MHz (PCS A-F)
  26 - UMTS Band 4: 1700 MHz (AWS A-F)
  27 - UMTS Band 5: US 850 MHz (CLR)
  50 - UMTS Band 8: 900 MHz (E-GSM)
  51 - UMTS Band 9: Japan 1700 MHz
  61 - UMTS Band 19: 800 MHz (800 Japan)
3G band Preference settings for the active sim(slot 0):
Index:
  23 - UMTS Band 1: 2100 MHz (IMT)
  24 - UMTS Band 2: 1900 MHz (PCS A-F)
  26 - UMTS Band 4: 1700 MHz (AWS A-F)
  27 - UMTS Band 5: US 850 MHz (CLR)
  50 - UMTS Band 8: 900 MHz (E-GSM)
  51 - UMTS Band 9: Japan 1700 MHz
  61 - UMTS Band 19: 800 MHz (800 Japan)

=====

Band index reference list:

For LTE and 5G, indices 1-128 correspond to bands 1-128.

For 3G, indices 1-64 maps to the 3G bands mentioned against each above.

IR1101#

```



CHAPTER 14

MAB 802-1x Support

- [MAB 802.1x Support, on page 153](#)

MAB 802.1x Support

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

For further information, see the [Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE](#)



CHAPTER 15

Enable Secure Data Wipe Capabilities

- [Enable Secure Data Wipe Capabilities, on page 155](#)

Enable Secure Data Wipe Capabilities

Secure data wipe is a Cisco wide initiative to ensure storage devices on all the IOS XE based platforms to be properly purged using NIST SP 800-88r1 compliant secure erase commands. Whenever possible, IoT platforms will leverage the corresponding ENG design and implementation available so far on their platforms.

This feature is supported on the following IoT platforms:

- IR1101
- IR1800
- IR8140
- ESR6300

When the enable secure data wipe is executed, the following will get wiped out:

- IR1101, IR1800, IR8140: NVRAM, rommon variables, and bootflash
- ESR6300: NVARM, rommon variables, bootflash

The router will be in rommon prompt with default factory settings (baud rate 9600) after the command is executed. The bootflash will not get formatted until booting with IOS image thru usbflash or tftp download if the platform is supported.

Performing a Secure Data Wipe

To enable the feature, perform the following:

```
Router#factory-reset all secure
```

```
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]Y
```



Important This operation may take hours. Please do not power cycle.

To check the log after the command is executed, and booting up IOS XE, perform the following:

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```



CHAPTER 16

Implementing Multicast Service Reflection

This chapter contains the following topics:

- [Multicast Service Reflection Overview, on page 157](#)

Multicast Service Reflection Overview

The Cisco Multicast Service Reflection feature provides the capability for users to translate externally received multicast or unicast destination addresses to multicast or unicast addresses that conform to their organization's internal addressing policy. Using this feature, users do not need to redistribute unicast routes from external sources at the translation boundary into their network infrastructure for Reverse Path Forwarding (RPF) to work properly. In addition, users can receive identical feeds from two ingress points in the network and route them independently.

Prerequisites for Implementing Multicast Service Reflection

- Configure your multicast-enabled network with the necessary infrastructure to run either Protocol Independent Multicast Sparse Mode (PIM-SM), Bidirectional PIM (bidir-PIM), or PIM Source Specific Multicast (PIM-SSM). The configuration process may include configuring RPs, interface boundaries, or SSM ranges.
- Confirm that the virtual interface for multicast service reflection (Vifl interface) is installed in your border router and the Multicast Service Reflection application is installed and operational.
- Each active receiver must initiate an Internet Group Management Protocol (IGMP) join to the multicast group that is defined on the router in the PIM domain.

Restrictions for Implementing Multicast Service Reflection

- When translating groups of multicast packets that are destined for the same multicast group but are originating from different sources, as in the case when using PIM-SSM, all multicast packets destined for a particular SSM group will get mapped to a single (S, G) after translation has occurred. For example, if (10.1.1.1, 232.1.1.1) and (10.1.1.2, 232.1.1.1) need to be translated, they will appear as a single entry, for example, (92.168.1.2, 232.239.1.1), where 92.168.1.2 is an IP address that resides in the Vifl IP subnet.
- PIM/IGMP control packets are not translated.

- The following types of translation are not supported in Cisco IOS XE software:
 - Unicast-to-Multicast Destination Translation
 - Unicast-to-Multicast Destination Splitting
- The use of a sub-interface as an input-interface has not been tested on platforms that are based on mcp_dev.

Information About Implementing Multicast Service Reflection

This section contains the following:

Benefits of Implementing Multicast Service Reflection

- Allows users to translate externally received multicast or unicast destination addresses to multicast or unicast addresses that conform to their company's internal addressing policy. This allows the separation of the private addressing scheme used by the content provider from the public addressing used by the service provider. The following types of translations are supported:
 - Multicast-to-Multicast Destination Translation
 - Multicast-to-Unicast Destination Translation
 - Multicast-to-Multicast Destination Splitting
 - Multicast-to-Unicast Destination Splitting
- Provides logical separation between private and public multicast networks.
- Provides the flexibility to forward multicast packets--translated or untranslated--out the same outgoing interface.
- Provides redundancy by allowing users to get identical feeds from two ingress points in the network and route them independently.
- Allows users to use the subnet of their choice to be the source network and scope it appropriately.

Rendezvous Point (RP)

A Rendezvous Point (RP) is a role that a router performs when operating in PIM-SM or bidirectional PIM. An RP is required only in networks running PIM-SM or bidirectional PIM. In PIM-SM, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, first hop designated routers with directly connected sources initially send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the last hop router with a directly connected receiver receives traffic from the shared tree, it immediately performs a shortest path tree switchover and sends a Join message towards the source, creating a source-based distribution tree between the source and the receiver.

PIM Sparse Mode

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic.

Unlike dense mode interfaces, sparse mode interfaces are added to the multicast routing table only when periodic Join messages are received from downstream routers, or when a directly connected member is on the interface. When forwarding from a LAN, sparse mode operation occurs if an RP is known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense mode fashion. If the multicast traffic from a specific source is sufficient, the first hop router of the receiver may send Join messages toward the source to build a source-based distribution tree.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network.

In sparse mode, a router assumes that other routers do not want to forward multicast packets for a group, unless there is an explicit request for the traffic. When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP tracks multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree. If the multicast traffic from a specific source is sufficient, the first hop router of the host may send Join messages toward the source to build a source-based distribution tree.

First-hop designated routers with directly connected sources register with the RP and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S, G) Join messages toward that source. Each router along the reverse path compares the unicast routing metric of the RP address to the metric of the source address. If the metric for the source address is better, it will forward a PIM (S, G) Join message toward the source. If the metric for the RP is the same or better, then the PIM (S, G) Join message will be sent in the same direction as the RP. In this case, the shared tree and the source tree would be considered congruent.

If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This behavior is the default behavior in Cisco IOS software. Network administrators can force traffic to stay on the shared tree by using the Cisco IOS **ip pim spt-threshold infinity** command.

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

Vif1 Interface

The Vif1 interface is similar to a loopback interface--it is a logical IP interface that is always up when the router is active.

The Vif1 interface needs to reside on its own unique subnet, and that subnet should be advertised in the Interior Gateway Protocol (IGP) updates (RIP, EIGRP, OSPF, ISIS).

The Vif1 interface maintains information about the input interface, private-to-public mgroup mappings, mask length, which defines your pool range, and the source of the translated packet.

Multicast Service Reflection Application

Cisco multicast service reflection is an application running in Cisco IOS software interrupt level switching that processes packets forwarded by Cisco IOS software to the Vif1 interface. Unlike IP multicast Network Address Translation (NAT), which only translates the source IP address, the IP reflect service translates both source and destination addresses. Multicast service reflection is especially useful when users that have not yet moved to the new multicast group still need to receive the untranslated stream.

Multicast service reflection is implemented using an interface CLI statement. Each configured multicast service reflection CLI statement establishes a packet match and rewrite operation acting on packets sent by Cisco IOS unicast or multicast packet routing onto the Vif1 interface. The matched and rewritten packet is sent back into Cisco IOS unicast or multicast packet routing, where it is handled like any other packet arriving from an interface.

The Vif1 interface is a receiver for the original stream and makes it appear that the new stream is coming from a source directly connected to the Vif1 subnet. The Vif1 interface is a Designated Router (DR) for active sources and registers with the appropriate RP.

More than one multicast service reflection operation can be configured to match the same packets, which allows you to replicate the same received traffic to multiple destination addresses.

How to Implement Multicast Service Reflection

This section contains the following:

Configuring Multicast Service Reflection

Perform this task to configure multicast service reflection.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip multicast-routing [distributed] Example: Router(config)# ip multicast-routing	Enables IP multicast routing. • Use the distributed keyword to enable the Multicast Distributed Switching feature.
Step 4	interface <i>type number</i> Example: Router(config)# interface ethernet 0	Enters interface configuration mode for the specified interface type and number.
Step 5	ip pim sparse-mode Example: Router(config-if)# ip pim sparse-mode	Enables PIM sparse mode on the interface.

	Command or Action	Purpose
Step 6	no shutdown Example: Router(config-if)# no shutdown	Enables an interface.
Step 7	exit Example: Router(config-if)# exit	Exits interface configuration mode, and returns to global configuration mode.
Step 8	Repeat Steps 4 through 7 for each PIM interface.	--
Step 9	interface Vif1 Example: Router(config)# interface Vif1	Enters interface configuration mode for the Vif1 interface.
Step 10	ip address ip-address mask [secondary] Example: Router(config-if)# ip address 10.1.1.1 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 11	ip pim sparse-mode Example: Router(config-if)# ip pim sparse-mode	Enables PIM sparse mode on an interface.
Step 12	ip service reflect input-interface destination destination-address to new-destination-address mask-len number source new-source-address Example: Router(config-if)# ip service reflect ethernet0 destination 224.1.1.0 to 239.2.2.0 mask-len 24 source 10.1.1.2	Matches and rewrites multicast packets routed onto the Vif1 interface. <ul style="list-style-type: none"> The matched and rewritten packets are sent back into Cisco multicast packet routing (or unicast routing if the destination is unicast), where they are handled like any other packets arriving from an interface.
Step 13	ip igmp static-group {* group-address [source {source-address ssm-map}]} Example: Router(config-if)# ip igmp static-group 224.1.1.1	Configures the router to be a statically connected member of the specified group on the interface, and forwards traffic destined for the multicast group onto the interface. <ul style="list-style-type: none"> This step is only applicable for multicast-to-multicast and multicast-to-unicast scenarios.
Step 14	end Example: Router(config-if)# end	Exits interface configuration mode, and returns to privileged EXEC mode.

Configuration Examples for Multicast Service Reflection

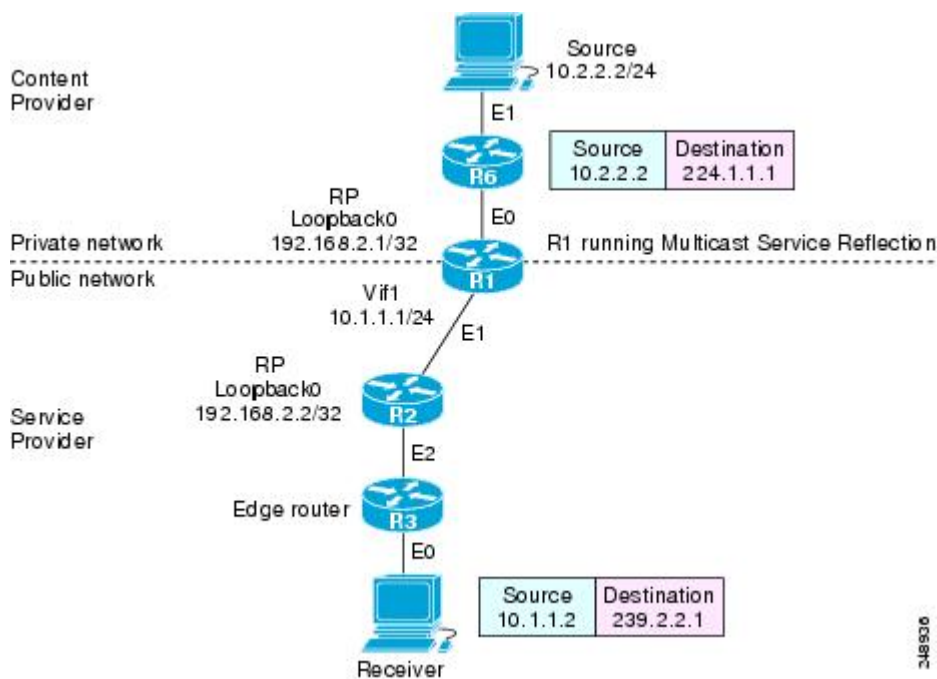
See the following examples.

Example Multicast-to-Multicast Destination Translation

The following example shows how to implement multicast service reflection (multicast-to-multicast destination translation) in a service provider network. Multicast-to-Multicast Destination Translation allows service providers to translate externally received content provider multicast destination addresses to multicast destination addresses that conform to the service provider's internal addressing policy.

This example uses the topology illustrated in the figure.

Figure 32: Multicast Service Reflection (Multicast-to-Multicast Destination Translation) in a Service Provider Network Example Topology



In this example topology, a content provider is sending financial market information to a service provider, which in turn is sending that information to active receivers (brokerage houses). The service provider may be receiving market data from multiple content providers.

Router R1 is an edge router in the service provider's PIM domain.

Router R1 has a loopback interface and is acting as the RP for the 224.1.1.0/24 address range.

Router R1 has a Vif1 interface and is running the multicast service reflection application.

Router R2 has a loopback interface and is acting as the RP for the 239.2.2.0/24 address range.

Enter these commands on the router running the multicast service reflection application (R1):

```
!
configure terminal
 ip multicast-routing
 interface <all IP numbered interfaces>
 ip pim sparse-mode
```



```

no shutdown
!
! Configure the loopback interface for the Service Provider RP
!
interface loopback 0
ip address 192.168.2.1 255.255.255.255
ip pim sparse-mode
!
ip pim rp-address 192.168.2.1 mcast-content-provider-groups override
ip pim rp-address 192.168.2.2 mcast-service-provider-groups override
ip access-list standard mcast-content-provider-groups permit 224.1.1.0 0.0.0.255
ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
!
! Configure the Vif1 virtual interface for multicast service reflection
!
interface Vif1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip service reflect Ethernet 0 destination 224.1.1.0 to 239.2.2.0 mask-len 24 source 10.1.1.2

ip igmp static-group 224.1.1.0
ip igmp static-group 224.1.1.1
ip igmp static-group 224.1.1.2
ip igmp static-group 224.1.1.3
.
.
.
ip igmp static-group 224.1.1.255

```

Enter these commands on the router that is the RP in the service provider network (R2):

```

ip multicast-routing
interface <all IP numbered interfaces>
 ip pim sparse-mode
 no shutdown
!
interface loopback 0
 ip address 192.168.2.2 255.255.255.255
 ip pim sparse-mode
!
ip pim rp-address 192.168.2.2 mcast-service-provider-groups override
ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
!

```

Enter these commands on all the other routers in the service provider network (R3):

```

ip multicast-routing
interface <all IP numbered interfaces>
 ip pim sparse-mode
 no shutdown
!
ip pim rp-address 192.168.2.2 mcast-service-provider-groups override
ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
end

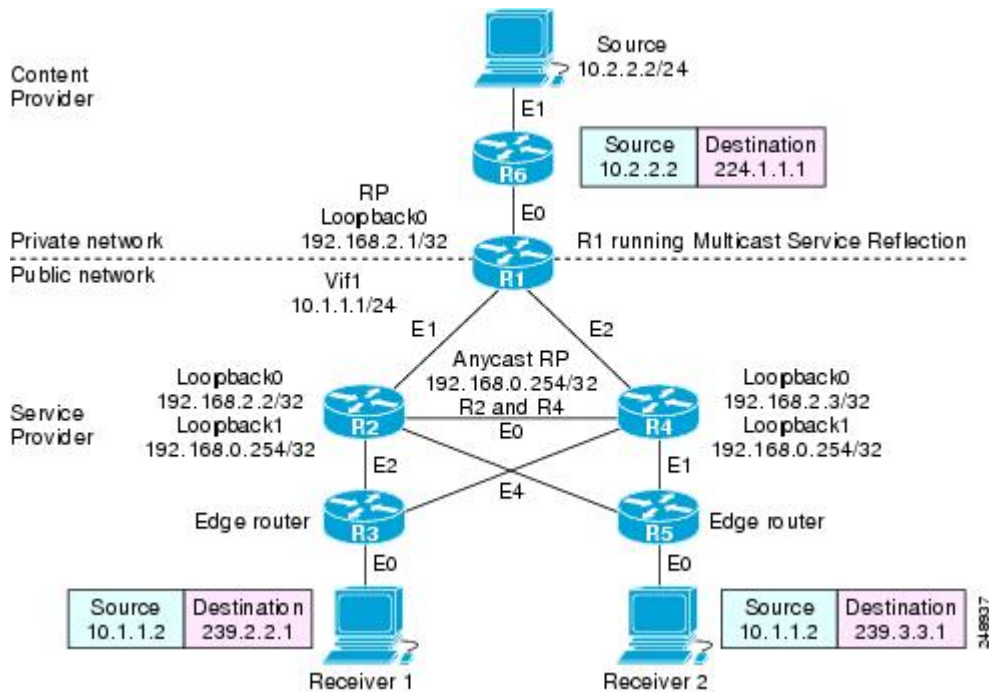
```

Example Multicast-to-Unicast Destination Translation

The following example shows how to implement multicast service reflection (multicast-to-unicast destination translation) in a service provider network. Multicast-to-Unicast Destination Translation allows service providers to translate externally received content provider multicast destination addresses to unicast destination addresses that conform to the service provider's internal addressing policy.

This example uses the topology illustrated in the figure.

Figure 33: Multicast Service Reflection (Multicast-to-Unicast Destination Translation) in a Service Provider Network Example Topology



In this example topology, a content provider is sending financial market information to a service provider, which in turn is sending that information to active receivers (brokerage houses). The service provider may be receiving market data from multiple content providers.

Router R1 is an edge router in the service provider's PIM domain.

Router R1 has a loopback interface and is acting as the RP for the 224.1.1.0/24 address range.

Router R1 has a Vif1 interface and is running the multicast service reflection application.

Routers R2 and R3 are non PIM enabled routers running unicast routing only in the service provider network.

Enter these commands on the router running the multicast service reflection application (R1):

```
configure terminal
ip multicast-routing
interface <all IP numbered interfaces>
ip pim sparse-mode
no shutdown
!

! Configure the loopback interface for the Service Provider RP
!
interface loopback 0
ip address 192.168.2.1 255.255.255.255
ip pim sparse-mode
!
ip pim rp-address 192.168.2.1 mcast-content-provider-groups override
ip access-list standard mcast-content-provider-groups permit 224.1.1.10 0.0.0.255
!
```

```

! Configure the Vif1 virtual interface for multicast service reflection
!
interface Vif1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip service reflect Ethernet 0 destination 224.1.1.0 to 10.3.3.0 mask-len 24 source 10.1.1.2
end

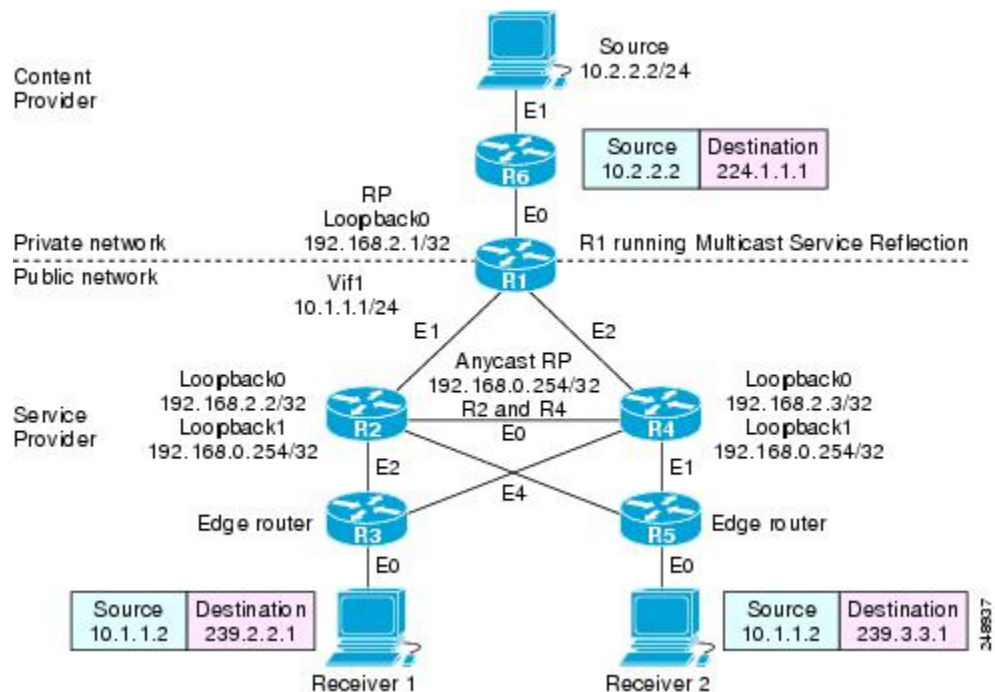
```

Example Multicast-to-Multicast Destination Splitting

The following example shows how to implement multicast service reflection (multicast-to-multicast destination splitting where the multicast single stream is converted into two unique multicast streams) in a service provider network. Multicast-to-Multicast Destination Splitting allows service providers to translate externally received content provider multicast destination addresses to multiple multicast destination addresses that conform to the service provider's internal addressing policy.

This example uses the topology illustrated in the figure.

Figure 34: Multicast Service Reflection (Multicast-to-Multicast Destination Splitting) in a Service Provider Network Example Topology



In this example topology, a content provider is sending financial market information to a service provider, which in turn is sending that information to active receivers (brokerage houses). The service provider may be receiving market data from multiple content providers.

Router R1 is an edge router in the service provider's PIM domain.

Router R1 has a loopback configured and is acting as an RP for the 224.1.1.0/24 address range.

Router R1 has a Vif1 interface and is running the multicast service reflection application.

Routers R2 and R4 have multiple loopback interfaces and are acting as anycast RPs for the 239.2.2.0 and 239.3.3.0 address ranges.

Router R3 and R5 are edge routers in the service provider's PIM domain.

Enter these commands on the router running the multicast service reflection application (R1):

```
configure terminal
 ip multicast-routing
 interface <all IP numbered interfaces>
 ip pim sparse-mode
 no shutdown
 !

! Configure the loopback interface for the Service Provider RP
interface loopback 0
 ip address 192.168.2.1 255.255.255.255
 ip pim sparse-mode
 ip pim rp-address 192.168.2.1 mcast-content-provider-groups override
 ip pim rp-address 192.168.0.254 mcast-service-provider-groups override
 ip access-list standard mcast-content-provider-groups permit 224.1.1.0 0.0.0.255
 ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
 ip access-list standard mcast-service-provider-groups permit 239.3.3.0 0.0.0.255
 !

! Configure the Vif1 virtual interface for multicast service reflection
interface Vif1
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
 ip service reflect Ethernet 0 destination 224.1.1.0 to 239.2.2.0 mask-len 24 source 10.1.1.2

 ip service reflect Ethernet 0 destination 224.1.1.0 to 239.3.3.0 mask-len 24 source 10.1.1.2

 ip igmp static-group 224.1.1.0
     ip igmp static-group 224.1.1.1
 ip igmp static-group 224.1.1.2
 ip igmp static-group 224.1.1.3
 ip igmp static-group 224.1.1.254
```

Enter these commands on the R2 router that is an anycast RP in the service provider network:

```
ip multicast-routing
interface <all IP numbered interfaces>
 ip pim sparse-mode
 no shutdown
interface loopback 0
 ip address 192.168.2.2 255.255.255.255
 ip pim sparse-mode
interface loopback 1
 description --- Anycast RP ---
 ip address 192.168.0.254 255.255.255.255
 ip pim sparse-mode
 ip msdp peer 192.168.2.3 connect-source Loopback0
 ip msdp originator-id Loopback0
 ip pim rp-address 192.168.0.254 mcast-service-provider-groups override
 ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
 ip access-list standard mcast-service-provider-groups permit 239.3.3.0 0.0.0.255
```

Enter these commands on the R4 router that is an anycast RP in the service provider network:

```
ip multicast-routing
```

```
interface <all IP numbered interfaces>
  ip pim sparse-mode
  no shutdown
  !
  interface loopback 0
  ip address 192.168.2.3 255.255.255.255
  ip pim sparse-mode
  interface loopback 1
  ip address 192.168.0.254 255.255.255.255
  ip pim sparse-mode
  !
ip pim rp-address 192.168.0.254 mcast-service-provider-groups override
ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
ip access-list standard mcast-service-provider-groups permit 239.3.3.0 0.0.0.255
!
ip msdp peer 192.168.2.2 connect-source Loopback0
ip msdp originator-id Loopback0
```

Enter these commands on the R3 and R5 routers in the service provider network:

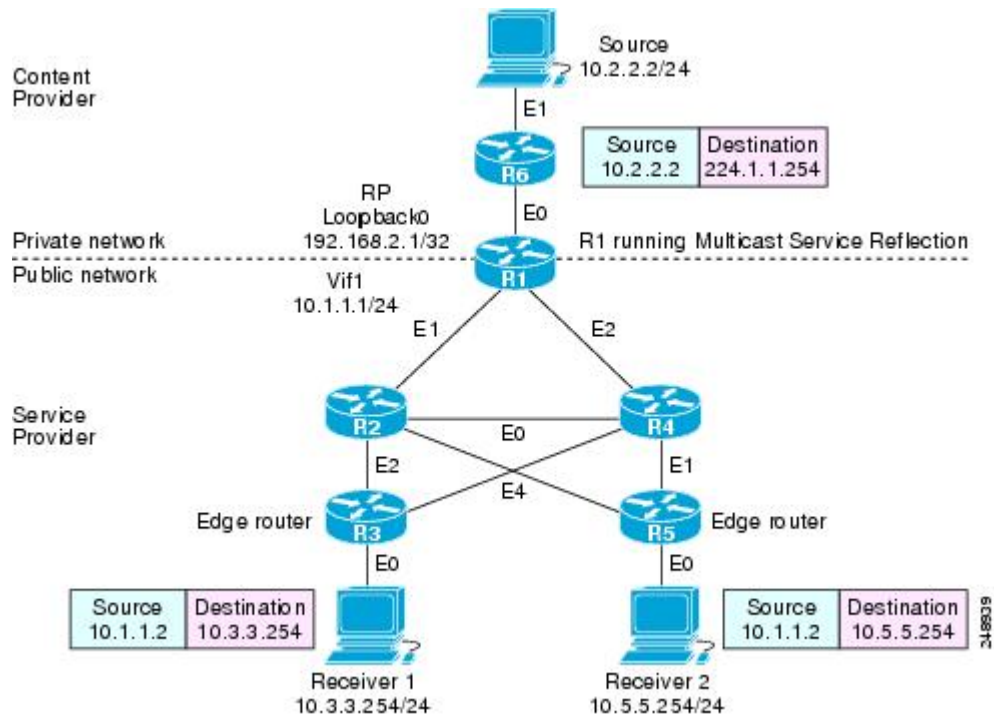
```
ip multicast-routing
  ip pim rp-address 192.168.0.254 mcast-service-provider-groups override
  ip access-list standard mcast-service-provider-groups permit 239.2.2.0 0.0.0.255
  permit 239.3.3.0 0.0.0.255
  !
```

Example Multicast-to-Unicast Destination Splitting

The following example shows how to implement multicast service reflection (multicast-to-unicast destination splitting where the multicast single stream is converted into two unique unicast streams) in a service provider network. Multicast-to-Unicast Destination Splitting allows service providers to translate externally received content provider multicast destination addresses to multiple unicast destination addresses that conform to the service provider's internal addressing policy.

This example uses the topology illustrated in the figure.

Figure 35: Multicast Service Reflection (Multicast-to-Unicast Destination Splitting) in a Service Provider Network Example Topology



In this example topology, a content provider is sending financial market information to a service provider, which in turn is sending that information to active receivers (brokerage houses). The service provider may be receiving market data from multiple content providers.

Router R1 is an edge router in the service provider's PIM domain.

Router R1 is acting as a RP for the 224.1.1.0/24 address range.

Router R1 has a Vif1 interface and is running the multicast service reflection application.

Routers R2, R3, R4 and R5 are not PIM enabled and are running unicast routing only in the service provider network.

Enter these commands on the router running the multicast service reflection application (R1):

```
configure terminal
 ip multicast-routing
 interface <all IP numbered interfaces>
 ip pim sparse-mode
 no shutdown
 !
 ! Configure the loopback interface for the Service Provider RP
 !
 interface loopback 0
 ip address 192.168.2.1 255.255.255.255
 ip pim sparse-mode
 !
 ip pim rp-address 192.168.2.1 mcast-content-provider-groups override
 ip access-list standard mcast-content-provider-groups permit 224.1.1.0 0.0.0.255
 !
 ! Configure the Vif1 virtual interface for multicast service reflection
```

```
!  
interface Vif1  
ip address 10.1.1.1 255.255.255.0  
ip pim sparse-mode  
ip service reflect Ethernet 0 destination 224.1.1.0 to 10.3.3.0 mask-len 24 source 10.1.1.2  
ip service reflect Ethernet 0 destination 224.1.1.0 to 10.5.5.0 mask-len 24 source 10.1.1.2  
  
ip igmp static-group 224.1.1.0  
ip igmp static-group 224.1.1.1  
ip igmp static-group 224.1.1.2  
ip igmp static-group 224.1.1.3  
.  
.  
ip igmp static-group 224.1.1.255  
!  
end
```




CHAPTER 17

Cellular Boot Time Improvements

- [Cellular Boot Time Improvements](#), on page 171

Cellular Boot Time Improvements

Numerous improvements have been made in the Cellular link up-time with IOS-XE release 17.9.1. In previous releases, the cellular interface was taking approximately two and a half minutes to come up and pass traffic after the router booted up. The Cellular link up-time has been improved by approximately 20% in this release.



CHAPTER 18

Cellular Pluggable Interface Module Configuration Guide

- [Cellular Pluggable Interface Module Configuration Guide](#), on page 173
- [Support for the P-5GS6-GL Pluggable Module on the ESR6300](#), on page 173
- [Galileo Support on the LTE Pluggable Modules](#), on page 173

Cellular Pluggable Interface Module Configuration Guide

The Cisco 4G LTE-Advanced Configuration chapter has been replaced by a new standalone guide called [Cellular Pluggable Interface Module Configuration Guide](#). This guide contains updated information on all aspects of using the Cisco Cellular PIM.



Important The Pluggable Module is not hot swappable. The router must be reloaded after a new module is installed.

Support for the P-5GS6-GL Pluggable Module on the ESR6300

Support for the P-5GS6-GL Pluggable Module works the same on the ESR6300 as it does on the other IoT Routers. For details, see [5G Sub-6 GHz Pluggable Interface Module](#) and [Cellular Pluggable Interface Module Configuration Guide](#).

Galileo Support on the LTE Pluggable Modules

With Cisco IOS XE 17.11.1a and earlier, the only GNSS constellation supported was GPS. This release introduces support for Galileo.



Note Only ONE constellation can be enabled at a time.

There are new CLI options available to support the new constellation:

Configuration Commands

```
config# controller cellular <slot/port>
(config-controller)# <no> lte gps constellation <gps | galileo | gnss >
```

Example:

```
(config-controller)#lte gps constellation ?
galileo  select Galileo as active constellation
gps      select GPS as active constellation
gnss     select multiple GNSS as active constellation
```



Note The default setting is gps mode.

The new galileo and gnss options in the above CLI are used to configure Galileo and Multiple/Simultaneous GNSS (GPS + Galileo etc) respectively.

If you disable the GPS configuration, ensure there is no constellation configured, consistent with GPS mode configuration. For example:

```
config# controller Cellular 0/1/0
(config-controller)# no lte gps constellation gps
```

Show Commands

The following example shows the current GNSS constellation as Galileo:

```
#show cellular 0/1/0 gps detail
GPS Feature = enabled
GPS Mode Configured = standalone
Current Constellation Configured = galileo | gps | gnss
GPS Port Selected = Dedicated GPS port
GPS Status = GPS acquiring
```

Any changes made to the configuration will require the router to be rebooted.

More information is available in the [Cellular Pluggable Interface Module Configuration Guide](#).



CHAPTER 19

Radio Aware Routing and Dynamic Link Exchange Protocol

This chapter contains the following sections:

- [Overview of Radio Aware Routing, on page 176](#)
- [Benefits of Radio Aware Routing, on page 177](#)
- [Restrictions and Limitations, on page 178](#)
- [Performance, on page 178](#)
- [System Components, on page 178](#)
- [Radio Aware Routing Topology, on page 179](#)
- [QoS Provisioning on PPPoE Extension Session, on page 182](#)
- [Example: Configuring the RAR Feature in Bypass Mode, on page 183](#)
- [Verifying RAR Session Details, on page 184](#)
- [Overview of DLEP, on page 190](#)
- [Configuring DLEP with OSPFv3, on page 192](#)
- [DLEP Configuration Modes, on page 196](#)
- [DLEP Configuration with GTSM, on page 202](#)
- [Configuring DLEP with OSPFv3, on page 202](#)
- [Configuring DLEP with EIGRP, on page 204](#)
- [DLEP with Quality of Service \(QoS\), on page 205](#)
- [Configuring DLEP on a Sub-Interface, on page 210](#)
- [Removing the DLEP Configuration, on page 212](#)
- [Configuring DLEP using the Web User Interface \(WebUI\), on page 213](#)
- [DLEP Validation Commands, on page 217](#)
- [Optional Configurations for DLEP, on page 219](#)
- [DLEP IPv6 Unicast, on page 220](#)
- [IPv4 and IPv6 Multicast Over DLEP, on page 221](#)
- [IPv6 Control Plane for DLEP, on page 222](#)
- [Clearing DLEP Clients and Neighbors, on page 222](#)
- [Troubleshooting with show commands, on page 223](#)
- [Troubleshooting with debug commands, on page 226](#)
- [Additional Debug Commands, on page 233](#)
- [SNMP MIB Support for DLEP, on page 234](#)
- [Related Documentation, on page 239](#)

Overview of Radio Aware Routing

Introduction

Relief workers, soldiers, public safety personnel, and others need the right information, in the right place, at the right time, wherever they are located. Mobile ad hoc networks are emerging to address these needs. The IETF request for comment, RFC RFC5578, defines a PPP-over-Ethernet (PPPoE) based mechanism for integrating IP routers and mobile radios in ad hoc networks, enabling faster convergence, more efficient route selection, and better performance for delaysensitive traffic.

Radio-Aware Routing (RAR) is a mechanism that uses radios to interact with the routing protocol OSPFv3/EIGRP to signal the appearance, disappearance, and link conditions of one-hop routing neighbors.

In large mobile networks, connections to the routing neighbors are often interrupted due to distance and radio obstructions. When these signals do not reach the routing protocols, protocol timers are used to update the status of a neighbor. Routing protocols have lengthy timers, which is not recommended in mobile networks.

The RAR feature is supported on the Cisco ESR6300 Embedded Series Router.

Mobile Ad Hoc Networking (MANET)

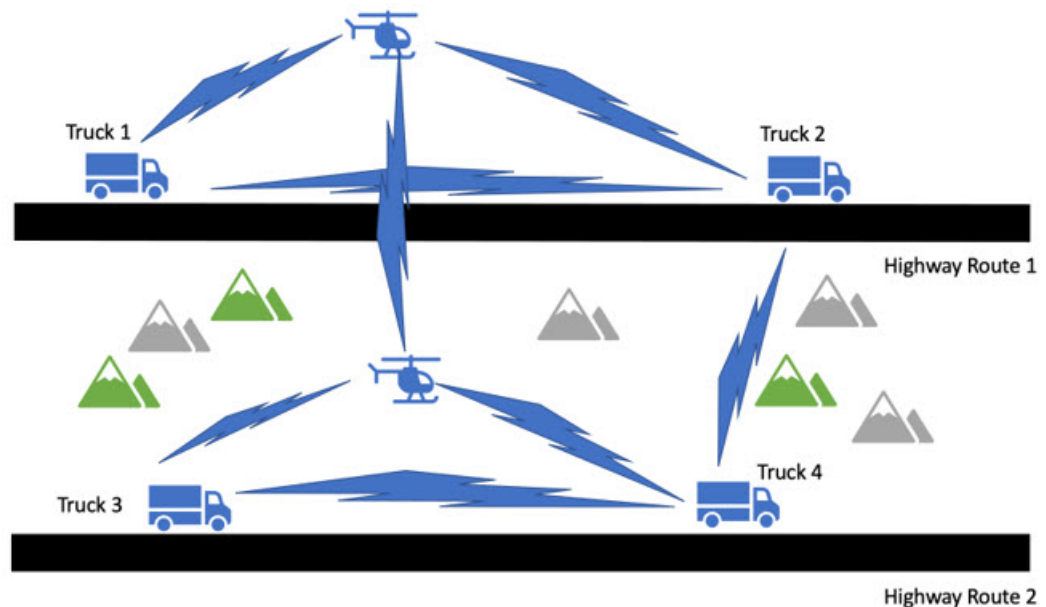
Mobile ad hoc networks are emerging as a means for delivering the benefits of IP networking to users operating beyond the reach of a fixed network. In ad hoc networks, mobile nodes associate on an extemporaneous or ad hoc basis. Ad hoc networks have numerous distinguishing characteristics when compared to conventional networking solutions:

- **Self-forming** — Nodes that come within radio range of each other can establish a network association without any pre-configuration or manual intervention.
- **Self-healing** — Nodes can join or leave rapidly without affecting operation of the remaining nodes.
- **No infrastructure** — In an ad hoc network, mobile nodes form their own network, and essentially become their own infrastructure.
- **Peer to peer** — Traditional networks typically support end systems operating in client-server mode. In an ad hoc network, mobile nodes can communicate and exchange information without prior arrangement and without reliance on centralized resources.
- **Predominantly wireless** — Historically networks have been mostly wired, and enhanced or extended through wireless access. The ad hoc environment is essentially wireless, but can be extended to support wired resources.
- **Highly dynamic** — Mobile nodes are in continuous motion and ad hoc networking topologies are constantly changing.

Collectively, these characteristics will enable ad hoc networks to deliver timely information to a new and underserved class of users. Ad hoc networking solutions can be applied to virtually any scenario that involves a cadre of highly mobile users or platforms (which may include stationary devices as well), a strong need to share IP-based information, and an environment in which fixed infrastructure is impractical, impaired, or impossible.

A Real-World Problem Description

Consider the following diagram:



The above network is a voice, video, data network between moving vehicles that consists of both ground and air vehicles, hence the network is mobile and it is a peer to peer mesh that changes as topographical obstructions are encountered. This is where we get the term mobile ad hock network or MANET for short.

In the scenario in the drawing, all 4 trucks always have connectivity with the helicopters that are flying over the same road. The two helicopters always have line of sight and will always have a connection between each other. The trucks may even be able to connect to the other helicopter or a truck on the opposite road when conditions are favorable.

Here we see that the path between trucks 1 and 3 are completely blocked. The path between Truck 2 and 4 is about to be blocked.

Our existing routing protocols such as OSPFv3 and EIGRP need to adjust its path metrics very quickly to maintain a cohesive operational network. The routing protocol also needs a way to get that information from the radios and that requires a radio to router protocol that is delivered by Cisco Radio Aware Routing in the form of two open protocols:

- PPP over Ethernet (PPPoE)
- Dynamic Link Exchange Protocol (DLEP)

Both protocols are discussed later in this document.

Benefits of Radio Aware Routing

The Radio Aware Routing feature offers the following benefits:

- Provides faster network convergence through immediate recognition of changes.
- Enables routing for failing or fading radio links.
- Allows easy routing between line-of-sight and non-line-of-sight paths.

- Provides faster convergence and optimal route selection so that delay-sensitive traffic, such as voice and video, is not disrupted
- Provides efficient radio resources and bandwidth usage.
- Reduces impact on the radio links by performing congestion control in the router.
- Allows route selection based on radio power conservation.
- Enables decoupling of the routing and radio functionalities.
- Provides simple Ethernet connection to RFC 5578 and DLEP compliant radios.

Restrictions and Limitations

The Radio Aware Routing and DLEP features have the following restrictions and limitations:

- Multicast traffic is not supported with DLEP, but is supported with PPPOE.
- DLEP does not support IPv6
- Cisco High Availability (HA) technology is not supported.
- Requires the Network Advantage license.



Note There is a condition that exists with DLEP that is not unique to the ESR6300. An ARP which has been learned on a VMI does not get deleted when the mapped physical interface goes down.



Note Previous releases of IOS XE offered support for IPv4 unicast traffic over an IPv4 DLEP session. IOS XE 17.12.1a provides support for IPv6 unicast, IPv4 multicast and IPv6 multicast over an IPv4 DLEP. See the [DLEP IPv6 Unicast, on page 220](#) section.

Performance

The Radio Aware Routing feature has the ability to support a maximum of 10 neighbors per radio or VMI interface, and a total of 30 to 40 neighbors.

System Components

The Radio Aware Routing (RAR) feature is implemented using the MANET (Mobile adhoc network) infrastructure comprising of different components such as PPPoE, Virtual multipoint interface (VMI), QoS, routing protocol interface and RAR protocols.

Point-to-Point Protocol over Ethernet PPPoE or PPPoE

PPPoE is a well-defined communication mechanism between the client and the server. In the RAR implementation, radio takes the role of the PPPoE client and router takes the role of the PPPoE server. This allows a loose coupling of radio and router, while providing a well-defined and predictable communication mechanism.

As PPPoE is a session or a connection oriented protocol, it extends the point-to-point radio frequency (RF) link from an external radio to an IOS router.

PPPoE Extensions

PPPoE extensions are used when the router communicates with the radio. In the Cisco IOS implementation of PPPoE, each individual session is represented by virtual access interface (connectivity to a radio neighbor) on which, QoS can be applied with these PPPoE extensions.

RFC5578 provides extensions to PPPoE to support credit-based flow control and session-based real time link metrics, which are very useful for connections with variable bandwidth and limited buffering capabilities (such as radio links).

Virtual Multipoint Interface (VMI)

Though PPPoE Extensions provides most of the setup to communicate between a router and a radio, VMI addresses the need to manage and translate events that higher layers (example, routing protocols) consume. In addition, VMI operates in the Bypass mode.

In Bypass mode, every Virtual Access Interface (VAI) representing a radio neighbor is exposed to routing protocols OSPFv3 and EIGRP, so that, the routing protocol directly communicates with the respective VAI for both unicast and multicast routing protocol traffic.



Note DLEP only supports aggregate mode. The preferred mode for PPPOE is bypass.

In Aggregate mode, VMI is exposed to the routing protocols (OSPF) so that the routing protocols can leverage VMI for their optimum efficiency. When the network neighbors are viewed as a collection of networks on a point-to-multipoint link with broadcast and multicast capability at VMI, VMI helps in aggregating the multiple virtual access interfaces created from PPPoE. VMI presents a single multi access layer 2 broadcast capable interface. The VMI layer re-directs unicast routing protocol traffic to the appropriate P2P link (Virtual-Access interface), and replicates any Multicast/Broadcast traffic that needs to flow. Since the routing protocol communicates to a single interface, the size of the topology database is reduced, without impacting the integrity of the network.

Radio Aware Routing Topology

This section provides a high level description on how RAR, MANETs, and PPPoE work together.

About MANETs

Mobile Ad Hoc Networks (MANETs) for device-to-radio communications address the challenges faced when merging IP routing and mobile radio communications in ad hoc networking applications.

Through the device-to-radio link, the radio can inform the device immediately when a node joins or leaves, and this enables the device to recognize topology changes more quickly than if it had to rely on timers. Without this link-status notification from the radio, the device would likely time out while waiting for traffic. The link-status notification from the radio enables the device to respond faster to network topology changes. Metric information regarding the quality of a link is passed between the device and radio, enabling the device to more intelligently decide on which link to use.

With the link-status signaling provided by the device-to-radio link, applications such as voice and video work better because outages caused by topology changes are reduced or eliminated. Sessions are more stable and remain active longer.

Cross-layer feedback for device-to-radio integration of Radio-Aware Routing (RAR) takes advantage of the functions defined in RFC 5578. The RFC 5578 is an Internet Engineering Task Force (IETF) standard that defines PPP over Ethernet (PPPoE) extensions for Ethernet-based communications between a device and a mobile radio, that operates in a variable-bandwidth environment and has limited buffering capabilities. These extensions provide a PPPoE session-based mechanism for sharing radio network status such as link-quality metrics and establishing flow control between a device and an RAR-compliant radio.

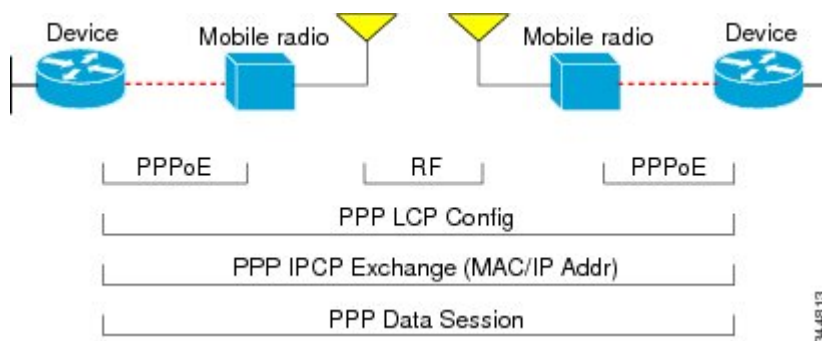
An RAR-compliant radio initiates a Layer 2 PPPoE session with its adjacent device on behalf of every device and radio neighbor discovered in the network. These Layer 2 sessions are the means by which radio network status for each neighbor link is reported to the device. The radio establishes the correspondence between each PPPoE session and each link to a neighbor.

PPPoE Interfaces for Mobile Radio Communications

The Mobile Ad Hoc Network (MANET) implementation uses PPP over Ethernet (PPPoE) sessions to enable intranodal communications between a device and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (device-to-device). This is duplicated each time a radio establishes a new radio link. The virtual multipoint interface (VMI) on the device can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Underneath the VMI are virtual access interfaces that are associated with each of the PPP and PPPoE connections.

A PPPoE session is established between a device and a radio on behalf of every other device and radio neighbor located in the MANET. These Layer 2 sessions are the means by which radio network status gets reported to the Layer 3 processes in the device. The figure below shows the PPPoE session exchange between mobile devices and directional radios in a MANET network.

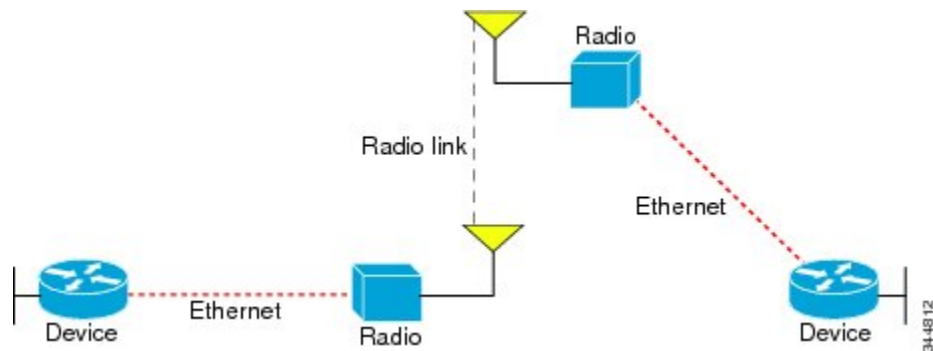
Figure 36: PPPoE Session Exchange Between Mobile Devices and Directional Radios



This capability requires that a Radio-Aware Routing (RAR)-compliant radio be connected to a device through Ethernet. The device always considers the Ethernet link to be up. If the radio side of the link goes down, the

device waits until a routing update timeout occurs to declare the route down and then updates the routing table. The figure below shows a simple device-to-radio link topology.

Figure 37: Device-to-Radio Link



Neighbor Up and Down Signaling

Mobile Ad Hoc Networks (MANETs) are highly dynamic environments. Nodes might move into, or out of, radio range at a fast pace. Each time a node joins or leaves, the network topology must be logically reconstructed by the devices. Routing protocols normally use timer-driven hello messages or neighbor timeouts to track topology changes, but MANETs reliance on these mechanisms can result in unacceptably slow convergence.

The neighbor up/down signaling capability provides faster network convergence by using link-status signals generated by the radio. The radio notifies the device each time a link to another neighbor is established or terminated by the creation and termination of PPP over Ethernet (PPPoE) sessions. In the device, the routing protocols (Open Shortest Path First version 3 [OSPFv3] or Enhanced Interior Gateway Routing Protocol [EIGRP]) respond immediately to these signals by expediting formation of a new adjacency (for a new neighbor) or tearing down an existing adjacency (if a neighbor is lost). For example, if a vehicle drives behind a building and loses its connection, the device immediately senses the loss and establishes a new route to the vehicle through neighbors that are not blocked. This high-speed network convergence is essential for minimizing dropped voice calls and disruptions to video sessions.

When virtual multipoint interfaces (VMIs) with PPPoE are used and a partner node has left or a new one has joined, the radio informs the device immediately of the topology change. Upon receiving the signal, the device immediately declares the change and updates the routing tables. The signaling capability provides these advantages:

- Reduces routing delays and prevents applications from timing out
- Enables network-based applications and information to be delivered reliably and quickly over directional radio links
- Provides faster convergence and optimal route selection so that delay-sensitive traffic such as voice and video are not disrupted
- Reduces impact on radio equipment by minimizing the need for internal queueing and buffering
- Provides consistent quality of service for networks with multiple radios

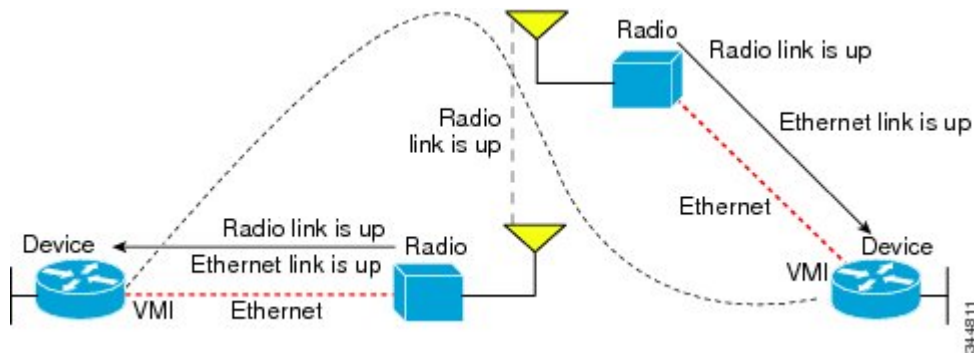
The messaging allows for flexible rerouting when necessary because of these factors:

- Fading of the radio links
- Congestion of the radio links

- Radio link power fade
- Utilization of the radio

The figure below shows the signaling sequence that occurs when radio links go up and down:

Figure 38: Up and Down Signaling Sequence



PPPoE Credit-based and Metric-based Scaling and Flow Control

Each radio initiates a PPP over Ethernet (PPPoE) session with its local device as soon as the radio establishes a link to another radio. Once the PPPoE sessions are active for each node, a PPP session is then established end-to-end (device-to-device). This process is duplicated each time a radio establishes a new link.

The carrying capacity of each radio link might vary due to location changes or environmental conditions, and many radio transmission systems have limited buffering capabilities. To minimize the need for packet queueing in the radio, PPPoE protocol extensions enable the device to control traffic buffering in congestion situations. Implementing flow-control on these device-to-radio sessions allows use of quality of service (QoS) features such as fair queueing.

The flow-control solution utilizes a credit-granting mechanism documented in RFC 5578. When the PPPoE session is established, the radio can request a flow-controlled session. If the device acknowledges the request, all subsequent traffic must be flow controlled. If a flow-control session is requested and cannot be supported by the device, the session is terminated. Typically, both the radio and the device initially grant credits during session discovery. Once a device exhausts its credits, it must stop sending until additional credits are granted. Credits can be added incrementally over the course of a session.

Metrics scaling is used with high-performance radios that require high-speed links. The radio can express the maximum and current data rates with different scaler values. Credit scaling allows a radio to change the default credit grant (or scaling factor) of 64 bytes to its default value. You can display the maximum and current data rates and the scalar value set by the radio in the `show vmi neighbor detail` command output.

QoS Provisioning on PPPoE Extension Session

The following example describes QoS provisioning on PPPoE extension session:

```
policy-map rar_policer
  class class-default
    police 10000 2000 1000 conform-action transmit exceed-action drop violate-action drop
policy-map rar_shaper
  class class-default
    shape average percent 1
```

```
interface Virtual-Template2
 ip address 92.92.2.1 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

Example: Configuring the RAR Feature in Bypass Mode

The following example is an end-to-end configuration of RAR in the bypass mode:



Note Before you begin the RAR configuration, you must first configure the **subscriber authorization enable** command to bring up the RAR session. Without enabling authorization, the Point-to-Point protocol does not recognize this as a RAR session and may not tag *manet_radio* in presentation of a PPPoE Active Discovery Initiate (PADI). By default, bypass mode does not appear in the configuration. It appears only if the mode is configured as bypass.

Configure a Service for RAR

```
policy-map type service rar-lab
 ppoe service manet_radio //note: Enter the ppoe service policy name as manet_radio
!
```

Configure Broadband

```
bba-group ppoe VMI2
 virtual-template 2
 service profile rar-lab
!
interface GigabitEthernet0/0/0
 description Connected to Client1
 negotiation auto
 ppoe enable group VMI2
!
```

Configuration in Bypass Mode

- IP Address Configured under Virtual-Template Explicitly

```
interface Virtual-Template2
 ip address 192.168.90.3 255.255.255.0
 no ip redirects
 peer default ip address pool PPPoEpool2
 ipv6 enable
 ospfv3 1 network manet
 ospfv3 1 ipv4 area 0
 ospfv3 1 ipv6 area 0
 no keepalive
 service-policy input rar_policer Or/And
 service-policy output rar_shaper
```

- VMI Unnumbered Configured under Virtual Template

```

interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper

```

Configure the Virtual Multipoint Interface in Bypass Mode

```

interface vmi2 //configure the virtual multi interface
ip address 192.168.2.1 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode bypass

```

Configure OSPF Routing

```

router ospfv3 1
router-id 1.1.1.1
!
address-family ipv4 unicast
redistribute connected metric 1 metric-type 1
log-adjacency-changes
exit-address-family
!
address-family ipv6 unicast
redistribute connected metric-type 1
log-adjacency-changes
exit-address-family
!
ip local pool PPPoEpool2 192.168.2.3 192.168.2.254

```

Verifying RAR Session Details

To retrieve RAR session details, use the following show commands:

```

Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
    1646 packets sent, 2439363 received
    176216 bytes sent, 117250290 received

PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 32928 PADG Timer index: 0
PADG last rcvd Seq Num: 17313
PADG last nonzero Seq Num: 17306

```

```

PADG last nonzero rcvd amount: 2
PADG Timers: (ms)  [0]-1000  [1]-2000  [2]-3000  [3]-4000  [4]-5000
PADG xmit: 33308  rcvd: 17313
PADG rcvd: 17313  rcvd: 19709
In-band credit pkt xmit: 7 rcvd: 2434422
Last credit packet snapshot
  PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
  PADG rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
  PADG xmit: seq_num = 17313, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 61, bcn = 65533
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
  PADQ xmit: 0  rcvd: 0

```

```

session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
  1389302 packets sent, 1852 received
  77869522 bytes sent, 142156 received

```

```

PPPoE Flow Control Stats
Local Credits: 65535  Peer Credits: 65535  Local Scaling Value 64 bytes
Credit Grant Threshold: 28000  Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 18787  PADG Timer index: 0
PADG last rcvd Seq Num: 18784
PADG last nonzero Seq Num: 18768
PADG last nonzero rcvd amount: 2
PADG Timers: (ms)  [0]-1000  [1]-2000  [2]-3000  [3]-4000  [4]-5000
PADG xmit: 18787  rcvd: 18784
PADG rcvd: 18784  rcvd: 18787
In-band credit pkt xmit: 1387764 rcvd: 956
Last credit packet snapshot
  PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
  PADG rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
  PADG xmit: seq_num = 18784, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 0, bcn = 64222
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
  PADQ xmit: 0  rcvd: 1

```

Router#**show pppoe session packets**

Total PPPoE sessions 2

SID	Pkts-In	Pkts-Out	Bytes-In	Bytes-Out
9	2439391	1651	117252098	176714
10	1858	1389306	142580	77869914

Router#**show vmi counters**

Interface vmi2: - Last Clear Time =

```

Input Counts:
  Process Enqueue  = 0 (VMI)
  Fastswitch      = 0
  VMI Punt Drop:
    Queue Full    = 0

```

Output Counts:

Transmit:

```

        VMI Process DQ =          4280
        Fastswitch VA  =           0
        Fastswitch VMI =           0
    Drops:
        Total          =           0
        QOS Error      =           0
        VMI State Error =           0
        Mcast NBR Error =           0
        Ucast NBR Error =           0
    Interface vmi3: - Last Clear Time =

    Input Counts:
        Process Enqueue =           0 (VMI)
        Fastswitch      =           0
    VMI Punt Drop:
        Queue Full     =           0

    Output Counts:
    Transmit:
        VMI Process DQ =          2956
        Fastswitch VA  =           0
        Fastswitch VMI =           0
    Drops:
        Total          =           0
        QOS Error      =           0
        VMI State Error =           0
        Mcast NBR Error =           0
        Ucast NBR Error =           0
    Interface vmi4: - Last Clear Time =

    Input Counts:
        Process Enqueue =           0 (VMI)
        Fastswitch      =           0
    VMI Punt Drop:
        Queue Full     =           0

    Output Counts:
    Transmit:
        VMI Process DQ =           0
        Fastswitch VA  =           0
        Fastswitch VMI =           0
    Drops:
        Total          =           0
        QOS Error      =           0
        VMI State Error =           0
        Mcast NBR Error =           0
        Ucast NBR Error =           0
    Router#

    Router#show vmi neighbor details
    1 vmi2 Neighbors
    1 vmi3 Neighbors
    0 vmi4 Neighbors
    2 Total Neighbors

    vmi2  IPV6 Address=FE80::21E:E6FF:FE43:F500
          IPV6 Global Addr:::
          IPV4 Address=92.92.2.2, Uptime=05:15:01
          Output pkts=89, Input pkts=0
          No Session Metrics have been received for this neighbor.
          Transport PPPoE, Session ID=9
          INTERFACE STATS:
            VMI Interface=vmi2,

```



```

    Input qcount=0, drops=0, Output qcount=0, drops=0
    V-Access intf=Virtual-Access2.1,
    Input qcount=0, drops=0, Output qcount=0, drops=0
    Physical intf=GigabitEthernet0/0/0,
    Input qcount=0, drops=0, Output qcount=0, drops=0

```

```

PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 33038 PADG Timer index: 0
PADG last rcvd Seq Num: 17423
PADG last nonzero Seq Num: 17420
PADG last nonzero rcvd amount: 2
PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000
PADG xmit: 33418 rcvd: 17423
PADG xmit: 17423 rcvd: 19819
In-band credit pkt xmit: 7 rcvd: 2434446
Last credit packet snapshot
PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
PADG rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
PADG xmit: seq_num = 17423, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 61, bcn = 65533
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 0

```

```

vmi3 IPV6 Address=FE80::21E:7AFF:FE68:6100
IPV6 Global Addr=:
IPV4 Address=91.91.91.4, Uptime=05:14:55
Output pkts=6, Input pkts=0
METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
CURRENT: MDR=128000 bps, CDR=128000 bps
Lat=0 ms, Res=100, RLQ=100, load=0
MDR Max=128000 bps, Min=128000 bps, Avg=128000 bps
CDR Max=128000 bps, Min=128000 bps, Avg=128000 bps
Latency Max=0, Min=0, Avg=0 (ms)
Resource Max=100%, Min=100%, Avg=100%
RLQ Max=100, Min=100, Avg=100
Load Max=0%, Min=0%, Avg=0%
Transport PPPoE, Session ID=10
INTERFACE STATS:
VMI Interface=vmi3,
Input qcount=0, drops=0, Output qcount=0, drops=0
V-Access intf=Virtual-Access2.2,
Input qcount=0, drops=0, Output qcount=0, drops=0
Physical intf=GigabitEthernet0/0/1,
Input qcount=0, drops=0, Output qcount=0, drops=0

```

```

PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 18896 PADG Timer index: 0
PADG last rcvd Seq Num: 18894
PADG last nonzero Seq Num: 18884
PADG last nonzero rcvd amount: 2
PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000
PADG xmit: 18896 rcvd: 18894
PADG xmit: 18894 rcvd: 18896
In-band credit pkt xmit: 1387764 rcvd: 961
Last credit packet snapshot

```

Verifying RAR Session Details

```

PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
PADC rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
PADC xmit: seq_num = 18894, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 0, bcn = 64222
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 1

```

```

Router#show vmi neighbor details vmi 2
      1 vmi2 Neighbors

```

```

vmi2  IPV6 Address=FE80::21E:E6FF:FE43:F500
      IPV6 Global Addr:::
      IPV4 Address=92.92.2.2, Uptime=05:16:03
      Output pkts=89, Input pkts=0
      No Session Metrics have been received for this neighbor.
      Transport PPPoE, Session ID=9
      INTERFACE STATS:
        VMI Interface=vmi2,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        V-Access intf=Virtual-Access2.1,
          Input qcount=0, drops=0, Output qcount=0, drops=0
        Physical intf=GigabitEthernet0/0/0,
          Input qcount=0, drops=0, Output qcount=0, drops=0

```

```

PPPoE Flow Control Stats
Local Credits: 65535 Peer Credits: 65535 Local Scaling Value 64 bytes
Credit Grant Threshold: 28000 Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 33100 PADG Timer index: 0
PADG last rcvd Seq Num: 17485
PADG last nonzero Seq Num: 17449
PADG last nonzero rcvd amount: 2
PADG Timers: (ms) [0]-1000 [1]-2000 [2]-3000 [3]-4000 [4]-5000
PADG xmit: 33480 rcvd: 17485
PADC xmit: 17485 rcvd: 19881
In-band credit pkt xmit: 7 rcvd: 2434460
Last credit packet snapshot
PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
PADC rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
PADC xmit: seq_num = 17485, fcn = 65535, bcn = 65535
In-band credit pkt xmit: fcn = 61, bcn = 65533
In-band credit pkt rcvd: fcn = 0, bcn = 65534
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 0

```

```

Router#show platform hardware qfp active feature ess session

```

```

Current number sessions: 2
Current number TC flow: 0
Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle
T=TC

```

Session	Type	Segment1	SegType1	Segment2	SegType2	Feature	Other
21	PPP	0x0000001500001022	PPPOE	0x0000001500002023	LTERM	-----	
24	PPP	0x0000001800003026	PPPOE	0x0000001800004027	LTERM	-----	

```

Router#show platform software subscriber pppoe_fctl evsi 21
PPPoE Flow Control Stats

```

```

Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
Credit Grant Threshold: 28000   Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 33215   PADG Timer index: 0
PADG last rcvd Seq Num: 17600
PADG last nonzero Seq Num: 17554
PADG last nonzero rcvd amount: 2
PADG Timers: (ms)   [0]-1000   [1]-2000   [2]-3000   [3]-4000   [4]-5000
PADG xmit: 33595   rcvd: 17600
PADG rcvd: 17600
PADG xmit: 17600   rcvd: 19996
In-band credit pkt xmit: 7 rcvd: 2434485
Last credit packet snapshot
  PADG xmit: seq_num = 33215, fcn = 0, bcn = 65535
  PADG rcvd: seq_num = 33215, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17600, fcn = 0, bcn = 65535
  PADG xmit: seq_num = 17600, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534

```

```

BQS buffer statistics
Current packets in BQS buffer: 0
Total en-queue packets: 0 de-queue packets: 0
Total dropped packets: 0

```

```
Internal flags: 0x0
```

```
Router#show platform hardware qfp active feature ess session id 21
Session ID: 21
```

```

EVSI type: PPP
SIP Segment ID: 0x1500001022
SIP Segment type: PPPOE
FSP Segment ID: 0x1500002023
FSP Segment type: LTERM
QFP if handle: 16
QFP interface name: EVSI21
SIP TX Seq num: 0
SIP RX Seq num: 0
FSP TX Seq num: 0
FSP RX Seq num: 0
Condition Debug: 0x00000000
  session

```

```
Router#show ospfv3 neighbor
```

```

OSPFv3 1 address-family ipv4 (router-id 3.3.3.3)

Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:01:32   19           Virtual-Access2.1

OSPFv3 1 address-family ipv6 (router-id 3.3.3.3)

Neighbor ID      Pri   State           Dead Time   Interface ID  Interface
1.1.1.1          0    FULL/ -         00:01:52   19           Virtual-Access2.1
Router#

```

```
Router#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

    90.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       90.90.90.0/24 is directly connected, Virtual-Access2.1
O       90.90.90.4/32 [110/1] via 90.90.90.4, 00:00:03, Virtual-Access2.1
L       90.90.90.5/32 is directly connected, Virtual-Access2.1
    92.0.0.0/32 is subnetted, 1 subnets
C       92.92.2.21 is directly connected, Virtual-Access2.1

```

Overview of DLEP

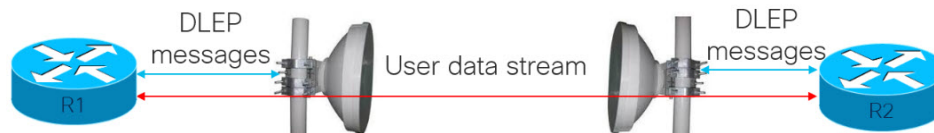
Cisco Dynamic Link Exchange Protocol (DLEP) is the latest protocol in the Radio Aware Routing (RAR) family. DLEP addresses the challenges faced when merging IP routing and radio frequency (RF) communications.

Cisco provides capabilities that enable:

- Optimal route selection based on feedback from radios
- Faster convergence when nodes join and leave the network
- Efficient integration of point-to-point, point-to-multipoint and broadcast multi-access radio topologies with multi-hop routing
- Flow-controlled communications between the radio and its partner router using rate-based Quality of Service (QoS) policies
- Dynamic shaping of fluctuating RF bandwidth in near real time to provide optimized use of actual RF bandwidth

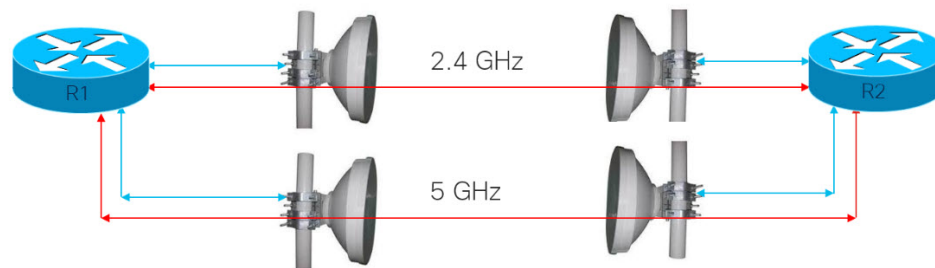
DLEP Topology and Packet Flow

The DLEP exchange between the router and radio allows the radio to tell the router about the link quality. This is somewhat analogous to the way the bar icon on your cell phone tells you about your Wi-Fi or LTE signal quality.



With DLEP, we can make use of routing distances with equal cost, where metrics are updated based in real time based on best path.

Without DLEP, there are two equal cost paths to any unadjusted routing protocol. With DLEP, routing metrics can be adjusted in real-time to favor the best path.



Note Atmospheric conditions and interference will ultimately favor one band versus the other.

DLEP Packet Flow

There are three different scenarios for packet flow:

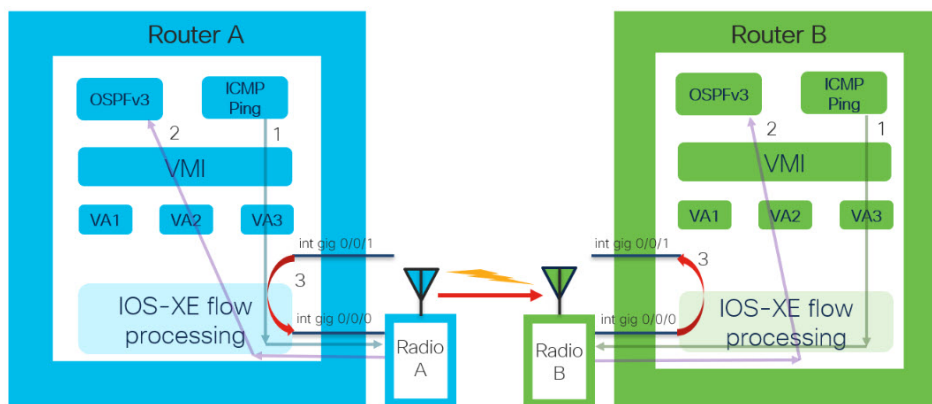
- Packet sent from IOS-XE to the DLEP neighbor (radio)
- Packet sent from DLEP neighbor (radio) to IOS-XE
- Non-DLEP traffic passing between the ESR-6300 Layer 3 (WAN) interfaces, for example, user traffic

Interfaces in IOS-XE Platform

- Virtual Multipoint Interface (VMI)
 - The VMI interface acts as an umbrella interface for all virtual access interfaces, which is used for routing protocols such as OSPFv3 and EIGRP.
 - Routing protocols, for example OSPFv3, see a single VMI interface instead of all VA interfaces. This helps reduce routing table size without impacting the integrity of network.
- Virtual Template (VT)
 - Virtual Template serves as the template for every Virtual Access interface.
- Virtual Access (VA) interface
 - One VA is created for each DLEP Neighbor (Radio) discovered.
- Underlying physical Layer 3 WAN interface (Gi 0/0/0 and Gi 0/0/1), or even sub-interface (Gi 0/0/0.2 or Gi0/0/1.2)

Packet Flow Diagram with Flow Types

The following diagram describes the packet flow:



Item	Description
1	Packet sent from IOS-XE to DLEP neighbor (to Radio): packet with DST MAC of neighbor MAC, neighbor IP sent out from DLEP Physical interface.
2	DLEP Packet (from radio) received thru DLEP Physical interface to IOS-XE: packet needs to be delivered to IOS routing protocol marked as from VMI interface.
3	End to End user data.

License Requirements

The Cisco Dynamic Link Exchange Protocol (DLEP) feature requires the Network Advantage license.

Configuring DLEP with OSPFv3

This section provides the following major sections for initiating, verifying, and managing all aspects of Dynamic Link Exchange Protocol (DLEP) on an interface. DLEP uses following interfaces that need to be configured:

- Physical interface
- VMI interface
- Virtual Templates



Important Before attaching a Virtual-Template to a physical interface, you need to configure the VMI and Virtual-Template. See the following example of the error you receive:

```
Router(config)#int gi0/0/0
Router(config-if)#ip dlep vtemplate 1
DLEP: ERROR. A valid VMI and Virtual Template MUST be present before configuring ip dlep
DLEP: ERROR. An Interface IP address MUST be specified for DLEP.
```

Configuring the Virtual Multipoint Interface

By default, virtual multipoint interfaces (VMIs) operate in aggregate mode, which means that all the virtual access interfaces created by DLEP sessions are aggregated logically under the configured VMI. Applications above Layer 2, such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First version 3 (OSPFv3), should be defined only on the VMI. Packets sent to the VMI are forwarded to the correct virtual access interface.

To configure the VMI, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable Router#</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 Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	Enters global configuration mode.
Step 3	interface vmi <i>number</i> Example: <pre>Router(config)# interface vmi 1 Router(config-if)#</pre>	Creates a VMI and enters interface configuration mode. This example creates VMI1.
Step 4	ip unnumbered <i>interface</i> Example: <pre>Router(config-if)# ip unnumbered gigabitEthernet {0/0/0 or 0/0/1 or 0/0/0.2}</pre>	Tells the VMI interface to use the physical interface IP address.
Step 5	physical-interface <i>interface</i> Example: <pre>Router(config-if)# physical-interface gigabitEthernet {0/0/0 or 0/0/1 or 0/0/0.2}</pre>	Binding physical interface to VMI interface, for packet flow.
Step 6	ipv6 enable Example: <pre>Router(config-if)# ipv6 enable</pre>	Enable ipv6 support under VMI interface. OSPFv3 IPv4 needs to have ipv6 support enabled on the interface level.

	Command or Action	Purpose
Step 7	Configure routing protocols. Example: Router (config-if) # ospfv3 1 ipv4 area 0	Enable VMI interface to participate in OSPFv3 or EIGRP routing.
Step 8	exit Example: Router (config-if) # exit Router (config) #	Exits the current mode.
Step 9	router ospfv3 1 Example: Router (config) # router ospfv3 1	Global configuration for OSPFv3
Step 10	address-family ipv4 unicast Example: Router (config-router) # address-family ipv4 unicast Router (config-router-af) #	Adding address family for IPv4 unicast routing under global OSPFv3 configuration.

Configuring the Virtual Template

DLEP configuration requires virtual template to be defined. Perform this task to create the DLEP virtual template:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router (config) #	Enters global configuration mode.
Step 3	interface Virtual-Template number Example: Router (config) # interface Virtual-Template 1 Router (config-if) #	Creates Virtual-Template interface and enters interface configuration mode. Note You need to use the same virtual-template interface for configuring DLEP on physical interface.

	Command or Action	Purpose
Step 4	ip unnumbered <i>interface</i> Example: <pre>Router(config-if)#ip unnumbered gigabitEthernet {0/0/0 or 0/0/1 or 0/0/0.2}</pre>	Tells the Virtual-Template interface to use the physical interface IP address.
Step 5	ipv6 enable Example: <pre>Router(config-if)# ipv6 enable Router(config)#</pre>	Enable ipv6 support under Virtual-Template interface. OSPFv3 IPv4 needs to have ipv6 support enabled on interface level.
Step 6	exit Example: <pre>Router(config-if)# exit Router(config)#</pre>	Exits the current mode.

Configuring the Physical Interface

DLEP configuration is currently supported on the WAN interface of IOS-XE platforms. As described above, you need to configure both the VMI and Virtual-Template interface before configuring the physical interface. There are various ways that DLEP configuration can be attached to WAN interface, here are some of the examples:

1. DLEP template with well-known ip address [**Recommended**]
2. DLEP template with TCP/UDP port based between server (Router) and client (Radio)
3. DLEP template with dynamic port on server (Router)
4. DLEP template attach in discovery mode

For each of the four modes mentioned above, the user also has the option to enable Generalized TTL Security Mechanism (GTSM).

To configure DLEP on an interface, perform the following procedure:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable Router#</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	
Step 3	<pre>interface <i>gi0/0/0 or gi0/0/1</i> Example: Router(config)# interface gigabitEthernet 0/0/0 Router(config-if)#</pre>	Enters interface configuration mode.
Step 4	<pre>ipv6 enable Example: Router(config-if)#ipv6 enable</pre>	Enable ipv6 support under interface level.
Step 5	<pre>Assigning IP address to physical interface Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0</pre>	Assign physical IP address to the WAN interface.
Step 6	<pre>ip dlep vtemplate <i>port number</i> Example: Router(config-if)#ip dlep vtemplate number 1</pre>	<p>Attaches DLEP Template to WAN interface, for discovery mode. Other configuration examples mentioned separately.</p> <p>Note Before attaching a DLEP template to a WAN interface, you need to configure a physical ip address, and create VMI and virtual templates.</p>
Step 7	<pre>no shutdown Example: Router(config-if)# no shutdown</pre>	Bring up the interface.
Step 8	<pre>exit Example: Router(config-if)# exit Router(config)#</pre>	Exits the current mode.

DLEP Configuration Modes

As mentioned in the previous section, DLEP virtual templates can be attached in different modes to the WAN or sub-interface of the router.



Note You must have VMI and Virtual-Templates already configured prior to continuing with any of the configuration modes in this section.

Configure DLEP Client/Server Based On Port Number

In this example, you are configuring the DLEP server, and client UDP and TCP ports.

Command or Action	Purpose
<pre>Router(config)#interface gi0/0/0 Router(config-if)# ip address 10.0.0.1 255.255.255.0 Router(config-if)# ipv6 enable Router(config-if)# ip dlep vtemplate 1 port 11113 tcp port 11114 client ip 10.0.0.3 port 11115 Router(config-if)# no shutdown</pre>	DLEP configuration where server (router) is listening to UDP port 11113 and TCP port 11114. Whereas client (radio) listening to TCP port 11115. UDP port of client is by default on 854.

Validate the above configuration using the **show dlep clients** command.

```
Router# show dlep clients
DLEP Clients for all interfaces:

DLEP Clients for Interface GigabitEthernet0/0/0
DLEP Server IP=10.0.0.1:11113 Sock=0

DLEP Client IP=10.0.0.3:11115 TCP Socket fd=1
Peer ID=1, Virtual template=1
Description: DLEP-Radiol-Path-1
Peer Timers (all values in milliseconds):
Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps
```

Configure DLEP with Dynamic Port on Server (Router)

In this example, you are configuring the DLEP server, and client UDP and TCP ports.

Command or Action	Purpose
<pre>Router(config)#interface gi0/0/0 Router(config-if)# ip address 10.0.0.1 255.255.255.0 Router(config-if)# ipv6 enable Router(config-if)# ip dlep vtemplate 1 client ip 10.0.0.3 port 11115 Router(config-if)# no shutdown</pre>	DLEP configuration where server (router) is listening to default UDP/TCP ports. Whereas client (radio) is listening to TCP port 11115. UDP port of client is by default on 854.

Validate the above configuration using the **show dlep clients** and **show dlep counters** commands.

```
Router# show dlep clients
DLEP Clients for all interfaces:
```

Configure DLEP with Dynamic Port on Server (Router)

```

DLEP Clients for Interface GigabitEthernet0/0/0
DLEP Server IP=10.0.0.1:55555 Sock=0

DLEP Client IP=10.0.0.3:11115 TCP Socket fd=1
Peer ID=1, Virtual template=1
Description: DLEP-Radiol-Path-1
Peer Timers (all values in milliseconds):
Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps

Router# show dlep counters
DLEP Counters for GigabitEthernet0/0/0

Last Clear Time =

DLEP Version = RFC 8175
DLEP Server IP=10.0.0.1:55555
DLEPv5 TCP Port = 55556

Peer Counters:
RX Peer Discovery      0      TX Peer Offer          0
RX Peer Offer         0      TX Peer Discovery      0
RX Peer Init          0      TX Peer Init Ack       0
RX Peer Init Ack      1      TX Peer Init           1
RX Heartbeat          58     TX Heartbeat           58
RX Peer Terminate     0      TX Peer Terminate Ack  0
RX Peer Terminate Ack 0      TX Peer Terminate     0

Neighbor Counters:
RX Neighbor Up        0      TX Neighbor Up Ack     0
RX Metric             0
RX Neighbor Down      0      TX Neighbor Down Ack   0
RX Neighbor Down Ack  0      TX Neighbor Down       0

Exception Counters:
RX Invalid Message    0      RX Unknown Message     0
Pre-Existing Neighbor 0      Neighbor Resource Error 0
Neighbor Not Found    0      Neighbor Msg Peer Not Up 0

Timer Counters:
Peer Heartbeat Timer   58
Peer Terminate Ack Timer 0
Neighbor Terminate Ack Timer 0
Neighbor Activity Timer 0
Radio Connect Timer    5

Single Timer Wheel "Manet Infra Wheel"
Granularity      = 250 msec
Wheel size       = 4096
Spoke index      = 3592
Tick count       = 3592
Flags            = 0x00

```

```

Active timers      = 1
High water mark   = 2
Started timers    = 164
Restarted timers  = 2
Cancelled timers   = 3
Expired timers    = 158
Long timers       = 0
Long timer revs   = 0
Timer suspends    = 0

```

Attach DLEP Template in Discovery Mode

When in discovery mode, the DLEP server will send out Peer Discovery signals, and wait for a Peer Offer signal from the radio.

Command or Action	Purpose
<pre> Router(config)#interface gi0/0/0 Router(config-if)# ip address 10.0.0.1 255.255.255.0 Router(config-if)# ipv6 enable Router(config-if)# ip dlep vtemplate 1 Router(config-if)# no shutdown </pre>	<p>DLEP configuration where server (router) is listening to default UDP/TCP ports.</p> <p>Note To receive the peer discovery messages, on client need to explicitly configure UDP port on client to 55555.</p>

Validate the above configuration using the **show dlep clients** and **show dlep counters** commands.

```

Router# show dlep clients
DLEP Clients for all interfaces:

DLEP Clients for Interface GigabitEthernet0/0/0
DLEP Server IP=10.0.0.1:55555 Sock=0

DLEP Client IP=10.0.0.3:11115 TCP Socket fd=1
Peer ID=1, Virtual template=1
Description: DLEP-Radiol-Path-1
Peer Timers (all values in milliseconds):
  Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps

Router# show dlep counters
DLEP Counters for GigabitEthernet0/0/0

Last Clear Time =

DLEP Version = RFC 8175
DLEP Server IP=10.0.0.1:55555
DLEPv5 TCP Port = 55556

Peer Counters:
RX Peer Discovery      0          TX Peer Offer          0

```

```

RX Peer Offer          3      TX Peer Discovery      194
RX Peer Init          0      TX Peer Init Ack      0
RX Peer Init Ack      3      TX Peer Init          3
RX Heartbeat         710     TX Heartbeat          707
RX Peer Terminate     0      TX Peer Terminate Ack 0
RX Peer Terminate Ack 0      TX Peer Terminate     2

Neighbor Counters:
RX Neighbor Up        0      TX Neighbor Up Ack    0
RX Metric             0
RX Neighbor Down      0      TX Neighbor Down Ack  0
RX Neighbor Down Ack  0      TX Neighbor Down      0

Exception Counters:
RX Invalid Message    0      RX Unknown Message    0
Pre-Existing Neighbor 0      Neighbor Resource Error 0
Neighbor Not Found    0      Neighbor Msg Peer Not Up 0

Timer Counters:
Peer Heartbeat Timer      709
Peer Terminate Ack Timer  2
Neighbor Terminate Ack Timer 0
Neighbor Activity Timer   0
Radio Connect Timer       3

Single Timer Wheel "Manet Infra Wheel"
Granularity      = 250 msec
Wheel size       = 4096
Spoke index      = 8
Tick count       = 24584
Flags            = 0x00
Active timers    = 1
High water mark  = 2
Started timers   = 1209
Restarted timers = 4
Cancelled timers = 14
Expired timers   = 1190
Long timers      = 0
Long timer revs  = 0
Timer suspends   = 0

```

Using a DLEP Template with a Well-Known IP Address

DLEP works based on RFC 8175, and it will use well-known ip address 224.0.0.117 on the server to communicate with radios. There are some additional pre-requisites that need to be enabled to make it work.

Procedure

	Command or Action	Purpose
Step 1	ip multicast-routing distributed Example: ip multicast-routing distributed	Enable multicast routing on Router
Step 2	interface interface Example:	Configure IPv4 address of the Server.

	Command or Action	Purpose
	<pre>Router(config)# interface gi0/0/0 Router(config-if)# ip address 10.1.2.3 255.255.255.0 Router(config-if)# ipv6 enable Router(config-if)# no shutdown</pre>	
Step 3	<p>ip pim sparse-dense-mode</p> <p>Example:</p> <pre>Router(config-if)# ip pim sparse-dense-mode</pre>	Enable sparse-dense mode.
Step 4	<p>Configure forwarding</p> <p>Example:</p> <pre>Router(config-if)# ip mfib cef in Router(config-if)# ip mfib cef out Router(config-if)# ip mfib forwarding in Router(config-if)# ip mfib forwarding out</pre>	Enable the router to forward multicast traffic.
Step 5	<p>ip dlep vtemplate <Number> well-known ip <ip-address></p> <p>Example:</p> <pre>Router(config-if)# ip dlep vtemplate 1 well-known ip 224.0.0.117</pre>	<p>Enable DLEP vTemplate to listen to multi-cast traffic.</p> <p>Note Under the command show running-configuration the output will display as “ip dlep vtemplate 1” which means “well-known ip 224.0.0.117” is hidden</p>

What to do next

Validate the above configuration using the **show dlep clients** command.

```
Router# show dlep clients
```

```
DLEP Clients for all interfaces:
DLEP Clients for Interface GigabitEthernet0/0/0
DLEP Server IP=10.1.2.3:55555 Sock=2

DLEP Client IP=10.1.2.4:854 TCP Socket fd=3
Peer ID=1, Virtual template=1
Description: OONF DLEP Radio
Peer Timers (all values in milliseconds):
  Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link Latency Metric : 1000 microseconds
Link CDR RX Metric : 104857600 bps
Link CDR TX Metric : 104857600 bps
Link MDR RX Metric : 104857600 bps
Link MDR TX Metric : 104857600 bps
```

DLEP Configuration with GTSM

Generalized TTL Security Mechanism (GTSM) can be used to provide an additional layer of security for the DLEP session.

The following table describes the different configuration modes:

DLEP Configuration Mode	Command to attach DLEP template under WAN or sub-interface
DLEP template with TCP/UDP port based between server and client.	Router(config)# interface gi0/0/0 Router(config-if)# ip dlep vtemplate 1 port 11113 tcp port 11114 gtsm client ip 10.0.0.3 port 11115
DLEP configuration with dynamic port on server.	Router(config)# interface gi0/0/0 Router(config-if)# ip dlep vtemplate 1 gtsm client ip 10.0.0.3 port 11115
DLEP template attach in discovery mode.	Router(config)# interface gi0/0/0 Router(config-if)# ip dlep vtemplate 1 gtsm
DLEP template with well-known ip address.	Router(config)# interface gi0/0/0 Router(config-if)# ip dlep vtemplate 1 gtsm well-known ip 224.0.0.117

Configuring DLEP with OSPFv3

This section describes configuring DLEP using OSPFv3.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enable privileged EXEC mode.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enter global configuration mode.
Step 3	ipv6 unicast-routing Example: Router(config)# ipv6 unicast-routing Router(config-if)#	Enable ipv6 unicast routing. OSPFv3 IPv4 needs to have ipv6 support enabled on the interface level.
Step 4	interface vmi number Example:	Creates VMI interface and enters interface configuration mode.

	Command or Action	Purpose
	Router# interface vmi 1 Router(config-if)#	
Step 5	ip unnumbered interface Example: Router(config-if)# ip unnumbered gigabitEthernet 0/0/0 or 0/0/1 or 0/0/0.2	Specifies VMI interface to use physical interface IP address.
Step 6	physical-interface interface Example: Router(config-if)# physical-interface gigabitEthernet 0/0/0 or 0/0/1 or 0/0/0.2	Binding physical interface to VMI interface, for packet flow.
Step 7	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable ipv6 support under VMI interface. OSPFv3 IPv4 needs to have ipv6 support enabled on the interface level.
Step 8	Configuring Routing Protocols Example: Router(config-if)# ospfv3 1 ipv4 area 0	Enable VMI interface to participate in OSPFv3 or EIGRP routing. This example is for OSPFv3. Note DLEP works only with OSPFv3 or EIGRP.
Step 9	exit Example: Router(config-if)# exit Router(config)#	Exits the current mode.
Step 10	interface virtual-template number Example: Router(config)# interface Virtual-Template 1 Router(config-if)#	Creates Virtual-Template interface and enters interface configuration mode Note Need to use same virtual-template interface for attaching on physical-interface
Step 11	ip unnumbered interface Example: Router(config-if)# ip unnumbered gigabitEthernet 0/0/0 or 0/0/1 or 0/0/0.2	Specifies Virtual-Template interface to use physical interface IP address.
Step 12	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable ipv6 support under Virtual-Template interface. OSPFv3 IPv4 needs to have ipv6 support enabled on interface level.
Step 13	exit Example: Router(config-if)# exit Router(config)#	Exits the current mode.
Step 14	interface gi0/0/0 or gi0/0/1 Example:	Enter configuration mode for interface.

	Command or Action	Purpose
	Router(config)# interface gi0/0/0 Router(config-if)#	
Step 15	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable ipv6 support under interface level. OSPFv3 IPv4 needs to have ipv6 support enabled on the interface level.
Step 16	Assigning IP address to physical interface Example: Router(config-if)# ip address 12.0.0.1	Assign physical IP address to WAN interface.
Step 17	ip dlep vtemplate <i>number</i> Example: Router(config-if)# ip dlep vtemplate 1 port 11117 tcp port 11115 client ip 12.0.0.2 port 859	Attaching DLEP Template to WAN interface.
Step 18	no shutdown Example: Router(config-if)# no shutdown	Bring up the interface.
Step 19	exit Example: Router(config-if)# exit Router(config)#	Exits the current mode.

Configuring DLEP with EIGRP

This section describes configuring DLEP using EIGRP.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enable privileged EXEC mode.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enter global configuration mode.
Step 3	interface vmi <i>number</i> Example:	Creates VMI interface and enters interface configuration mode.

	Command or Action	Purpose
	Router(config)# interface vmi 1 Router(config-if)#	
Step 4	ip unnumbered interface Example: Router(config-if)# ip unnumbered gigabitEthernet 0/0/0 or 0/0/1 or 0/0/0.2	Tells VMI interface to use physical interface IP address.
Step 5	physical-interface interface Example: Router(config-if)# physical-interface gigabitEthernet 0/0/0 or 0/0/1 or 0/0/0.2	Binding physical interface to VMI interface, for packet flow.
Step 6	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable ipv6 support under VMI interface. OSPFv3 IPv4 needs to have ipv6 support enabled on interface level.
Step 7	no ip split-horizon eigrp number Example: Router(config-if)# no ip split-horizon eigrp 1	Disable routing loops with EIGRP process.
Step 8	exit Example: Router(config-if)# exit Router(config)#	Exits the current mode.
Step 9	router eigrp <AS-NO> Example: Router(config)# router eigrp 1 Router(config-router)# router-id 1.1.1.1 Router(config-router)# network 10.0.0.0 0.0.0.255	Enable global configuration for EIGRP. Enable all the networks that can be part of EIGRP.

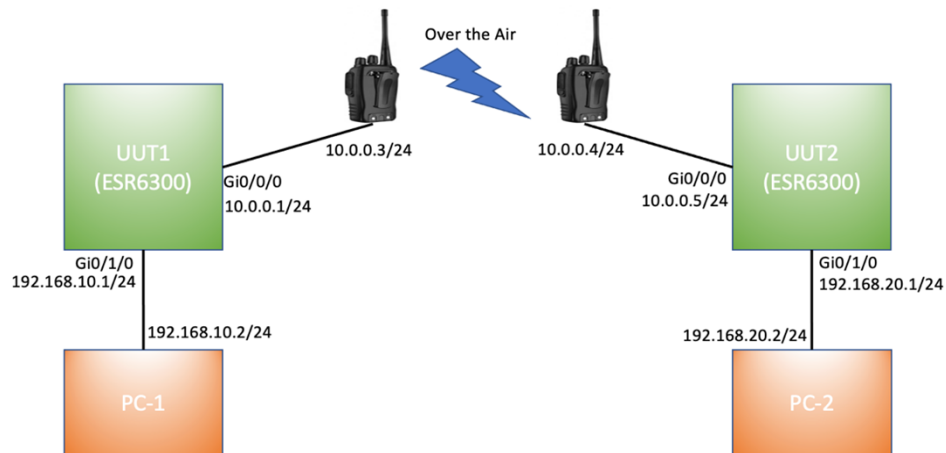
DLEP with Quality of Service (QoS)

Quality of Service (QoS) for DLEP needs to be configured on the Virtual-Template which is associated with the physical interface. QoS policy can be verified using the command **sh policy-map interface Virtual-Access**, as the actual data packets for DLEP will flow through the Virtual Access interfaces that will be created when DLEP neighbors come up.

Before proceeding, it is a good idea to familiarize yourself with content in the [Quality of Service \(QoS\) Configuration Guide for IOS-XE](#).

DLEP QoS Example

The following figure shows an example topology for DLEP with QoS.



Based on above figure, the QoS policy is applied to egress of Virtual-Template attached to WAN interface Gi0/0/0.

UUT1 Running Configuration

```

UUT1# show running-config
Building configuration...

Current configuration : 7773 bytes
!
!
version 17.8
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname UUT1
!
boot-start-marker
boot system bootflash:/c6300-universalk9.SSA.bin
!
ipv6 unicast-routing
!
class-map match-any CMAP_VIDEO
  match dscp 33
  match dscp 35
  match dscp 37
  match dscp 39
  match dscp af41
class-map match-any CMAP_VOICE
  match dscp 41
  match dscp 43
  match dscp 45
  match dscp 47
  match dscp 49
class-map match-any CMAP_DATA
  match dscp 9
  match dscp 11
  match dscp 13
  match dscp 15
  match dscp af11
!

```

```
policy-map Queue_Map
  class CMAP_VOICE
    bandwidth percent 40
    set dscp af11
  class CMAP_VIDEO
    bandwidth percent 50
  class CMAP_DATA
    bandwidth percent 10
    set dscp af23
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.255
  ipv6 enable
  ospfv3 1 ipv4 area 0
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.255.255.0
  ip dlep vtemplate 1 port 11113 tcp port 11114 client ip 10.0.0.3 port 11115
  negotiation auto
  ipv6 address 1000::1/64
  ipv6 enable
!
interface GigabitEthernet0/0/1
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/1/0
  switchport access vlan 30
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface Virtual-Template1
  ip unnumbered GigabitEthernet0/0/0
  ipv6 enable
  service-policy output Queue_Map
!
interface Vlan1
  no ip address
!
interface Vlan30
  ip address 192.168.10.1 255.255.255.0
  ipv6 address 1010::1/64
  ipv6 enable
  ospfv3 1 ipv6 area 0
!
interface Async0/2/0
  no ip address
  encapsulation scada
!
interface vm11
  ip unnumbered GigabitEthernet0/0/0
  ipv6 address FE80::7E31:EFF:FE85:1E78 link-local
  ipv6 enable
  ospfv3 1 ipv4 area 0
  physical-interface GigabitEthernet0/0/0
!
router ospfv3 1
!
  router-id 1.1.1.1
```

```

address-family ipv4 unicast
exit-address-family
!
end
UUT1#

```

Validation for DLEP QoS

For the above example, where QoS policy is applied to Virtual-Template1, data packets are flowing through Virtual-Access2 interface which is created when DLEP neighbors came up.



Note The CLI `show policy-map interface Virtual-Template1` will not show the stats.

```

UUT1#show policy-map interface Virtual-Template 1
Virtual-Template1

```

```

Service-policy output: Queue_Map

```

Service policy content is displayed for cloned interfaces only such as virtual access and sessions.

See the output for Virtual-Access 2:

```

UUT1#show policy-map interface Virtual-Access 2
Virtual-Access2

```

```

Service-policy output: Queue_Map

```

```

Class-map: CMAP_VOICE (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
Match: dscp 41
Match: dscp 43
Match: dscp 45
Match: dscp 47
Match: dscp 49
Queueing
queue limit 208 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 40% (400000 kbps)
QoS Set
  dscp af11
  Marker statistics: Disabled

Class-map: CMAP_VIDEO (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
Match: dscp 33
Match: dscp 35
Match: dscp 37
Match: dscp 39
Match: dscp af41 (34)
Queueing
queue limit 208 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
bandwidth 50% (500000 kbps)

Class-map: CMAP_DATA (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
Match: dscp 9

```

```

Match: dscp 11
Match: dscp 13
Match: dscp 15
Match: dscp af11 (10)
Queueing
queue limit 208 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 1024337/34827458
bandwidth 10% (100000 kbps)
QoS Set
  dscp af23
  Marker statistics: Disabled

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any

queue limit 208 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0

```

Edit the Virtual-Template

Before you begin

To edit the Virtual-Template, you need to remove the configuration for **ip dlep vtemplate** on the WAN interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enable privileged EXEC mode.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enter global configuration mode.
Step 3	interface Virtual-Template <i>number</i> Example: Router(config)# interface Virtual-Template 1 Router(config-if)#	Creates VMI interface and enters interface configuration mode.
Step 4	Service-policy [input/output] <Policy-map> Example: Router(config-if)# service-policy output Queue_Map	Apply policy-map to Egress/Ingress interface of Virtual-Template.

Configuring DLEP on a Sub-Interface

DLEP can also be configured on a sub-interface. The following is an example:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enable privileged EXEC mode.
Step 2	configure terminal Example: Router# configure terminal Router (config)#	Enter global configuration mode.
Step 3	interface interface Example: Router (config)# interface gi0/0/0 Router (config-int)# no shut	WAN interface should be in active state.
Step 4	interface sub-interface Example: Router (config-if)# interface gi0/0/0.2	Creating sub-interface gi0/0/0.2
Step 5	Encapsulation dot1q <VLAN> native Example: Router (config-subif)# encapsulation dot1q 2 native	Adding encapsulation dot1q over VLAN 2, and making it native.
Step 6	ip address <IP> <SUBNET> Example: Router (config-subif)# ip address 10.0.0.1 255.255.255.0	Adding IPv4 address for sub-interface.
Step 7	ipv6 enable Example: Router (config-subif)# ipv6 enable	Adding IPv4 address for sub-interface. OSPFv3 IPv4 needs to have ipv6 support enabled on the interface level.
Step 8	interface vmi number Example: Router (config-subif)# interface vmi 1 Router (config-if)#	Creates VMI interface and enters interface configuration mode.
Step 9	ip unnumbered interface Example:	Specifies VMI interface to use physical interface IP address.

	Command or Action	Purpose
	Router(config-if)# ip unnumbered gigabitEthernet 0/0/0.2	
Step 10	physical-interface <i>interface</i> Example: Router(config-if)# physical-interface gigabitEthernet 0/0/0.2	Binding physical interface to VMI interface, for packet flow.
Step 11	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable ipv6 support under VMI interface. OSPFv3 IPv4 needs to have ipv6 support enabled on interface level.
Step 12	interface <i>sub-interface</i> Example: Router(config-if)# interface gi0/0/0.2	Sub-interface configuration to add DLEP template.
Step 13	ip dlep vtemplate <number> Example: Router(config-subif)# ip dlep vtemplate 1 gtsm client 10.0.0.2	Attaching DLEP Template to sub-interface
Step 14	exit Example: Router(config-if)# exit Router(config)#	Exits the current mode.
Step 15	router eigrp <AS-NO> Example: Router(config)# router eigrp 1 Router(config-router)# router-id 1.1.1.1 Router(config-router)# network 10.0.0.0 0.0.0.255	Enable global configuration for EIGRP.

Example

```
Router# show running-config
Building configuration...
Current configuration : 7726 bytes
!
!
version 17.8
hostname Router
!
boot-start-marker
boot system bootflash:/c6300-universalk9.SSA.bin
boot-end-marker
!
ipv6 unicast-routing
subscriber templating
!
license udi pid ESR-6300-CON-K9 sn FOC234304H3
```

```

license boot level network-advantage
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
ipv6 enable
ospfv3 1 ipv4 area 0
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
!
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
ip address 10.0.0.1 255.255.255.0
ip dlep vtemplate 1 port 11113 tcp port 11114 client ip 10.0.0.2 port 11115
ipv6 enable
!
interface Virtual-Template1
ip unnumbered GigabitEthernet0/0/0.10
!
interface vm1
ip unnumbered GigabitEthernet0/0/0.10
ipv6 address FE80::7E31:EFF:FE85:1E78 link-local
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
physical-interface GigabitEthernet0/0/0.10
!
router ospfv3 1
!
address-family ipv4 unicast
exit-address-family
!
address-family ipv6 unicast
exit-address-family
!
end

Router#

```

Removing the DLEP Configuration

Before editing or removing any configuration related to virtual template or VMI interface, you will need to remove the configuration for dlep vtemplate attached to WAN or sub-interface. If you try to edit the vmi interface, or the virtual-template, you will receive the following messages:

```

Router(config)#interface vm1
vm1 is associated with an instance of DLEP running on GigabitEthernet0/0/0.
Please remove DLEP configuration before making any changes to the VMI configuration.
Router(config)#interface Virtual-Template1
Virtual-Template1 is associated with an instance of DLEP running on GigabitEthernet0/0/0.
Please remove DLEP configuration before making any changes to the virtual-template.

```

Procedure

	Command or Action	Purpose
Step 1	enable Example:	Enable privileged EXEC mode.

	Command or Action	Purpose
	Router> enable Router#	
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enter global configuration mode.
Step 3	interface interface Example: Router(config)# interface gi0/0/0	Interface mode.
Step 4	no ip dlep vtemplate 1 Example: Router(config-if)# no ip dlep vtemplate 1	Detach DLEP configuration.
Step 5	no int vmi <number> Example: Router(config-if)# no int vmi 1	Removing vmi interface on Router.
Step 6	no int Virtual-Template <number> Example: Router(config-if)# no int Virtual-Template 1	Removing Virtual template on Router.

With the above configuration, DLEP will be removed from router. However, Virtual-Access interfaces that are created while bringing up DLEP neighbors, will still show up in the output of the **show ip interface brief** command until the system is rebooted.

Configuring DLEP using the Web User Interface (WebUI)

The following images illustrate how to configure DLEP using the WebUI.

Configuring DLEP on Physical Interface

Navigate to **Configuration > Interface > Ethernet**. Select the interface to configure and then apply the DLEP Virtual Template. Click on **Update & Apply to Device**.

Configuring DLEP using the Web User Interface (WebUI)

Configuration > Interface > Ethernet

Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address	Layer
GigabitEthernet0/0/0	UP	UP	unassigned	Unassigned	L3
GigabitEthernet0/0/1	UP	DOWN	unassigned	Unassigned	L3
GigabitEthernet0/1/0	UP	DOWN	unassigned	Unassigned	L2
GigabitEthernet0/1/1	UP	DOWN	unassigned	Unassigned	L2
GigabitEthernet0/1/2	UP	DOWN	unassigned	Unassigned	L2
GigabitEthernet0/1/3	UP	DOWN	unassigned	Unassigned	L2

Configure Interface GigabitEthernet0/0/1

General Advanced

Description: (1-200 Characters)

Admin Status: UP

Port Fast: stable

Media Type: auto-select

VRF: None

Configure as LAN or WAN: LAN WAN

IP Options: IPv4 IPv6

IPv4 Type: Static

IP Address*: XXX.XXX.XXX.XXX

Subnet Mask*: XXX.XXX.XXX.XXX

Secondary IP:

NAT: DISABLED

CSPF: None

BFD: None

DLEP-Virtual Template: None

Cancel Update & Apply to Device

Configuring DLEP on the Sub-Interface

Navigate to **Configuration > Interface > Ethernet**. Select the sub-interface to configure and then apply the DLEP Virtual Template. Click on **Update & Apply to Device**.

Configuration > Interface > Ethernet

Ethernet | GigabitEthernet0/0/0

+ Add - Delete

Sub Interface	Admin Status	Operational Status
GigabitEthernet0/0/0.1	UP	DOWN
GigabitEthernet0/0/0.30	UP	UP
GigabitEthernet0/0/0.10	UP	UP

Sub Interface Details

Sub Interface Name: GigabitEthernet0/0/0.1

VRF: None

Dot1Q Encapsulation:

VLAN ID*: 1-4094

Secondary Tag:

IP Options: IPv4 IPv6

IPv4 Type: Static

IP Address*: XXX.XXX.XXX.XXX

Subnet Mask*: XXX.XXX.XXX.XXX

Secondary IP:

DLEP-Virtual Template: None

Configuring the Virtual-Template

Navigate to **Configuration > Interface > Logical**. Select the **Virtual-Template** tab. From here you can Add, Edit, or Delete interfaces.

Configuration > Interface > Logical

Port Channel Loopback Dialer Virtual-Template VMI

+ Add - Delete



Name	Admin Status	Operational Status	Description
Virtual-Template2	UP	DOWN	undefined
Virtual-Template3	UP	UP	undefined
Virtual-Template5	UP	DOWN	undefined

1 - 3 of 3 items

Add/Edit the Virtual-Template

Select **Add**. The **Add Virtual Interface** window appears.

Add Virtual Interface

Virtual Template*	<input type="text"/>
Description	<input type="text"/>
IP Unnumbered	None ▼
IPv6	<input type="checkbox"/>
Input User Defined QoS	test123 ▼ 
Output User Defined QoS	None ▼ 

Click on **Apply to Device**.









Configuring the VMI

Navigate to **Configuration > Interface > Logical**. Select the **VMI** tab. From here you can Add, Edit, or Delete interfaces.

Configuration > Interface > Logical

Port Channel Loopback Dialer Virtual-Template **VMI**

[+ Add](#) [× Delete](#)

Name	Admin Status	Operational Status	Description
vm1			undefined
vm2			undefined
vm3			undefined
vm5			undefined

1 - 4 of 4 items

Add/Edit the VMI

Select **Add**. The **Add VMI** window appears.

Add VMI

VMI*	<input type="text"/>								
Description	<input type="text"/>								
IP Unnumbered	None ▾								
Physical Interface	None ▾								
IPv6	<input type="checkbox"/>								
IPv6 Link Local Address	<input type="text" value="fe80::x"/>								
OSPFv3	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px;">▾</div> <div style="margin-left: 5px;">IPv4 Area</div> <div style="margin-left: 10px;">Manet <input type="checkbox"/> +</div> </div> <table style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 15%;">Process ID</th> <th style="width: 15%;">IPv4 Area</th> <th style="width: 15%;">Manet</th> <th style="width: 15%;">Remove</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">0</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Process ID	IPv4 Area	Manet	Remove	0			
Process ID	IPv4 Area	Manet	Remove						
0									
Disable EIGRP Split Horizon	<input type="checkbox"/>								

Cancel
Apply to Device

Click on **Apply to Device**.

Monitoring DLEP

Navigate to **Monitoring > General > DLEP**. There are two tabs available for monitoring **Neighbors** or **Clients**. The Neighbors tab will display information equivalent to the CLI **show dlep neighbors**. The Clients tab will display information equivalent to the CLI **show dlep clients**.

DLEP Neighbors

Under the Neighbors tab, select the interface.

Monitoring > General > DLEP

Neighbors

Clients

Interface	Local IP
GigabitEthernet0/0/0.10	10.0.0.1

1
10 ▾
1 - 1 of 1 items

Open the interface to view the details.

Monitoring > General > DLEP
 Neighbors Clients
 Interface
 GigabitEthernet0/0/0.10

DLEP Neighbors for Interface GigabitEthernet0/0/0.10

Interface					GigabitEthernet0/0/0.10
Local IP					10.0.0.1
Session ID	MAC Address	Remote IP Address	Remote IPv6 LL	Associated Virtual Access Interface	
2234	2345.4321.7890	10.0.0.8	FE30:D78:5DFF-FE5D:3530	Virtual-Access1	

1
10 ▾
1 - 1 of 1 items

DLEP Clients

The Clients tab works in the same manner as the Interface tab. Select the interface and open it to view the details.

Interface	Local IP	Peer ID	Local Radio IP	Virtual template	Description
GigabitEthernet0/0/1	14.0.0.1	1	14.0.0.1	1	DLEP ONE Radio

DLEP Validation Commands

This section contains examples of how to verify the DLEP configuration on the router.

DLEP Configuration

Command	Information
<pre>Router# show dlep config ? GigabitEthernet GigabitEthernet IEEE 802.3z Output modifiers <cr> <cr></pre>	DLEP configuration is supported only on WAN or sub-interface.

```
Router# show dlep config g0/0/1
DLEP Configuration for GigabitEthernet0/0/1

DLEP Peer Description -
DLEP Version = RFC 8175
DLEP Server IP=10.0.0.1:11117
DLEPv27 TCP Port = 11118
Virtual template=2
Timers (all values are in seconds):
Missed heartbeat threshold=2, Peer Terminate ACK timeout=10
Dlepv27 Applicable configs(in seconds):
Heartbeat interval=5, Discovery interval =5, Session Ack timeout=10
Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

DLEP Clients

Command	Information
<pre>Router# show dlep clients ? GigabitEthernet GigabitEthernet IEEE 802.3z Output modifiers <cr> <cr></pre>	DLEP clients is supported only on WAN or sub-interface.

```
Router# show dlep clients
DLEP Clients for all interfaces:
```

```
DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Server IP=10.0.0.1:11117 Sock=0 --> Local Router IP address
```

```

DLEP Client IP=10.0.0.2:859 TCP Socket fd=1 --> Directly connected Radio to the router
Peer ID=2, Virtual template=2
Description: DLEP_RadioSIM2
Peer Timers (all values in milliseconds):
  Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
  Link RLQ RX Metric : 100
  Link RLQ TX Metric : 100
  Link Resources Metric : 100
  Link MTU Metric : 100
  Link Latency Metric : 250 microseconds
  Link CDR RX Metric : 100000000 bps
  Link CDR TX Metric : 100000000 bps
  Link MDR RX Metric : 100000000 bps
  Link MDR TX Metric : 100000000 bps
Router#

```

DLEP Neighbor

Command	Information
<pre> Router# show dlep neighbor ? GigabitEthernet GigabitEthernet IEEE 802.3z Output modifiers <cr> <cr> </pre>	DLEP neighbors is supported only on WAN or sub-interface.

```

Router# show dlep neighbor
DLEP Neighbors for all interfaces:

DLEP Neighbors for Interface GigabitEthernet0/0/1
DLEP Server IP=10.0.0.1:11117 Sock=0 ---> Local Router IP address

SID=2151 MAC_Address=a453.0e94.f861
Addresses:
IPv4 : 16.0.0.1 ---> Mac-Address and IPv4 address of neighbor's end-point device
Supported Metrics:
  RLQ RX Metric : 100
  RLQ TX Metric : 100
  Resources Metric : 100
  MTU Metric : 1500
  Latency Metric : 250 microseconds
  CDR RX Metric : 100000000 bps
  CDR TX Metric : 100000000 bps
  MDR RX Metric : 100000000 bps
  MDR TX Metric : 100000000 bps

```

DLEP Counters

Command	Information
<pre> Router# show dlep counters ? GigabitEthernet GigabitEthernet IEEE 802.3z Output modifiers <cr> <cr> </pre>	DLEP Counters is supported only on WAN or sub-interface, which will summarize port information, counters for peer, and neighbors.


```

UUT1# show dlep counters
DLEP Counters for GigabitEthernet0/0/1

Last Clear Time =

DLEP Version = RFC 8175
DLEP Server IP=10.0.0.1:11117
DLEPv5 TCP Port = 11118

Peer Counters:
RX Peer Discovery      0      TX Peer Offer          0
RX Peer Offer         0      TX Peer Discovery     0
RX Peer Init          0      TX Peer Init Ack      0
RX Peer Init Ack      1      TX Peer Init          1
RX Heartbeat          41     TX Heartbeat          41
RX Peer Terminate     0      TX Peer Terminate Ack 0
RX Peer Terminate Ack 0      TX Peer Terminate     0

Neighbor Counters:
RX Neighbor Up        1      TX Neighbor Up Ack    1
RX Metric             0
RX Neighbor Down      0      TX Neighbor Down Ack  0
RX Neighbor Down Ack  0      TX Neighbor Down      1

Exception Counters:
RX Invalid Message    0      RX Unknown Message    0
Pre-Existing Neighbor 0      Neighbor Resource Error 1
Neighbor Not Found    0      Neighbor Msg Peer Not Up 0

Timer Counters:
Peer Heartbeat Timer   41
Peer Terminate Ack Timer 0
Neighbor Terminate Ack Timer 0
Neighbor Activity Timer 0
Radio Connect Timer    5

Single Timer Wheel "Manet Infra Wheel"
Granularity      = 250 msec
Wheel size       = 4096
Spoke index      = 3730
Tick count       = 3423890
Flags            = 0x00
Active timers    = 1
High water mark  = 1
Started timers   = 171177
Restarted timers = 2
Cancelled timers = 5
Expired timers   = 171169
Long timers      = 0
Long timer revs  = 0
Timer suspends  = 0

```

Optional Configurations for DLEP

There are set of optional commands that are available to configure for the **ip dlep** CLI under the WAN or sub-interface. Based on those commands, you can define the set of timeout intervals between peers, neighbors, and how long to send heart-beat intervals to radio's.

Command	Purpose
<code>ip dlep set heartbeat-threshold ?</code> <2-8> Threshold of missed heartbeat messages	Set the heartbeat-threshold, between Server and Client.
<code>ip dlep set nbr-activity-timeout ?</code> <0-240> Neighbor Activity timer duration in seconds	Set the neighbor activity timeout.
<code>ip dlep set nbr-down-ack-timeout ?</code> <1-50> Neighbor Down ACK timer duration in seconds	Set the neighbor acknowledgment timeout.
<code>ip dlep set peer-description ?</code> LINE Peer Description Name	Defines the description with Peer.
<code>ip dlep set peer-heartbeat-interval ?</code> <1-60> Peer Heartbeat Interval timer duration in seconds	Set the heartbeat interval between Server and client.
<code>ip dlep set peer-discovery-interval ?</code> <1-60> Peer Discovery Interval timer duration in seconds	Set the peer discovery interval timer.
<code>ip dlep set peer-init-ack-timeout ?</code> <1-60> Peer Init ACK timer duration in seconds	Set the peer with init acknowledge messages from client.
<code>ip dlep set peer-terminate-ack-timeout ?</code> <1-50> Peer Terminate ACK timer duration in seconds	Set the peer terminate acknowledge timer between client and server.

DLEP IPv6 Unicast

Previous releases of IOS XE offered support for IPv4 unicast traffic over an IPv4 DLEP session. IOS XE 17.12.1a provides support for IPv6 unicast over an IPv4 DLEP session.

This section provides a subset of the overall DLEP information that is found in the [IP Routing Configuration Guide, Cisco IOS XE 17.x](#).

Feature Limitations

DLEP has the following restrictions and limitations:

- Multicast traffic is not supported with DLEP, but is supported with PPPOE.
- DLEP cannot be deployed with High Availability (HA) configuration.
- You must configure the VMI and Virtual-Template before attaching the Virtual-Template to a physical interface.
- The ESR6300 is connected over DLEP radio links and only 1 radio per interface (WAN port only) is supported.
- All configurations for the virtual-template need to be removed individually using the no form of the respective configuration commands, before removing the virtual-template using the no interface virtual-template command.

- Changing of configurations on the virtual-template and VMI interfaces is not supported while DLEP is enabled on the physical interface. In order to make such changes, disable DLEP by removing the DLEP configuration from the physical interface, make the changes, and re-configure DLEP on the physical interface.
- DLEP interface does not support Jumbo frames (frames > 1500 bytes in size).
- Routing of internally generated application traffic (e.g. pingv6) with source as DLEP VMI / physical interface is not supported.
- Viewing information about DLEP neighbors using the show ipv6 neighbor command is not supported.

IPv4 and IPv6 Multicast Over DLEP

DLEP Multicast is now supported with IOS XE 17.13.1. See the following configuration examples:

IPv4 Multicast

Global Command Examples:

```
ip multicast-routing distributed
ip pim rp-address <rp ip addr> [access-list for group]
```

Physical Interface Command Examples:

```
interface GigabitEthernet0/0/1
 ip address 28.28.28.1 255.255.255.0
 ip pim sparse-mode
 ip igmp version 3
 negotiation auto
 ipv6 address 1111::3/120
 ipv6 enable
```

VMI Command Examples:

```
interface vmi 5
 ip pim sparse-mode
```

Loopback Command Examples:

```
interface Loopback0
 ip address 7.7.7.7 255.255.255.255
 ip pim sparse-mode
 ipv6 address 2000::2/128
 ipv6 enable
```

IPv6 Multicast

Global Command Examples:

```
ipv6 pim
ipv6 multicast-routing
ipv6 pim rp-address <rp ipv6 addr> [access-list for group]
```

Physical Interface Command Examples:

```
interface GigabitEthernet0/0/2
 ip address 38.38.38.1 255.255.255.0
 ip igmp version 3
 ipv6 mld version 2
 negotiation auto
```

```

ipv6 address 1111::3/120
ipv6 enable
ipv6 pim register-source loopback0

```

VMI Command Examples:

```

interface vmi 5
ip pim sparse-mode

```

Loopback Command Examples:

```

interface Loopback0
ip address 7.7.7.7 255.255.255.255
ip pim sparse-mode
ipv6 address 2000::2/128
ipv6 enable

```

Remove Commands

Remove Command Examples:

```

Router(config-if)# no ip dlep vtemplate 1
Router(config-if)# no int vmi 1
Router(config-if)# no int Virtual-Template 1

```

Show Commands

Show Command Examples:

```

show ip interface brief
show dlep config
show dlep clients
show dlep neighbors

```

IPv6 Control Plane for DLEP

IOS-XE 17.13.1 supports DLEP control plane session support on an IPv6 network. When both the router and radio are running an IPv6 stack, the router can initiate DLEP session setup over IPv6. Both manual mode and auto discovery mode are supported. When the router is configured with an IPv6 address and transport layer port details of listening radio, the router initiates DLEP session setup in manual mode.

Clearing DLEP Clients and Neighbors

This section describes how the `clear dlep client <interface> <peer id>` command works, and possible ramifications.

When the **clear dlep client** command is issued on a router, the router sends a "Session Termination" message to the radio. The radio responds to this message by sending a "Session Termination Response" message. When the router receives the "Session Termination Response" message, it tears down the peer session.

When the radio is stopped gracefully, and after the **clear dlep client** command is issued on the router, the router will still send "Session Termination" message to the radio, but it won't be received by the radio, since it is already turned off. The router will automatically tear down the peer session after the timeout (heartbeat timer expiry) is reached.

The following shows an example:



Note First obtain the Peer ID from the output of the **show dlep client** CLI. Then, use that as the input to the **clear dlep client** CLI.

```
Router#show dlep client gi0/0/1

DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Local IP=15.0.0.10:5555 Sock=0

DLEP Local Radio IP=15.0.0.2:856 TCP Socket fd=1
Peer ID=20, Virtual template=2
Description: DLEP_Radio_2042
Peer Timers (all values in milliseconds):
Heartbeat=60000, Dead Interval=120000, Terminate ACK=240000
Neighbor Timers (all values in seconds):
Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps
Router#

Router#clear dlep client gi0/0/1 20
DLEP: Clear Client (peer) peer_id=20 from 15.0.0.10

There is another clear dlep command that can be used. The clear dlep neighbor <interface> <session id> CLI
will clear dlep neighbors. The session id can be obtained from show dlep neighbor command.

Router#clear dlep neighbor gi0/0/1 2215
DLEP: Clear neighbor sid=2215 from 195.0.0.2
```

Troubleshooting with show commands

The following series of figures illustrates what the output of various show commands mean in a sample installation.

Figure 39: Sample Installation

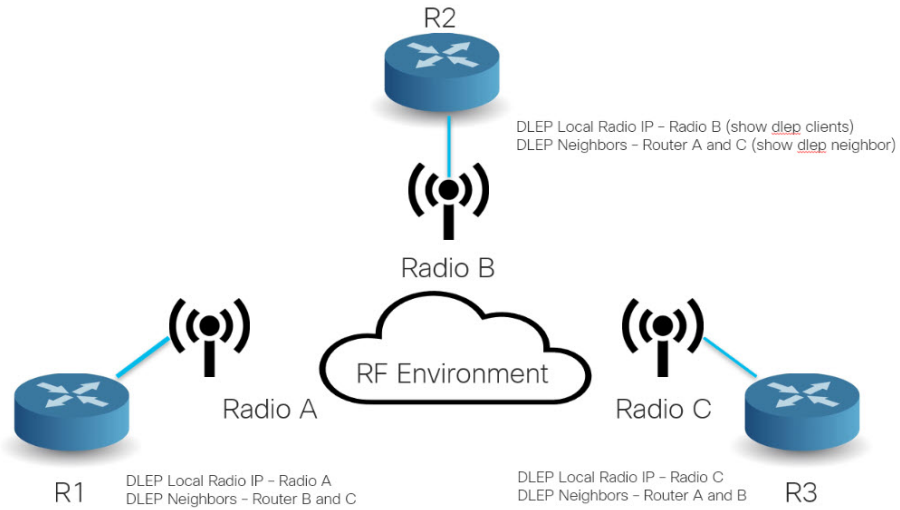


Figure 40: Show DLEP Configuration

show `dlep config`

```
sh dlep config GigabitEthernet0/0/0
DLEP Configuration for GigabitEthernet0/0/0

DLEP Peer Description -
DLEP Version = RFC 8175
DLEP Server IP=10.0.0.5:55555
DLEPv27 TCP Port = 55556
Virtual template=2
Timers (all values are in seconds):
Missed heartbeat threshold=2, Peer Terminate ACK timeout=10
Dlep27 Applicable configs(in seconds):
Heartbeat interval=5, Discovery interval =5, Session Ack timeout=10
Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

Local Router IP address

Figure 41: Show DLEP Clients

show dlep clients

```

show dlep clients
DLEP Clients for all interfaces:

DLEP Clients for Interface GigabitEthernet0/0/0
DLEP Server IP=10.0.0.5:55555 Sock=0

DLEP Client IP=10.0.0.4:11121 TCP Socket fd=1
Peer ID=3, Virtual template=2
Description: DLEP-Radio2-Path-1
Peer Timers (all values in milliseconds):
Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps

```

Local Router IP address

Directly connected Radio IP address

Attached virtual template for directly connected Radio from the router

Metrics from directly connected radio

Figure 42: Show DLEP Neighbors

show dlep neighbors

```

show dlep neigh
DLEP Neighbors for all interfaces:

DLEP Neighbors for Interface GigabitEthernet0/0/0
DLEP Server IP=10.0.0.5:55555 Sock=0

SID=2152 MAC_Address=7c31.0e85.1e78
Addresses:
IPv4 : 10.0.0.1 IPv6 LL : FE80::7E31:EFF:FE85:1E78
Supported Metrics:
RLQ RX Metric : 100
RLQ TX Metric : 100
Resources Metric : 100
MTU Metric : 1500
Latency Metric : 250 microseconds
CDR RX Metric : 100000000 bps
CDR TX Metric : 100000000 bps
MDR RX Metric : 100000000 bps
MDR TX Metric : 100000000 bps

```

Local Router IP address

MAC address of end-point router interface

IPv4 address and IPv6 link-local of end-point router

Supported Metrics to reach end-point router directly connected radio; based on the routing distance metrics will update appropriately

Figure 43: Show DLEP Counters

show dlep counters

```

show dlep counters GigabitEthernet0/0/0
DLEP Counters for GigabitEthernet0/0/0

Last Clear Time =

DLEP Version = RFC 8175
DLEP Server IP=10.0.0.1:55555
DLEPv5 TCP Port = 55556

```

→ Local Router IP address

Peer Counters:			
RX Peer Discovery	0	TX Peer Offer	0
RX Peer Offer	1	TX Peer Discovery	18
RX Peer Init	0	TX Peer Init Ack	0
RX Peer Init Ack	1	TX Peer Init	1
RX Heartbeat	18	TX Heartbeat	18
RX Peer Terminate	0	TX Peer Terminate Ack	0
RX Peer Terminate Ack	0	TX Peer Terminate	0
Neighbor Counters:			
RX Neighbor Up	1	TX Neighbor Up Ack	1
RX Metric	0		
RX Neighbor Down	0	TX Neighbor Down Ack	0
RX Neighbor Down Ack	0	TX Neighbor Down	0
Exception Counters:			
RX Invalid Message	0	RX Unknown Message	0
Pre-Existing Neighbor	0	Neighbor Resource Error	0
Neighbor Not Found	0	Neighbor Msg Peer Not Up	0
Timer Counters:			
Peer Heartbeat Timer	18		
Peer Terminate Ack Timer	0		
Neighbor Terminate Ack Timer	0		
Neighbor Activity Timer	0		
Radio Connect Timer	1		

Troubleshooting with debug commands

This section shows two different troubleshooting scenarios.



Note We recommend using debug commands only when under the guidance of Cisco TAC.

Scenario 1 : DLEP client is not reachable

In this scenario, the router is not running in discovery mode, and the client/radio attributes have been explicitly configured.

Step 1: The output of **show dlep clients** indicates that there is no active client:

```
Router# show dlep clients
```

```
DLEP Clients for all interfaces:
```

```
DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Server IP=14.0.0.3:11117 Sock=-1
```

Step 2: Check the DLEP configuration:

```
Router#show dlep config
```

```
DLEP Configuration for GigabitEthernet0/0/1
```

```

DLEP Peer Description -
DLEP Version = RFC 8175
DLEP Server IP=14.0.0.3:11117
DLEPv27 TCP Port = 11118
Virtual template=2
Timers (all values are in seconds):
Missed heartbeat threshold=2, Peer Terminate ACK timeout=10

```



```
Dlepv27 Applicable configs(in seconds):
Heartbeat interval=60, Discovery interval =5, Session Ack timeout=10
Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

```
Router#show run int g0/0/1
Building configuration...
```

```
Current configuration : 245 bytes
!
interface GigabitEthernet0/0/1
 ip address 14.0.0.3 255.255.255.0
 ip dlep set peer-heartbeat-interval 60
 ip dlep vtemplate 2 port 11117 tcp port 11118 client ip 14.0.0.6 port 859
 negotiation auto
 ipv6 address 1111::1/120
 ipv6 enable
end
```

Step 3: Verify that the configuration on the radio (client) matches the configuration on the router (server) and that the router can reach the radio.

```
Router#show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.199.184.2 9 0013.5f22.0b4a ARPA GigabitEthernet0/0/0
Internet 10.199.184.3 8 0018.7414.4e80 ARPA GigabitEthernet0/0/0
Internet 10.199.184.19 - a453.0e94.f638 ARPA GigabitEthernet0/0/0
Internet 14.0.0.2 4 000c.297a.6b3d ARPA GigabitEthernet0/0/1
Internet 14.0.0.3 - a453.0e94.f639 ARPA GigabitEthernet0/0/1
Internet 14.0.0.6 0 Incomplete ARPA
```

```
Router#ping 14.0.0.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.0.0.6, timeout is 2 seconds:
...
Success rate is 0 percent (0/3)
```

Step 4: We are unable to ping the client '14.0.0.6'. A quick check of the radio configuration revealed that the client IP address was actually 14.0.0.2.

```
Router#show run int g0/0/1
Building configuration...

Current configuration : 245 bytes
!
interface GigabitEthernet0/0/1
 ip address 14.0.0.3 255.255.255.0
 ip dlep set peer-heartbeat-interval 60
 ip dlep vtemplate 2 port 11117 tcp port 11118 client ip 14.0.0.6 port 859
 negotiation auto
 ipv6 address 1111::1/120
 ipv6 enable
end
```

Step 5: Correct the client IP address.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0/1
Router(config-if)#no ip dlep vtemplate 2 port 11117 tcp port 11118 client ip 14.0.0.6 port
859
Router(config-if)# ip dlep set peer-heartbeat-interval 60
Router(config-if)#ip dlep vtemplate 2 port 11117 tcp port 11118 client ip 14.0.0.6 port 859
Router(config-if)#^Z
Router#
*Feb 18 19:43:48.951: %SYS-5-CONFIG_I: Configured from console by console
```

Step 6: Verify the fix.

```

Router#show dlep counters
DLEP Counters for GigabitEthernet0/0/1

Last Clear Time =

DLEP Version = RFC 8175
DLEP Server IP=14.0.0.3:11117
DLEPv5 TCP Port = 11118

Peer Counters:
RX Peer Discovery      0      TX Peer Offer          0
RX Peer Offer         0      TX Peer Discovery      0
RX Peer Init          0      TX Peer Init Ack      0
RX Peer Init Ack      1      TX Peer Init          1
RX Heartbeat          0      TX Heartbeat          0
RX Peer Terminate     0      TX Peer Terminate Ack 0
RX Peer Terminate Ack 0      TX Peer Terminate     0

Neighbor Counters:
RX Neighbor Up        0      TX Neighbor Up Ack    0
RX Metric             0
RX Neighbor Down      0      TX Neighbor Down Ack  0
RX Neighbor Down Ack  0      TX Neighbor Down      0

Exception Counters:
RX Invalid Message   0      RX Unknown Message    0
Pre-Existing Neighbor 0      Neighbor Resource Error 0
Neighbor Not Found   0      Neighbor Msg Peer Not Up 0

Timer Counters:
Peer Heartbeat Timer      0
Peer Terminate Ack Timer  0
Neighbor Terminate Ack Timer 0
Neighbor Activity Timer   0
Radio Connect Timer       1

Single Timer Wheel "Manet Infra Wheel"
Granularity      = 250 msec
Wheel size       = 4096
Spoke index      = 1710
Tick count       = 9902
Flags            = 0x00
Active timers    = 1
High water mark  = 1
Started timers   = 95
Restarted timers = 4
Cancelled timers = 4
Expired timers   = 86
Long timers     = 0
Long timer revs = 0
Timer suspends  = 0

Router#
Router#show dlep clients

DLEP Clients for all interfaces:

DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Server IP=14.0.0.3:11117 Sock=0

DLEP Client IP=14.0.0.2:859 TCP Socket fd=1

```

```
Peer ID=3, Virtual template=2
Description: DLEP_RadioSIM2
Peer Timers (all values in milliseconds):
  Heartbeat=60000, Dead Interval=120000, Terminate ACK=240000
Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10
```

```
Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps
```

Scenario 2: DLEP session keeps timing out

In this scenario, the router is running in discovery mode.

Step 1: The DLEP session keeps flapping as indicated by the output of **show dlep client** sometimes shows an active client and sometimes it does not. Also, the VMI and virtual-access interfaces keep going up and down.

```
Router#show dlep clients
```

```
DLEP Clients for all interfaces:
```

```
DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Server IP=14.0.0.3:55555 Sock=0
```

```
DLEP Client IP=14.0.0.2:859 TCP Socket fd=1
Peer ID=13, Virtual template=2
Description: DLEP_RadioSIM2
Peer Timers (all values in milliseconds):
  Heartbeat=5000, Dead Interval=10000, Terminate ACK=20000
Neighbor Timers (all values in seconds):
  Activity timeout=0, Neighbor Down ACK=10
```

```
Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps
```

```
Router#
```

```
*Feb 18 20:01:32.577: %SYS-5-CONFIG_P: Configured programmatically by process Manet Infra
Background from console as console
*Feb 18 20:01:32.580: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3,
changed state to up
*Feb 18 20:01:32.584: %LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
*Feb 18 20:01:32.625: %LINEPROTO-5-UPDOWN: Line protocol on Interface vmi2, changed state
to up
Router#
```

```

Router#
*Feb 18 20:01:44.864: %LINEPROTO-5-UPDOWN: Line protocol on Interface vmi2, changed state
to down
*Feb 18 20:01:44.873: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3,
changed state to down
*Feb 18 20:01:44.878: %LINK-3-UPDOWN: Interface Virtual-Access3, changed state to down
*Feb 18 20:01:44.889: %SYS-5-CONFIG_P: Configured programmatically by process VTEMPLATE
Background Mgr from console as console

```

Step 2: Turn on the following debug commands to troubleshoot:

```

debug dlep server
debug dlep timer detail
debug dlep client error
debug dlep client infra
debug dlep client packet detail
debug dlep client state

```

Step 3: The debug logs indicate that the router/server sent a peer discovery signal and received a peer offer in return.

```

*Feb 18 20:14:59.553: dlepv27_encoder_signal_packet_start DLEP_SIGNAL_PEER_DISCOVERY(1)
*Feb 18 20:14:59.553: dlepv27_encoder_signal_packet_end tlv block size=0 packet length=8
*Feb 18 20:15:04.609: dlepv27_encoder_signal_packet_start DLEP_SIGNAL_PEER_DISCOVERY(1)
*Feb 18 20:15:04.609: dlepv27_encoder_signal_packet_end tlv block size=0 packet length=8
*Feb 18 20:15:04.611: dlepv27_decoder_signal_packet DLEP_SIGNAL_PEER_OFFER(2) data length
30
*Feb 18 20:15:04.611: dlepv27_decoder_peer_type_tlv DLEP_TLV_PEER_TYPE flag - 0
dlepv27_decoder_parse_tlv_block last tlv 4; current block_len 11; next tlv 2
IPv4 Addr 14.0.0.2dlepv27_decoder_ipv4_conn_point_tlv DLEP_TLV_IPv4_CONN_POINT
dlepv27_decoder_parse_tlv_block last tlv 2; current block_len 0;
*Feb 18 20:15:04.611:
*Feb 18 20:15:04.611: dlepv27_decoder_packet rc(RC_DLEP_OK-0) state 0 signal 1 packet_len
38
*Feb 18 20:15:09.648: %DLEP_MSG-4-CONNECT_ERROR: TCP connect to Radio 14.0.0.2 failed via
Gi0/0/1. Error code: Resource temporarily unavailable

```

Step 4: Observe that the router/server then sent a session initialization message, and received an acknowledgement in return. The acknowledgement also carries the attributes of the radio/client. An examination of those attributes reveals that the heartbeat interval on the radio is set to 60 seconds.

```

*Feb 18 20:15:09.648: dlepv27_encoder_msg_packet_start DLEP_MSG_SESSION_INITIALIZATION(1)
*Feb 18 20:15:09.648: dlepv27_encoder_msg_packet_end tlv block size=13 packet length=17
*Feb 18 20:15:09.649: Adding Peer for address 14.0.0.2(859), peer_id=22
*Feb 18 20:15:09.649: MANET_Infra: insert s=FFFF771137A8, type=2 (client insert)
*Feb 18 20:15:09.650: MANET_Infra: Insert=FFFF745209B0 successful (client insert)
*Feb 18 20:15:09.650: MANET_Infra: insert s=FFFF771137A8, type=1 (client insert)
*Feb 18 20:15:09.650: MANET_Infra: Insert=FFFF64C3CEE8 successful (client insert)
*Feb 18 20:15:09.650: -0 Allocated peer context at 0xFFFF771137A8
*Feb 18 20:15:09.650: dlepv27_decoder_msg_packet DLEP_MSG_SESSION_INITIALIZATION_ACK(2)
data length 132
dlepv27_decoder_status_tlv DLEP_TLV_STATUS status_code=0 desc ()
dlepv27_decoder_parse_tlv_block last tlv 1; current block_len 127; next tlv 4

*Feb 18 20:15:09.650: dlepv27_decoder_peer_type_tlv DLEP_TLV_PEER_TYPE flag - 0
dlepv27_decoder_parse_tlv_block last tlv 4; current block_len 108; next tlv 5
dlepv27_decoder_heartbeat_interval_tlv DLEP_TLV_HEARTBEAT_INTERVAL heartbeat=60000
dlepv27_decoder_parse_tlv_block last tlv 5; current block_len 100; next tlv 12

*Feb 18 20:15:09.650: dlepv27_decoder_latency_data_rate_value DLEP_TLV_LINK_MDR_METRIC_RX
value=100000000
dlepv27_decoder_parse_tlv_block last tlv 12; current block_len 88; next tlv 13

*Feb 18 20:15:09.650: dlepv27_decoder_latency_data_rate_value DLEP_TLV_LINK_MDR_METRIC_TX
value=100000000

```

```

dlepv27_decoder_parse_tlv_block last tlv 13; current block_len 76; next tlv 14

*Feb 18 20:15:09.650: dlepv27_decoder_latency_data_rate_value DLEP_TLV_LINK_CDR_METRIC_RX
value=100000000
dlepv27_decoder_parse_tlv_block last tlv 14; current block_len 64; next tlv 15

*Feb 18 20:15:09.650: dlepv27_decoder_latency_data_rate_value DLEP_TLV_LINK_CDR_METRIC_TX
value=100000000
dlepv27_decoder_parse_tlv_block last tlv 15; current block_len 52; next tlv 16

*Feb 18 20:15:09.650: dlepv27_decoder_latency_data_rate_value DLEP_TLV_LINK_LATENCY_METRIC
value=250
dlepv27_decoder_parse_tlv_block last tlv 16; current block_len 40; next tlv 18
dlepv27_decoder_rlq_resource_value DLEP_TLV_LINK_RLQ_METRIC_RX value=100
dlepv27_decoder_parse_tlv_block last tlv 18; current block_len 35; next tlv 19
dlepv27_decoder_rlq_resource_value DLEP_TLV_LINK_RLQ_METRIC_TX value=100
dlepv27_decoder_parse_tlv_block last tlv 19; current block_len 30; next tlv 17
dlepv27_decoder_rlq_resource_value DLEP_TLV_LINK_RESOURCES value=100
dlepv27_decoder_parse_tlv_block last tlv 17; current block_len 25; next tlv 20
dlepv27_decoder_mtu_tlv DLEP_TLV_LINK_MTU mtu=100
dlepv27_decoder_parse_tlv_block last tlv 20; current block_len 19; next tlv 8
IPv4 Addr 14.0.0.2dlepv27_decoder_ipv4_address_tlv DLEP_TLV_IPV4_ADDRESS operation=1
dlepv27_decoder_parse_tlv_block last tlv 8; current block_len 10; next tlv 10
IPv4 Subnet Addr 255.255.255.0dlepv27_decoder_ipv4_address_subnet_tlv
DLEP_TLV_IPV4_ATTACHED_SUBNET operation=1 mask=24
dlepv27_decoder_parse_tlv_block last tlv 10; current block_len 0;
*Feb 18 20:15:09.651:
*Feb 18 20:15:09.651: dlepv27_decoder_packet rc(RC_DLEP_OK-0) state 1 signal 0 packet_len
136
Router#

```

Step 5: The router appears to be sending heartbeats 5 seconds apart:

```

*Feb 18 20:15:14.569: dlepv27_decoder_msg_packet DLEP_MSG_PEER_HEARTBEAT(16) data length 0

*Feb 18 20:15:14.569: -curr_state Dlep In-Session State normalized_event=Dlep Peer Heartbeat
Event p2peer=0xFFFF771137A8 peer_id=22 p2neighbor=0x0
*Feb 18 20:15:14.569: dlepv27_decoder_packet rc(RC_DLEP_OK-0) state 2 signal 0 packet_len
4
Router#
*Feb 18 20:15:19.569: dlepv27_decoder_msg_packet DLEP_MSG_PEER_HEARTBEAT(16) data length 0

*Feb 18 20:15:19.569: -curr_state Dlep In-Session State normalized_event=Dlep Peer Heartbeat
Event p2peer=0xFFFF771137A8 peer_id=22 p2neighbor=0x0
*Feb 18 20:15:19.569: dlepv27_decoder_packet rc(RC_DLEP_OK-0) state 2 signal 0 packet_len
4
Router#

```

Step6: The router is terminating the session, and receiving an acknowledgement of the same:

```

*Feb 18 20:15:24.569: dlepv27_decoder_msg_packet DLEP_MSG_SESSION_TERM(5) data length 5
dlepv27_decoder_status_tlv DLEP_TLV_STATUS status_code=0 desc ()
dlepv27_decoder_parse_tlv_block last tlv 1; current block_len 0;
*Feb 18 20:15:24.569:
*Feb 18 20:15:24.569: -curr_state Dlep In-Session State normalized_event=Dlep Peer Term
Event p2peer=0xFFFF771137A8 peer_id=22 p2neighbor=0x0
*Feb 18 20:15:24.569: -curr_state Dlep Terminating State normalized_event=Dlep Peer Term
ACK Event p2peer=0xFFFF771137A8 peer_id=22 p2neighbor=0x0
*Feb 18 20:15:24.569: dlepv27_encoder_msg_packet_start DLEP_MSG_SESSION_TERM_ACK(6)
*Feb 18 20:15:24.569: dlepv27_encoder_msg_packet_end tlv block size=12 packet length=16
*Feb 18 20:15:24.570: -curr_state Dlep Session Reset State normalized_event=Dlep Peer
sessoin reset Event p2peer=0xFFFF771137A8 peer_id=22 p2neighbor=0x0
*Feb 18 20:15:24.570: -0 Restart all peers on IDB GigabitEthernet0/0/1

```

```
*Feb 18 20:15:24.570: dlepv27_decoder_packet rc(RC_DLEP_OK-0) state 2 signal 0 packet_len
9
```

Step 7: An examination of the DLEP config reveals that the heartbeat on the router is set to 5 seconds:

```
Router#show dlep config
DLEP Configuration for GigabitEthernet0/0/1

DLEP Peer Description -
DLEP Version = RFC 8175
DLEP Server IP=14.0.0.3:55555
DLEPv27 TCP Port = 55556
Virtual template=2
Timers (all values are in seconds):
Missed heartbeat threshold=2, Peer Terminate ACK timeout=10
Dlepv27 Applicable configs(in seconds):
Heartbeat interval=5, Discovery interval =5, Session Ack timeout=10
Neighbor activity timeout=0, Neighbor Down ACK timeout=10
```

Step 8: Change the heartbeat to 60 seconds:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0/1
Router(config-if)#no ip dlep
Router(config-if)#no ip dlep vtemplate
Router(config-if)#no ip dlep vtemplate 2
Router(config-if)#ip dlep set peer-heartbeat-interval 60
Router(config-if)# ip dlep vtemplate 2
Router(config-if)#^Z
```

Step 9: Verify the change fixed the problem:

```
Router#show dlep clients

DLEP Clients for all interfaces:

DLEP Clients for Interface GigabitEthernet0/0/1
DLEP Server IP=14.0.0.3:55555 Sock=0

DLEP Client IP=14.0.0.2:859 TCP Socket fd=1
Peer ID=51, Virtual template=2
Description: DLEP_RadioSIM2
Peer Timers (all values in milliseconds):
Heartbeat=60000, Dead Interval=120000, Terminate ACK=240000
Neighbor Timers (all values in seconds):
Activity timeout=0, Neighbor Down ACK=10

Supported Metrics:
Link RLQ RX Metric : 100
Link RLQ TX Metric : 100
Link Resources Metric : 100
Link MTU Metric : 100
Link Latency Metric : 250 microseconds
Link CDR RX Metric : 100000000 bps
Link CDR TX Metric : 100000000 bps
Link MDR RX Metric : 100000000 bps
Link MDR TX Metric : 100000000 bps
Router#
*Feb 18 20:38:03.708: %SYS-5-CONFIG_P: Configured programmatically by process Manet Infra
Background from console as console
*Feb 18 20:38:03.712: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3,
changed state to up
```

```
*Feb 18 20:38:03.716: %LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
*Feb 18 20:38:03.722: %LINEPROTO-5-UPDOWN: Line protocol on Interface vmi2, changed state
to up
```

Additional Debug Commands

The following commands are available.



Note We recommend using debug commands only when under the guidance of Cisco TAC.

DLEP

```
debug dlep server detail
debug dlep timer detail
debug dlep neighbor error
debug dlep neighbor infrastructure detail
debug dlep neighbor infrastructure error
debug dlep neighbor metrics
debug dlep neighbor state
debug dlep neighbor all
debug dlep client error
debug dlep client infrastructure
debug dlep client packet dump
debug dlep client packet detail
debug dlep client state
```

VMI

```
debug vmi bma
debug vmi packet
debug vmi error
debug vmi multicast
debug vmi neighbor
debug vmi registries
```

Virtual Template

```
debug vtemplate cloning
debug vtemplate error
debug vtemplate event
debug vtemplate subinterface
```

PPPOE

```
debug pppoe errors
debug pppoe events
debug pppoe packets
debug pppoe data
```

SSS

```
debug sss error
debug sss event
```

SNMP MIB Support for DLEP

From Release IOS XE 17.14.1, the CISCO-DLEP-MIB is introduced. Using this MIB, user can retrieve the Dynamic Link Exchange Protocol (DLEP) feature parameters on Cisco ESR6300 Embedded Series Router. For information about DLEP protocol, see [DLEP](#).



Note CISCO-DLEP-MIB traps are not supported in the IOS XE 17.14.1.

Use the following SNMP objects to get the DLEP information:

1. DLEP Interface
2. DLEP Neighbor
3. DLEP Client
4. DLEP Config

DLEP Interface

The following table provides information about the DLEP configured interfaces:

Object Name	Purpose
dlepInterfaceIndex	Interface SNMP index with DLEP configuration
dlepInterfaceName	Interface name corresponds to the DLEP interface index
dlepInterfaceNbrSessionId	All session ids per interfaces

DLEP Neighbor

The following table provides information about the DLEP neighbors that were discovered.

Object Name	Purpose
dlepNeighborSessionId	Neighbor session id
dlepNeighborInterfaceIndex	Neighbor interface SNMP index with DLEP configuration
dlepNeighborInterfaceName	Name of the interface where the DLEP session is established.
dlepNeighborAddress	IPv4 addresses of neighboring DLEP devices
dlepNeighborAddressV6LL	IPv6 link local addresses of neighboring DLEP devices
dlepNeighborAddressV6GBL	IPv6 global addresses of neighboring DLEP devices

Object Name	Purpose
dlepNeighborIpUpTime	Uptime of a specific neighbor
dlepNeighborMetricsMTU	The maximum transmission unit (MTU) metric of a specific neighbor
dlepNeighborMetricsCdrRx	The rate at which the specific neighbor is currently operating for receiving traffic
dlepNeighborMetricsCdrTx	The rate at which the specific neighbor is currently operating for transmitting traffic
dlepNeighborMetricsMdrRx	The maximum theoretical data rate that can be achieved while receiving data on the neighbor device.
dlepNeighborMetricsMdrTx	The maximum theoretical data rate that can be achieved while transmitting data on the neighbor device.
dlepNeighborMetricsRlqRx	Quality of the specific neighbor to a destination for receiving traffic
dlepNeighborMetricsRlqTx	Quality of the specific neighbor to a destination for transmitting traffic
dlepNeighborMetricsLatency	Latency metric (in milliseconds) of a specific neighbor
dlepNeighborMetricsResource	Finite resource metric of a specific neighbor
dlepNeighborMetricsVac	Radio virtual access number information
dlepNeighborSessionOperStatus	State of the neighbor
dlepNeighborMetricsMacAddress	The MAC address of the neighbor

DLEP Client

The following table provides information about the DLEP client details:

Object Name	Purpose
dlepClientInterfaceIndex	Client interface SNMP index with DLEP configuration
dlepClientInterfaceName	Interface name corresponds to DLEP client interface index
dlepClientPeerId	Client peer id that corresponds to DLEP client interface index
dlepNeighborCount	Number of neighbors up on client
dlepClientDescription	Client description as configured
dlepClientAddressType	Local client address type

Object Name	Purpose
dlepClientLocalAddress	Local client address
dlepClientLocalRadioAddress	Local client radio address
dlepClientUpTime	Client uptime
dlepClientMetricsSummary	Summary of client metrics
dlepClientMetricsCdrRx	Client radio current data rate receive (CDRR) currently operating for receiving traffic
dlepClientMetricsCdrTx	Client radio current data rate transmit (CDRT) currently operating for transmitting traffic
dlepClientMetricsMdrRx	Client radio maximum data rate receive (MDRR)
dlepClientMetricsMdrTx	Client radio maximum data rate transmit (MDRT)
dlepClientMetricsRlqRx	Client relative link quality receive (RLQR)
dlepClientMetricsRlqTx	Client relative link quality transmit (RLQT)
dlepClientMetricsLatency	Client radio latency to indicate the amount of latency, in microseconds
dlepClientMetricsResources	The amount of finite client radio resource metric available for data transmission
dlepClientMetricsMTU	Client MTU
dlepClientConfigSummary	Summary of client configuration
dlepClientPort	Configured TCP port number
dlepClientConfigVT	Configured number of virtual templates
dlepClientConfigHeartBeat	Configured radio client heartbeat interval in milliseconds
dlepClientConfigDeadInterval	Configured radio client dead interval in milliseconds
dlepClientConfigTerminate	Configured radio client terminates acknowledgment configuration interval
dlepClientSessionOperStatus	Configured terminate interval in milliseconds
dlepClientMetricsNeighborDown	Configured radio neighbor down acknowledgment configuration

DLEP Config

The following table provides information about the DLEP configuration details:

Object name	Purpose
dlepConfigInterfaceIndex	The configuration interface SNMP index with DLEP configuration
dlepConfigInterfaceName	The DLEP enabled interface name
dlepConfigPeerInterfaceDescription	Configuration description
dlepConfigSummary	Summary of configuration
dlepConfigLocalAddressType	Configured local address type
dlepConfigLocalAddress	Configured local address
dlepConfigLocalTCPPort	Configured local TCP port number
dlepConfigLocalUDPPort	Configured local UDP port number
dlepConfigRemoteAddressType	Configured remote address type
dlepConfigRemoteAddress	Configured remote address
dlepConfigRemoteTCPPort	Configured remote TCP port number
dlepConfigRemoteUDPPort	Configured remote UDP port number
dlepConfigSessionMode	Configuration mode
dlepConfigVirtualTemplate	Configured virtual-template number
dlepConfigMissedHeartbeatThreshold	Configured threshold for a missed heartbeat
dlepConfigHeartbeatInterval	Configured heartbeat interval in milliseconds
dlepConfigDiscoveryInterval	Configured discovery interval in milliseconds
dlepConfigSessionAckTimeout	Configured session acknowledgment interval in milliseconds
dlepConfigPeerTerminateAckTimeout	Configured terminate acknowledgment interval in milliseconds
dlepConfigNeighborDownAckTimeout	Configured neighbor down acknowledgment interval in milliseconds

DLEP Counters

The following table provides information about the details of DLEP counters:

Object Name	Purpose
dlepCounterInterfaceIndex	The SNMP interface index with DLEP configuration
dlepCountersInterfaceName	Interface name that corresponds to the dlepConfigIfIndex

Object Name	Purpose
dlepCounterLastClearTime	Last clear time of counters
dlepCounterLocalIpType	Local IP type
dlepCounterLocalIp	Local IP
dlepCounterLocalTCPPort	Local TCP port
dlepCounterLocalUDPPort	Local UDP port
dlepCounterRXPeerDiscovery	Number of peer discovery packets received
dlepCounterRXPeerOffer	Number of peer offer packets received
dlepCounterRXPeerInit	Number of peer initialization packets received
dlepCounterRXPeerInitAck	Number of peer initialization acknowledgment packets received
dlepCounterRXHeartbeat	Number of heartbeat packets received
dlepCounterRXPeerTerminate	Number of peers terminate packets received
dlepCounterRXPeerTerminateAck	Number of peers terminate acknowledgment packets received
dlepCounterTXPeerOffer	Number of peer offer packets transferred
dlepCounterTXPeerDiscovery	Number of peer discovery packets transferred
dlepCounterTXPeerInitAck	Number of peer initialization acknowledgment packets transferred
dlepCounterTXPeerInit	Number of peer initialization packets transferred
dlepCounterTXHeartbeat	Number of heartbeat packets transferred
dlepCounterTXPeerTerminateAck	Number of peers terminate acknowledgment packets transferred
dlepCounterTXPeerTerminate	Number of peers terminate packets transferred
dlepCounterRXNeighborUp	Number of neighbors up packets received
dlepCounterRXMetric	Number of metrics packets received
dlepCounterRXNeighborDown	Number of neighbors down packets received
dlepCounterRXNeighborDownAck	Number of neighbors down acknowledgment packets received
dlepCounterTXNeighborUpAck	Number of neighbors up acknowledgment packets transferred

Object Name	Purpose
dlepCounterTXNeighborDownAck	Number of neighbors down acknowledgment packets transferred
dlepCounterTXNeighborDown	Number of neighbors down packets transferred
dlepCounterRXInvalidMessage	Number of invalid message packets received
dlepCounterPreExistingNeighbor	Number of pre-existing neighbor packets
dlepCounterNeighborNotFound	Number of neighbors not found packets
dlepCounterRXUnknownMessage	Number of unknown message packets received
dlepCounterNeighborResourceError	Number of neighbor resource error packets
dlepCounterNeighborMsgPeerNotUp	Number of neighbor message peers not up packets
dlepCounterPeerHeartbeatTimer	Number of peer heartbeat packets
dlepCounterPeerTerminateAckTimer	Number of peers terminate acknowledgment packets
dlepCounterNeighborTerminateAckTimer	Number of neighbors terminate acknowledgment packets
dlepCounterRadioConnectTimer	Radio connect timer counter
dlepLocalCountersSummary	Summary of all DLEP counters
dlepCountersPeersSummary	Summary of DLEP peer counters information
dlepCountersNeighborsSummary	Summary of DLEP neighbor counters information
dlepCountersExceptionsSummary	Summary of DLEP exceptions counters
dlepCountersTimersSummary	Summary of DLEP timer counters

Related Documentation

Additional information can be found in the following resources:

Radio Aware Routing is discussed in this [Cisco white paper](#).

[Internet Engineering Task Force \(IETF\) RFC 8175](#)



CHAPTER 20

IPv6 Multicast Over PPPoE

This chapter contains the following sections:

- [PPPoE in MANET, on page 241](#)
- [Feature Requirements, on page 244](#)
- [Enabling IPv6 Routing, on page 245](#)
- [Creating a Subscriber Profile, on page 245](#)
- [Configuring License Level, on page 246](#)
- [Configuring PPPoE Service Policy, on page 246](#)
- [Configuring QoS Provisioning, on page 247](#)
- [Configuring PPPoE Service Selection, on page 247](#)
- [Configuring PPPoE on an Ethernet Interface, on page 248](#)
- [Configuring a Virtual Template Interface, on page 248](#)
- [Configuring VMI interface and Enabling Multicast Support, on page 250](#)
- [Configuring the Loopback Interface, on page 251](#)
- [Configuring the OSPFv3 IPv4 Address Family Process , on page 252](#)
- [Configuring the OSPFv3 IPv6 Address Family Process , on page 253](#)
- [Configuring IPv6 PIM Bootstrap Router \(BSR\), on page 254](#)
- [Configuring IPv6 Multicast Group, on page 254](#)
- [Verifying Virtual Template Interface, on page 255](#)
- [Verifying PPPoE Session Details, on page 256](#)
- [Verifying BSR Election, on page 257](#)
- [IPv6 Multicast Routing Table , on page 258](#)
- [IPv6 Multicast over PPPoE , on page 259](#)
- [Verifying VMI Neighbors, on page 259](#)
- [Verifying OSPF Neighbor, on page 261](#)
- [Sample Running Configuration, on page 261](#)
- [Debug Commands, on page 265](#)

PPPoE in MANET

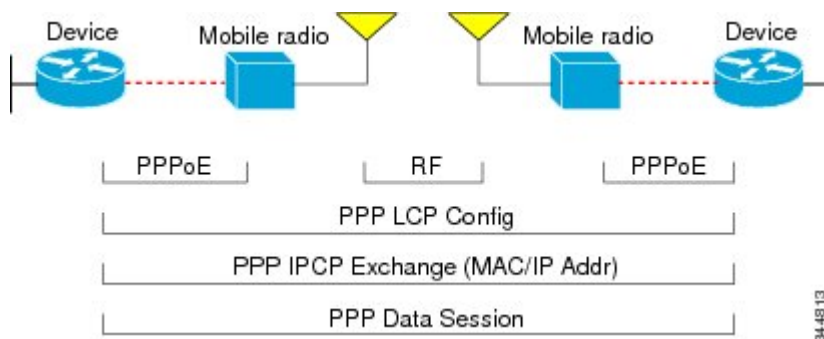
PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems.

The Cisco MANET solution employs PPPoE sessions to enable intra-nodal communications between a router and its partner radio. Each radio initiates the PPPoE session as soon as the radio establishes a radio link to another radio. After the PPPoE sessions are active, a PPP session is established end-to-end (router-to-router).

This is duplicated each time a radio establishes a new radio link. The Virtual Multipoint Interface (VMI) on the device can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Underneath the VMI are virtual access interfaces that are associated with each of the PPP and PPPoE connections.

A PPPoE session is established between a device and a radio on behalf of every other device and radio neighbor located in the MANET. These Layer 2 sessions are the means by which radio network status gets reported to the Layer 3 processes in the device. The following figure shows the PPPoE session exchange between mobile devices and directional radios in a MANET network.

Figure 44: PPPoE Session Exchange Between Mobile Devices and Directional Radios



Link Control Protocol (LCP) forms part of the Point-to-Point Protocol (PPP), within the family of Internet protocols. The routers exchange IP Control Protocol (IPCP) messages to negotiate options specific to the protocol.

VMI Interface

The VMI on the device can aggregate all of the per-neighbor PPPoE sessions from the radio Ethernet connection. The VMI maps the sessions to appear to Layer 3 routing protocols and applications as a single point-to-multipoint, multiaccess, broadcast-capable network. However, the VMI preserves the integrity of the PPPoE sessions on the radio side so that each point-to-point connection can have its own quality of service (QoS) queue.

The VMI also relays the link-quality metric and neighbor up/down signaling from the radio to the routing protocols. The VMI signals are used by the Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6 neighbors and the Open Shortest Path First version 3 (OSPFv3) for IPv6 neighbors.

The VMI can operate in two modes: bypass or aggregate.

Bypass Mode

This is the recommended mode for PPPOE in a MANET network.

In bypass mode, the virtual-access interfaces are directly exposed to applications running above L2. In bypass mode, you must still define a VMI because VMI continues to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware of the actual underlying virtual-access interfaces and send packets to them directly.

If you are running multicast applications that require virtual-access interfaces to be exposed to applications above L2 directly, you can configure VMI to operate in bypass mode. Most multicast applications require that the virtual-access interfaces be exposed directly to routing protocols for the multicast Reverse Path Forwarding (RPF) to operate as expected .

Aggregate Mode

In this mode, all the virtual-access interfaces created by PPPoE sessions are aggregated logically under the configured VMI. VMI on the router can aggregate multiple PPPoE sessions and multiplex them to look like a single interface to the routing processes. Applications above Layer 2 (L2), such as Enhanced Interior Gateway Routing Protocol (EIGRP) and OSPFv3, should be defined only on VMI. Underneath VMI are virtual access interfaces that are associated with each of the PPP/PPPoE connections. Packets sent to VMI are forwarded to the correct virtual-access interface(s).

Aggregate mode VMIs operate in Non-Broadcast Multiple Access (NBMA) mode. Multicast traffic is forwarded only to the NBMA neighbors where a listener for that group is present. This is the preferred mode when operating in PIM sparse mode.

Virtual Access Interface

The Virtual-Access interfaces are logically “underneath” the VMI interface. Each Virtual-Access interface represents a “destination” which is either a routing next-hop, or a multicast group. At the bottom of the interface hierarchy is the actual physical interface connecting the router and radio. The Virtual-Access interface funnels the traffic to the physical interface for transmission to the radio device.

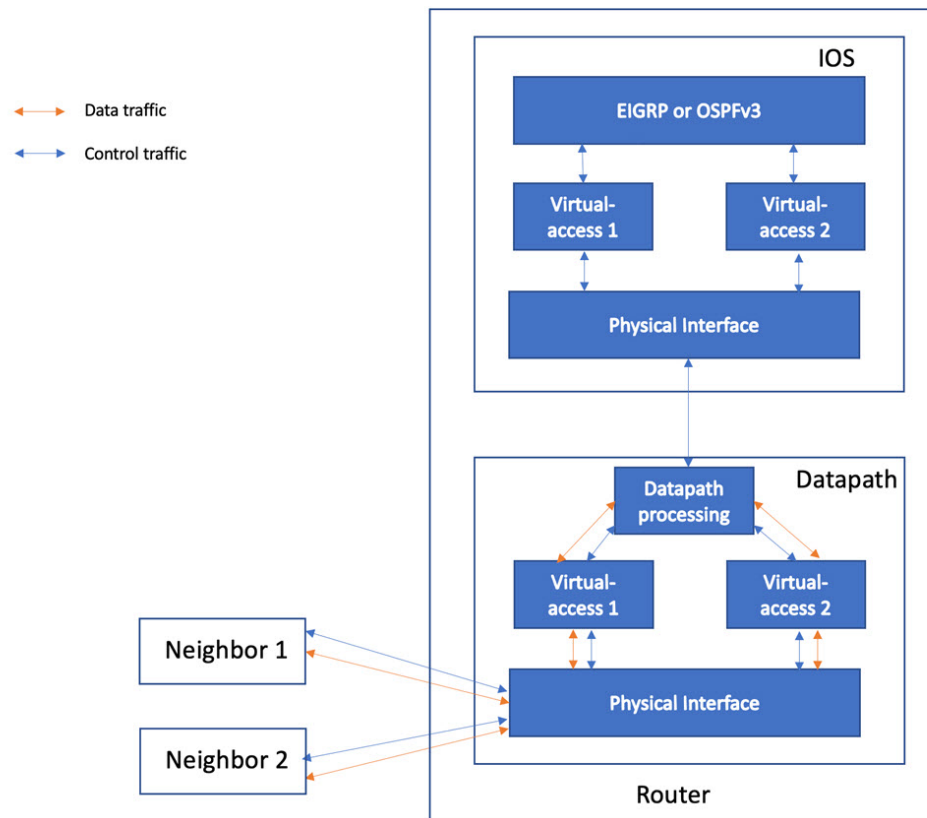
PPPOE Packet Flow

The Packet Flow diagram below illustrates the packet flow for both control and data packets over a PPPOE session when the VMI interface is in bypass mode.

All control traffic is sent to by the datapath to IOS where it is handed over to the appropriate protocol to be processed. The incoming interface for this traffic is the virtual-access interface associated with the neighbor which is the source of the traffic. In this case, Virtual-access1 corresponds to Neighbor 1 and Virtual-Access 2 corresponds to Neighbor 2.

All data traffic is processed by the datapath and does not typically get sent to IOS.

Figure 45: Packet Flow



Feature Requirements

For IPv6 multicast over PPPoE to function properly, the following must be configured:

- PPPoE (Virtual-template, VMI and physical interface)
- IPv6 unicast and multicast routing
- IPv6 PIM BSR
- IPv6 MLD



Note This feature requires the Network Advantage License.

Enabling IPv6 Routing

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	ipv6 unicast-routing Example: Router(config)# ipv6 unicast-routing	Enable IPv6 Unicast routing.
Step 3	ipv6 multicast-routing Example: Router(config)# ipv6 multicast-routing	Enables multicast routing on all IPv6-enabled interfaces, and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

Creating a Subscriber Profile

The Subscriber Profile Support feature is functionality for the Subscriber Service Switch architecture, a Cisco IOS subsystem that connects subscribers to network access services at Layer 2. This functionality affects how the Subscriber Service Switch Manager determines a service for each subscriber with a combination of a policy and a service lookup model.



Note Configuring a subscriber profile for PPPoE service selection is required for VMI to function properly.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	subscriber templating Example: Router(config)# subscriber templating	Configure subscriber templating.
Step 3	subscriber authorization enable Example: Router(config)# subscriber authorization enable	Enable Subscriber Service Switch type authorization.

Configuring License Level

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>license boot level type</code> Example: Router(config)# <code>license boot level network-advantage</code>	Configure License information. Note Must be configured as Network Advantage for IPv6 multicast routing.

Configuring PPPoE Service Policy

A service policy specifies class-based weighted fair queuing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>policy-map type service name</code> Example: Router(config)# <code>policy-map type service pppoe_rar</code>	Configure policy map type.
Step 3	<code>pppoe service name</code> Example: Router(config-service-policymap)# <code>pppoe service manet_radio</code>	Configure service policy map. Note Enter the PPPoE service policy name as <code>manet_radio</code> .

Configuring QoS Provisioning

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	policy-map name Example: Router(config)# policy-map rar_policer	Create a policy map name.
Step 3	class criteria_name Example: Router(config-pmap)# class class-default	Configure policy criteria as system default class.
Step 4	police target_rate conform-action action exceed-action action Example: Router(config-pmap-c)# police 10000000 conform-action transmit exceed-action drop	Configure QoS policy for the Virtual Template Interface.

Configuring PPPoE Service Selection

The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. The customer chooses one of the services offered, and the service is provided when the PPPoE session becomes active. This feature enables service providers to offer a variety of services and to charge customers according to the service chosen.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	bba-group pppoe name Example: Router(config)# bba-group pppoe rar_group_1	Configure PPPoE global group.

	Command or Action	Purpose
Step 3	virtual-template <i>number</i> Example: Router(config-bba-group)# virtual-template 1	Attach the Virtual Template to the PPPoE bba group.
Step 4	service profile <i>name</i> Example: Router(config-bba-group)# service profile pppoe_rar	Attach the service policy name .

Configuring PPPoE on an Ethernet Interface

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	interface [<i>type slot/port</i>] Example: Router(config)# interface GigabitEthernet0/0/0	Specifies an interface type and enters interface configuration mode.
Step 3	ipv6 enable Example: Router (config-if)# ipv6 enable	Enable IPv6 support under VMI interface. OSPFv3 IPv4 needs to have IPv6 support enabled on the interface level.
Step 4	pppoe enable group <i>group_name</i> Example: Router(config-if)# pppoe enable group rar_group_1	Enables PPPoE sessions on the interface or sub interface.

Configuring a Virtual Template Interface

You use the virtual template interface to dynamically clone configurations for each virtual access interface created for a virtual multipoint interface (VMI) neighbor. You can configure multiple virtual template interfaces for your VMI PPP over Ethernet (PPPoE) connections. The selection of which virtual template to use is predicated on the service name sent by the radio during PPPoE session establishment.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	interface Virtual-Template number Example: Router(config)# interface Virtual-Template 1	Creates a Virtual Template Interface for configuration and dynamic application to Virtual Access Interfaces.
Step 3	mtu size Example: Router(config-if)# mtu 1484	Sets the MTU size.
Step 4	ip unnumbered interface_type interface_number Example: Router(config-if)# ip unnumbered vmi 1	Enable IP processing without an explicit address. Specifies the Virtual Template Interface to use the VMI interface IP address.
Step 5	no ip redirects Example: Router(config-if)# no ip redirects	Disables ICMP redirect messages.
Step 6	ip tcp adjust-mss size Example: Router(config-if)# ip tcp adjust-mss 1444	Adjust the mss of transit packets.
Step 7	load-interval value Example: Router(config-if)# load-interval 30	Load interval delay.
Step 8	no peer default ip address Example: Router(config-if)# no peer default ip address	Disables peer default ip address.
Step 9	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable IPv6 support under Virtual Template Interface.
Step 10	ipv6 mtu size Example: Router(config-if)# ipv6 mtu 1484	Sets the IPv6 MTU size.
Step 11	ospfv3 1 network type Example:	Configure the Virtual Template Interface as MANET OSPF interface type.

	Command or Action	Purpose
	Router(config-if)# ospfv3 1 network manet	
Step 12	ospfv3 1 hello-interval <i>value</i> Example: Router(config-if)# ospfv3 1 hello-interval 10	Configure the hello interval value for OSPFv3.
Step 13	ospfv3 1 ipv4 area <i>id</i> Example: Router(config-if)# ospfv3 1 ipv4 area 0	Enable Virtual Template Interface to participate in OSPFv3 IPv4 routing.
Step 14	ospfv3 1 ipv6 area <i>id</i> Example: Router(config-if)# ospfv3 1 ipv6 area 0	Enable Virtual Template Interface to participate in OSPFv3 IPv6 routing.
Step 15	service-policy input <i>policy_map_name</i> Example: Router(config-if)# service-policy input rar_policer	Attach the created policy map name to the Virtual Template Interface.

Configuring VMI interface and Enabling Multicast Support

Used in router-to-radio communications, the Virtual Multipoint Interface (VMI) interface provides services that map outgoing packets to the appropriate Point-to-Point Protocol over Ethernet (PPPoE) sessions based on the next-hop forwarding address for that packet. The VMI interface also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability. When a packet with a multicast address is forwarded through the VMI interface, VMI replicates the packet and unicasts it to each of its neighbors.



Note VMI will map outgoing packets to the appropriate PPPoE sessions. It will use the next-hop forwarding address from each outgoing packet to perform this mapping.



Note VMI is required to have IP addresses assigned for VMI to work even though it will be shown as down/down while in bypass mode. The IPv4 address configured will not be advertised or used. Instead, the IPv4 address on the virtual-template will be used.

Procedure

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

	Command or Action	Purpose
	Router# configure terminal	
Step 2	interface vmi <i>number</i> Example: Router(config)# interface vmi 1	Creates a VMI and enters interface configuration mode.
Step 3	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable IPv6 support under VMI interface. OSPFv3 IPv4 needs to have IPv6 support enabled on the interface level.
Step 4	ip address <i>address mask</i> Example: Router(config-if)# ip address 71.0.0.1 255.255.255.0	Configures IPv4 address under VMI interface.
Step 5	ipv6 address <i>address/prefix</i> Example: Router(config-if)# ipv6 address 71::71/64	Configures IPv6 address under VMI interface.
Step 6	physical-interface <i>interface</i> Example: Router(config-if)# physical-interface gigabitEthernet {0/0/0 or 0/0/1 or 0/0/0.1}	Binds the physical interface (the interface connected to the radio client) to the VMI interface, for packet flow.
Step 7	mode <i>name</i> Example: Router(config-if)# mode bypass	Do not aggregate Virtual Access Interfaces under VMI. (Must be configured as bypass).

Configuring the Loopback Interface

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	interface loopback <i>number</i> Example: Router(config)# interface loopback 1	Assigns the loopback interface number.

	Command or Action	Purpose
Step 3	ip address <i>address mask</i> Example: Router(config-if)# ip address 1.1.1.1 255.255.255.255	Configuring IPv4 address for the loopback interface.
Step 4	ipv6 address <i>address/prefix</i> Example: Router(config-if)# ipv6 address 11::11/128	Configures IPv6 address for the loopback interface.
Step 5	ipv6 enable Example: Router(config-if)# ipv6 enable	Enable IPv6 support under the loopback interface.
Step 6	ospfv3 1 ipv4 area <i>id</i> Example: Router(config-if)# ospfv3 1 ipv4 area 0	Enable loopback interface to participate in OSPFv3 routing.
Step 7	ospfv3 1 ipv6 area <i>id</i> Example: Router(config-if)# ospfv3 1 ipv6 area 0	Enable loopback interface to participate in OSPFv3 routing.

Configuring the OSPFv3 IPv4 Address Family Process

The OSPFv3 address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, you may have two device processes per interface, but only one process per AF. If the IPv4 AF is used, an IPv4 address must first be configured on the interface, but IPv6 must be enabled on the interface. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the same interface is not supported.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	router ospfv3 <i>process_id</i> Example: Router(config)# router ospfv3 1	Global configuration for OSPFv3.
Step 3	router-id <i>ipv4_address</i> Example: Router(config-router)# router-id 101.101.101.101	Router ID for OSPFv3.

	Command or Action	Purpose
Step 4	address-family ipv4 unicast Example: Router(config-router)# address-family ipv4 unicast	Adding address family for IPv4 unicast routing under global OSPFv3 configuration.
Step 5	redistribute connected metric value metric-type type Example: Router(config-router-af)# redistribute connected metric 1 metric-type	Redistribute metrics from external routing protocol.
Step 6	log-adjacency-changes Example: Router(config-if)# log-adjacency-changes	Logs all state changes.

Configuring the OSPFv3 IPv6 Address Family Process

The OSPFv3 address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, you may have two device processes per interface, but only one process per AF. If the IPv4 AF is used, an IPv4 address must first be configured on the interface, but IPv6 must be enabled on the interface. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the same interface is not supported.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	router ospfv3 process_id Example: Router(config)# router ospfv3 1	Global configuration for OSPFv3.
Step 3	router-id ipv4_address Example: Router(config-router)# router-id 101.101.101.101	Router ID for OSPFv3.
Step 4	address-family ipv6 unicast Example: Router(config-router)# address-family ipv6 unicast	Adding address family for IPv6 unicast routing under global OSPFv3 configuration.
Step 5	redistribute connected metric value metric-type type Example:	Redistribute metrics from external routing protocol.

	Command or Action	Purpose
	Router(config-router-af)# redistribute connected metric 1 metric-type	
Step 6	log-adjacency-changes Example: Router(config-if)# log-adjacency-changes	Logs all state changes.

Configuring IPv6 PIM Bootstrap Router (BSR)

The bootstrap router (BSR) protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected and the mapping tables will be modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	ipv6 pim bsr candidate bsr loopback_ipv6_address Example: Router(config)# ipv6 pim bsr candidate bsr 11::11	Configures a device to be a candidate BSR. Note Must use the loopback ipv6 address configured earlier.
Step 3	ipv6 pim bsr candidate rp loopback_ipv6_address Example: Router(config-router)# ipv6 pim bsr candidate rp 11::11	Configures a device to be a candidate Rendezvous Point (RP). Note Must use the loopback ipv6 address configured earlier.

Configuring IPv6 Multicast Group

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries--receivers can be located anywhere on the Internet or in any private network.

Procedure

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

	Command or Action	Purpose
	Router# configure terminal	
Step 2	interface <i>interface_name</i> Example: Router# interface Vlan 10	Creates and enters interface configuration mode.
Step 3	ipv6 mld join-group <i>multicast_group_address</i> Example: Router(config-if)# ipv6 mld join-group FF06:6::1	Configure IPv6 mld join group under interface.

Verifying Virtual Template Interface

This section shows examples of command output to verify your setup.

```
Router# show vtemplate
Virtual access subinterface creation is globally enabled

      Active      Active      Subint  Interface
      Interface  Subinterface  Capable  Type
      -----
Vt1           0           1  Yes  Serial

Usage Summary

                                Interface  Subinterface
                                -----  -----
Current Serial  in use                2           1
Current Serial  free                 0           1
Current Ether   in use                0           0
Current Ether   free                 0           0
Current Tunnel  in use                0           0
Current Tunnel  free                 0           0
Current VPN     in use                0           0
Current VPN     free                 0           0
Total                               2           2

Cumulative created                3           27
Cumulative freed                   0           26

Base virtual access interfaces: 2
Total create or clone requests: 3
Cancelled create or clone requests: 0
Cumulative create request waiting for sso resources: 0
Current request queue size: 0
Current free pending: 0
Current recycle pending: 0
Current ordered recycle pending: 0

Maximum request duration: 32 msec
Average request duration: 24 msec
Last request duration: 32 msec

Maximum processing duration: 32 msec
Average processing duration: 24 msec
Last processing duration: 32 msec
Router#
```

Verifying PPPoE Session Details

This section shows examples of command output to verify your setup.

```

Router-1#show pppoe session
    1 session in LOCALLY_TERMINATED (PTA) State
    1 session total

Uniq ID  PPPoE  RemMAC          Port      VT  VA   StateSID  LocMAC      VA-st      Type
-----  -
    2      1      000c.296f.c985  Gi0/0/0    1   Vi1.1    PTA      7c31.0e85.1e78
UP
Router#

Router-2#show pppoe session
    1 session in LOCALLY_TERMINATED (PTA) State
    1 session total

Uniq ID  PPPoE  RemMAC          Port      VT  VA   StateSID  LocMAC      VA-st      Type
-----  -
    2      1      000c.29a1.ae42  Gi0/0/0    1   Vi1.1    PTA      d478.9b5d.0200
UP
Router#

Router-1# show pppoe session packets all
Total PPPoE sessions 1

session id: 1
local MAC address: 7c31.0e85.1e78, remote MAC address: 000c.296f.c985
virtual access interface: Vi1.1, outgoing interface: Gi0/0/0
    67 packets sent, 67 received
    6488 bytes sent, 5908 received

PPPoE Flow Control Stats
Local Credits: 1953  Peer Credits: 65535  Local Scaling Value 65534 bytes
Credit Grant Threshold: 28000  Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 38  PADG Timer index: 89
PADG last rcvd Seq Num: 0
PADG last nonzero Seq Num: 89
PADG last nonzero rcvd amount: 0
PADG Timers: (ms)  [0]-1000  [1]-2000  [2]-3000  [3]-4000  [4]-5000
PADG xmit: 36 rcvd: 0
PADG xmit: 127926272 rcvd: 36
In-band credit pkt xmit: 0 rcvd: 0
Last credit packet snapshot
PADG xmit: seq_num = 38, fcn = 65535, bcn = 0
PADG rcvd: seq_num = 38, fcn = 1953, bcn = 65535
PADG rcvd: seq_num = 0, fcn = 0, bcn = 61
PADG xmit: seq_num = 61, fcn = 1952, bcn = 0
In-band credit pkt xmit: fcn = 0, bcn = 0
In-band credit pkt rcvd: fcn = 0, bcn = 0
==== PADQ Statistics ====
PADQ xmit: 0 rcvd: 0
Router-1#

Router-2# show pppoe session packets all
Total PPPoE sessions 1

session id: 1
local MAC address: d478.9b5d.0200, remote MAC address: 000c.29a1.ae42

```

```

virtual access interface: Vi1.1, outgoing interface: Gi0/0/0
    78 packets sent, 75 received
    7408 bytes sent, 6642 received

PPPoE Flow Control Stats
Local Credits: 1950   Peer Credits: 65535   Local Scaling Value 65534 bytes
Credit Grant Threshold: 28000   Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 42   PADG Timer index: 96
PADG last rcvd Seq Num: 0
PADG last nonzero Seq Num: 96
PADG last nonzero rcvd amount: 0
PADG Timers: (ms)   [0]-1000   [1]-2000   [2]-3000   [3]-4000   [4]-5000
PADG xmit: 40   rcvd: 0
PADG xmit: 127795200   rcvd: 40
In-band credit pkt xmit: 0   rcvd: 0
Last credit packet snapshot
  PADG xmit: seq_num = 42, fcn = 65535, bcn = 0
  PADG rcvd: seq_num = 42, fcn = 1953, bcn = 65535
  PADG rcvd: seq_num = 0, fcn = 0, bcn = 66
  PADG xmit: seq_num = 63, fcn = 1950, bcn = 0
  In-band credit pkt xmit: fcn = 0, bcn = 0
  In-band credit pkt rcvd: fcn = 0, bcn = 0
  ==== PADG Statistics ====
  PADG xmit: 0   rcvd: 0
Router-2#

```

Verifying BSR Election

This section shows examples of command output to verify your setup.

```

Router-1#show ipv6 pim bsr election
PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
  This system is the Bootstrap Router (BSR)
    BSR Address: 61::61
    Uptime: 00:05:20, BSR Priority: 0, Hash mask length: 126
    RPF: FE80::7E31:EFF:FE85:1E78,Loopback0
    BS Timer: 00:00:41
    This system is candidate BSR
    Candidate BSR address: 61::61, priority: 0, hash mask length: 126
Router-1#

Router-2#show ipv6 pim bsr election
PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
    BSR Address: 61::61
    Uptime: 00:01:22, BSR Priority: 0, Hash mask length: 126
    RPF: FE80::7E31:EFF:FE85:1E78,Virtual-Access1.1
    BS Timer: 00:01:47
    This system is candidate BSR
    Candidate BSR address: 41::41, priority: 0, hash mask length: 126
Router-2#

```

IPv6 Multicast Routing Table

This section shows examples of command output to verify your setup.



Note "*" in the source address indicates that it is a mld join request entries.

```

Router-1#show ipv6 mroute
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, Y - Joined MDT-data group,
       y - Sending to MDT-data group
       g - BGP signal originated, G - BGP Signal received,
       N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
       q - BGP Src-Active originated, Q - BGP Src-Active received
       E - Extranet
Timers: Uptime/Expires
Interface state: Interface, State

(A000::2, FF06:6::1), 00:01:45/00:01:44, flags: SFT
  Incoming interface: Vlan30
  RPF nbr: A000::2
  Immediate Outgoing interface list:
    Virtual-Access1.1, Forward, 00:01:45/00:02:48

Router-1#

Router-2# show ipv6 mroute
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT, Y - Joined MDT-data group,
       y - Sending to MDT-data group
       g - BGP signal originated, G - BGP Signal received,
       N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
       q - BGP Src-Active originated, Q - BGP Src-Active received
       E - Extranet
Timers: Uptime/Expires
Interface state: Interface, State

(*, FF06:6::1), 00:04:33/00:03:29, RP 41::41, flags: SCL
  Incoming interface: Tunnel2
  RPF nbr: 41::41
  Immediate Outgoing interface list:
    Vlan30, Forward, 00:04:33/00:03:29

(A000::2, FF06:6::1), 00:01:41/00:02:43, flags: ST
  Incoming interface: Virtual-Access1.1
  RPF nbr: FE80::7E31:EFF:FE85:1E78
  Immediate Outgoing interface list:
    Vlan30, Forward, 00:01:41/00:02:49
Router-2

```


IPv6 Multicast over PPPoE

This new feature applies to the ESR6300 Router.

PPPoE is a session/connection-oriented protocol, which extends the point-to-point radio frequency (RF) link from an external radio to an IOS router. Router communication with the radio is represented by virtual access interface (connectivity to a radio neighbor).

VMI operates in the Bypass mode where each Virtual Access Interface (VAI) represents a radio neighbor. The VMI layer re-directs unicast routing protocol traffic to the appropriate P2P link (Virtual-Access interface) and replicates any Multicast traffic that needs to flow.

For IPV6 multicast over PPPoE to function properly, the following must be configured:

- PPPoE (Virtual-template, VMI and physical interface)
- IPV6 unicast and multicast routing
- IPv6 PIM BSR
- IPv6 MLD



Note This feature requires the Network Advantage License.

For additional information, see the [IPv6 Multicast over PPPoE](#) chapter.

Verifying VMI Neighbors

This section shows examples of command output to verify your setup.

The Multicast for Virtual Multipoint Interfaces feature enables multicast support for RFC 5578-compliant Radio-Aware Routing (RAR). Multicast is defined as a network group membership spanning the entire network. The virtual multipoint interface (VMI) operates in aggregate mode, which means that all virtual access interfaces created by PPP over Ethernet (PPPoE) sessions are aggregated logically under the configured VMI. Packets sent to the VMI are forwarded to the correct virtual access interface. When a VMI operates in aggregate mode, the interfaces operate in nonbroadcast multiple access (NBMA) mode. Multicast traffic is forwarded only to the NBMA neighbors where a listener for that group is present.

```
Router-1#show vmi neighbor detail
      1 vmi1 Neighbors

vmi1  IPV6 Address=FE80::D678:9BFF:FE5D:200
      IPV6 Global Addr=:
      IPV4 Address=81.0.0.1, Uptime=00:03:16
      Output pkts=0, Input pkts=0
      METRIC DATA: Total rcvd=2, Avg arrival rate (ms)=10220
      CURRENT: MDR=2000000000000 bps, CDR=1000000000 bps
              Lat=1 ms, Res=100, RLQ=90, load=1
      MDR      Max=2000000000000 bps, Min=2000000000000 bps, Avg=2000000000000 bps
      CDR      Max=10000000000 bps, Min=10000000000 bps, Avg=10000000000 bps
      Latency  Max=1, Min=1, Avg=1 (ms)
      Resource Max=100%, Min=100%, Avg=100%
```

```

        RLQ      Max=90, Min=90, Avg=90
        Load     Max=1%, Min=0%, Avg=0%
Transport PPPoE, Session ID=2
INTERFACE STATS:
  VMI Interface=vml,
    Input qcount=0, drops=0, Output qcount=0, drops=0
  V-Access intf=Virtual-Access1.1,
    Input qcount=0, drops=0, Output qcount=0, drops=0
  Physical intf=GigabitEthernet0/0/0,
    Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
Local Credits: 1954   Peer Credits: 65535   Local Scaling Value 65534 bytes
Credit Grant Threshold: 28000   Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 198   PADG Timer index: 283
PADG last rcvd Seq Num: 0
PADG last nonzero Seq Num: 283
PADG last nonzero rcvd amount: 0
PADG Timers: (ms)   [0]-1000   [1]-2000   [2]-3000   [3]-4000   [4]-5000
PADG xmit: 196 rcvd: 0
PADG rcvd: 128057344 rcvd: 196
In-band credit pkt xmit: 0 rcvd: 0
Last credit packet snapshot
  PADG xmit: seq_num = 198, fcn = 65535, bcn = 0
  PADG rcvd: seq_num = 198, fcn = 1954, bcn = 65535
  PADG rcvd: seq_num = 0, fcn = 0, bcn = 105
  PADG xmit: seq_num = 109, fcn = 1951, bcn = 0
In-band credit pkt xmit: fcn = 0, bcn = 0
In-band credit pkt rcvd: fcn = 0, bcn = 0
==== PADQ Statistics ====
  PADQ xmit: 0 rcvd: 1
Router-1#

Router#

Router-2#show vmi neighbor detail
      1 vml Neighbors

vm1   IPV6 Address=FE80::7E31:EFF:FE85:1E78
        IPV6 Global Addr:::
IPV4 Address=71.0.0.1, Uptime=00:01:50
        Output pkts=0, Input pkts=0
        No Session Metrics have been received for this neighbor.
        Transport PPPoE, Session ID=1
INTERFACE STATS:
  VMI Interface=vml,
    Input qcount=0, drops=0, Output qcount=0, drops=0
  V-Access intf=Virtual-Access1.1,
    Input qcount=0, drops=0, Output qcount=0, drops=0
  Physical intf=GigabitEthernet0/0/0,
    Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
Local Credits: 1953   Peer Credits: 65533   Local Scaling Value 65534 bytes
Credit Grant Threshold: 28000   Max Credits per grant: 65535
Credit Starved Packets: 0
PADG xmit Seq Num: 112   PADG Timer index: 168
PADG last rcvd Seq Num: 0
PADG last nonzero Seq Num: 168
PADG last nonzero rcvd amount: 0
PADG Timers: (ms)   [0]-1000   [1]-2000   [2]-3000   [3]-4000   [4]-5000

```

```

PADG xmit: 110 rcvd: 0
PADC xmit: 127991808 rcvd: 110
In-band credit pkt xmit: 0 rcvd: 0
Last credit packet snapshot
  PADG xmit: seq_num = 112, fcn = 65535, bcn = 0
  PADC rcvd: seq_num = 112, fcn = 1953, bcn = 65535
  PADG rcvd: seq_num = 0, fcn = 0, bcn = 70
  PADC xmit: seq_num = 71, fcn = 1952, bcn = 0
  In-band credit pkt xmit: fcn = 0, bcn = 0
  In-band credit pkt rcvd: fcn = 0, bcn = 0
  ==== PADQ Statistics ====
  PADQ xmit: 0 rcvd: 0

```

Router-2#

Verifying OSPF Neighbor

This section shows examples of command output to verify your setup.

```

Router-1#sh ospfv3 neighbor | i FULL
102.102.102.102 0 FULL/ - 00:00:33 24 Virtual-Access1.1
102.102.102.102 0 FULL/ - 00:00:34 24 Virtual-Access1.1
Router-1

Router-2# sh ospfv3 neighbor | i FULL
sh ospfv3 neighbor | i FULL
101.101.101.101 0 FULL/ - 00:00:33 23 Virtual-Access1.1
101.101.101.101 0 FULL/ - 00:00:33 23 Virtual-Access1.1
Router-2#

```

Sample Running Configuration

The following output shows a sample configuration with areas of interest highlighted.

```

Router-1#show run
Building configuration...

Current configuration : 7911 bytes
!
! Last configuration change at 13:04:28 UTC Wed Jun 8 2022
!
version 17.9
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform hardware throughput level 250M
platform punt-keepalive disable-kernel-core
!
hostname Router-1
!
boot-start-marker
boot system flash bootflash:c6300-universalk9.17.09.01.SSA.bin
boot-end-marker
!
!
no logging console
no aaa new-model
!

```

```

!
login on-success log
ipv6 unicast-routing
ipv6 multicast-routing
!
!
subscriber templating
subscriber authorization enable
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-4073554590
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-4073554590
  revocation-check none
  rsakeypair TP-self-signed-4073554590
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-4073554590
  certificate self-signed 01
    30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 34303733 35353435 3930301E 170D3232 30363038 31313137
    31345A17 0D333230 36303731 31313731 345A3031 312F302D 06035504 03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 30373335
    35343539 30308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
    0A028201 0100C54E 860F73AC F0A9EBC7 2C6D1204 49099324 85989550 32CA9B91
    3B3A2492 AEA1D550 0CD787DE 09F6B64F 3F01C578 3EFB3995 E448904A 957EAFD9
    B82EF201 3A28BE26 6B1615DA 35B35BEA D4B7B20F 2D2A3EC2 C1F52281 349E88E5
    F2BCBA37 CA72D461 97D1E817 7493ED38 7C7C1035 F7231D4E F59FADF9 EE0EE5EE
    1FD73691 E93EBE8C 262DC8B1 0FA25BF0 C2F65BF9 C57A406A 9F9CF3D3 3E6888C3
    D6B533AB 0DA71037 6C94A385 CECA4DD9 A037C344 5B761E6D F3B8D47B 4093BED8
    E497D649 63436773 7BE5A718 331C7F08 31071542 03AE588C 08605CF7 CC7C7D6F
    967759FC E2A943FF 8AD70094 825AAD4B DC66FEC8 5B7F2CDA 24F148E1 51AF106E
    FE212C21 651B0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
    301F0603 551D2304 18301680 14F49EA0 C5E78BB1 F0EA55AD 4C580FB7 BF1AE35C
    50301D06 03551D0E 04160414 F49EA0C5 E78BB1F0 EA55AD4C 580FB7BF 1AE35C50
    300D0609 2A864886 F70D0101 05050003 82010100 2083EBC1 E760806B 12F0ACEF
    8FDE2E11 E5B88B62 B85B5835 AB1D2471 EA6FCC2D B28F5EE2 1969C233 DBB8C435
    D7BAD49C 7781E485 97D5B5D0 DD05A0EE 5352535F 1657BE78 64E6BBA8 B627618E
    49041DFB 4FE4D16C FA6857EF E6EEDFBC 2E25AF9E 852EDF71 3B65E55F 62AB1B1E
    8B842F51 DAD55DB5 8A5BF87B 91F540D2 02E8576E 5D4550EA E7FCB6D7 6AD0E92A
    EEA7544 01C4095A BB02DB3A D45D73EB 971974FF B5DED058 F2F3A0E1 23BD3441
    899CDFC2 A3B36E7D E72D4BDB 480B8347 C26D6AB9 E7E5A140 B20B7B1D 7AC24A2C
    A69124B3 49BF18AF C99EF2A5 C4F484CE 9E2A70C1 D1EA4250 6E0D858E BBCFC6C1
    4FF6E0BC EB190067 E86EC80D 5D149D6F 462CA857
  quit
crypto pki certificate chain SLA-TrustPoint
  certificate ca 01
    30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
    32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
    6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
    3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
    43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
    526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
    82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
    CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520

```

```

1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 COBD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
no license feature hseck9
license udi pid ESR-6300-CON-K9 sn FOC234304H3
license boot level network-advantage
memory free low-watermark processor 45135
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
mode none
!
!
vlan internal allocation policy ascending
!
policy-map type service pppoe_rar
pppoe service manet_radio
!
!
bba-group pppoe rar_group_1
virtual-template 1
service profile pppoe_rar
!
!
interface Loopback0
ip address 61.0.0.1 255.255.255.255
ipv6 address 61::61/128
ipv6 enable
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
!
interface GigabitEthernet0/0/0
media-type rj45
negotiation auto
ipv6 enable
pppoe enable group rar_group_1
!
interface GigabitEthernet0/0/1

```

```

no ip address
shutdown
negotiation auto
!
interface GigabitEthernet0/1/0
  switchport access vlan 30
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface Virtual-Template1
  mtu 1484
  ip unnumbered vmil
  no ip redirects
  ip tcp adjust-mss 1444
  load-interval 30
  no peer default ip address
  ipv6 enable
  ipv6 mtu 1484
  ospfv3 1 network manet
  ospfv3 1 hello-interval 10
  ospfv3 1 ipv4 area 0
  ospfv3 1 ipv6 area 0
!
interface Vlan1
no ip address
!
interface Vlan30
  ip address 192.168.10.1 255.255.255.0
  ipv6 address A000::1/64
  ipv6 enable
  ospfv3 1 ipv4 area 0
  ospfv3 1 ipv6 area 0
!
interface Async0/2/0
no ip address
encapsulation scada
!
interface vmil
  ip address 71.0.0.1 255.255.255.0
  ipv6 address FE80::7E31:EFF:FE85:1E78 link-local
  ipv6 address 71::71/64
  ipv6 enable
  physical-interface GigabitEthernet0/0/0
  mode bypass
!
router ospfv3 1
  router-id 101.101.101.101
!
  address-family ipv4 unicast
    redistribute connected metric 1 metric-type 1
    log-adjacency-changes
  exit-address-family

```

```

!
address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
exit-address-family
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
ipv6 pim bsr candidate bsr 61::61
ipv6 pim bsr candidate rp 61::61
!
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  stopbits 1
line 0/0/0
line 0/2/0
line vty 0 4
  login
  transport input ssh
line vty 5 14
  login
  transport input ssh
!
call-home
  ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
  ! the email address configured in Cisco Smart License Portal will be used as contact email
  address to send SCH notifications.
  contact-email-addr sch-smart-licensing@cisco.com
  profile "CiscoTAC-1"
    active
    destination transport-method http
!
end

```

Debug Commands

This section shows debug commands for PPPoE, VMI, Virtual Template, and Subscriber Service.

PPPoE

Command or Action	Purpose
Router# debug pppoe data	PPPoE data packets
Router# debug pppoe errors	PPPoE protocol errors
Router# debug pppoe events	PPPoE protocol events
Router# debug pppoe packets	PPPoE control packets

VMI

Command or Action	Purpose
Router# debug vmi bma	Display VMI bma debug
Router# debug vmi error	Display internal VMI anomalies detected
Router# debug vmi multicast	Display VMI multicast packets
Router# debug vmi neighbor	Display VMI neighbor transaction debugging
Router# debug vmi packet	Display VMI packet trace
Router# debug vmi pppoe	Display VMI PPPoE packet/activity debug
Router# debug vmi registries	Display VMI registry calls

Virtual Template

Command or Action	Purpose
Router# debug vtemplate cloning	Virtual Template cloning information
Router# debug vtemplate error	Virtual Template errors
Router# debug vtemplate event	Virtual Template events
Router# debug vtemplate subinterface	Virtual Template subinterface command

Subscriber Service

Command or Action	Purpose
Router# debug sss errors	Subscriber Service Switch Manager errors
Router# debug ssss event	Subscriber Service Switch Manager events



CHAPTER 21

Implementation Options

This section contains the following topics:

- [SFP Overview, on page 267](#)
- [Power over Ethernet, on page 268](#)
- [Working with External USB3.0, on page 271](#)

SFP Overview

The ESR6300 supports two WAN ports with RJ45 and optical/copper SFP ports.

The 2 Combo-WAN ports are g0/0/0 and g0/0/1. Each port can either be in Copper RJ45 or SFP mode, which is software configurable.

The SFP Ports have the following characteristics:

- Optical interface and Copper RJ45 are supported
- Whichever link is connected first is detected as default by software
- Auto-negotiation is supported for 10Mbps, 100Mbps and 1000Mbps
- Both Optical and Cu SFPs are supported, GE and FE alike
- Copper FE SFPs are not supported on ESR6300
- Auto-negotiation for 10Mbps, 100Mbps, 1000Mbps in full-duplex and half-duplex mode is supported. For half duplex, Cisco supports only 10Mbps and 100Mbps.
- Auto-select is supported. Whichever interface is detected first is selected. Typically fiber SFP will come up faster than RJ45 Copper, and is faster than Copper SFP.
- RJ45 to SFP mode conversion involves an interface reset (shut/no shut, interface DOWN/UP). The syslog can be observed accordingly.



Note Prior to release 17.2.1, Jumbo MTU support is not available on the ESR6300. MTU>1500 packets will be fragmented. From release 17.2.1 going forward, MTU support is 64 - 9216 on the interface. If there are bursts of fragmented traffic expected beyond the device Non-drop rate capability, software implements a throttling mechanism and transmits MAC Pause frames to the other end to reduce rate of traffic. To resume normal operation, arp has to sent again to re-negotiate. The default ip arp timeout is 14,000 seconds. In these rare case scenarios, it is recommended to have much shorter arp timeout configurations.

Supported SFPs are found in the ESR6300 Hardware Technical Guide here:

<https://www.cisco.com/c/en/us/td/docs/routers/embedded/6300/hardware/tech-guide/ESR6300-tech-guide.html#pgfId-106538>

SFP Command Line

To configure the WAN port as an RJ45 or an SFP:

```
Router#config terminal
Router(config)#config terminal
Router(config)#interface g0/0/{0|1}
Router(config-if)#media type ?
auto-select  Use whichever connector is attached
  rj45        Use RJ45 connector
  sfp         Use SFP connector
```

To configure auto-failover:

```
Router(config-if)#media-type {rj45|sfp} ?
auto-failover Automatic Fail over
<cr>          <cr>
```

To validate your changes, use the following commands.

If SFP is detected:

```
Router#show inventory
```

To see if your configuration has taken effect:

```
Router#show run int g0/0/{0|1}
```

To reload the gigabit ethernet module:

```
Router#hwmodule subslot 0/0 reload force
```

Power over Ethernet

Power over Ethernet (PoE) is typically used to power up Access points, IP Cameras and IP Phones connected to the device's Ethernet ports.

The ESR6300 supports Power over Ethernet (PoE and PoE+) on the 4 LAN ports. PoE is NOT supported on the WAN ports. The power allocation is as follows:

- Supply 30W (PoE+) per port simultaneously on 4 LAN ports

- Supply 15.4W (PoE) per port simultaneously on 4 LAN ports
- The system integrator must have a 120W power supply



Note The Powered Device (PD) will be detected if it is IEEE-compliance or a Cisco standard device. Support for CDP and LLDP is available for power negotiation, and must be enabled on the ESR6300.



Note CDP and/or LLDP must be enabled on the ESR6300, and the PD must support CDP and/or LLDP for the device to be able to negotiate power levels between 15 and 30 watts.

Device Detection and Power Allocation

The router will detect a Cisco Pre-standard or an IEEE-compliant PD when the PoE is enabled and the connected device is not being powered by an AC adapter.

After device detection, the router determines the power requirements based on power classification class. Depending on the available power in the power budget, the router determines if a port can be powered. The router initially allocates this power when it detects and powers the device. Power negotiation using CDP/LLDP protocols happens thereafter.

Maximum power budget for 4 LAN ports combined at any time is $30W \times 4 = 120W$. On reload the PoE ports are powered down.(i.e they are powered down at rommon stage).

CLI for PoE

This section describes the CLI to use for configuring and displaying PoE.

Before you configure Power over Ethernet (PoE), note the following:

- **show inventory** and **show diag** commands will not display details of the vendor/system integrator's PoE controller.
- **show run** command will not reflect the current PoE configuration.
- On connecting a PD, power negotiation happens almost instantly. However, it takes 3-5 minutes to reflect accurate statistics using **show power inline**
- The default software mode is PoE and not PoE+ to prevent overdraw.
- There is limited support for LLDP-MED and LLDP-MDI.



Note Implementation of PoE is a partner option. The integrator is responsible for proper implementation into the finished product, therefore, it may or may not be available.

To configure auto or off:

```
power inline auto | never
```

Configuration example:

```
Router#config terminal
Router#interface g0/1/<1,2,3,4>
Router(config-if)#power inline {auto|never}
```

To enable CDP:

```
Router#config terminal
Router(config)#cdp run
Router(config)#exit
```

To enable LLDP:

```
Router#config terminal
Router(config)#lldp run
Router(config)#exit
```

To Verify your configuration:

```
Router#show power inline
Available:120.0(w) Used:21.1(w) Remaining:98.9(w)

Interface Admin Oper      Power   Device                Class Max
-----
Gi0/1/0    auto   on       14.7    IP Phone 8865         4    30.0
Gi0/1/1    auto   on        6.3    IP Phone 8811         2    30.0
Gi0/1/2    auto   off       0.0     n/a                   n/a  30.0
Gi0/1/3    auto   off       0.0     n/a                   n/a  30.0
Router#
```

To show power on a particular interface:

```
Router#show power inline {interface-id}
```

Displays PoE status for a router for the specified interface.

```
show power inline interface-id detail
```

To show power consumption:

```
Router#show power
Main PSU :
  Total Power Consumption from 3.3V Line : 0.36
  Total Power Consumption from 5V Line : 6.20
  Configured Mode : N/A
  Current runtime state same : N/A
  PowerSupplySource : External PS
POE Module :
  Configured Mode : N/A
  Current runtime state same : N/A
  Total power available : 120 Watts
Router#
```

The list of commands for debugging PoE follows:

Command	Description
Debug ilpower controller	Display PoE controller debug messages

Command	Description
Debug ilpower event	Display PoE event debug messages
Debug ilpower port	Display PoE port manager debug messages
Debug ilpower powerman	Display PoE power management debug messages
Debug ilpower cdp	Display PoE CDP debug messages
Debug ilpower registries	Display PoE registries debug messages
Debug ilpower scp	Display PoE scp debug messages

Working with External USB3.0

The ESR6300 provides access to a single USB 3.0 Type A device.

External USB3.0

The following details are important when working with an external USB device:

- The USB is for storage only and can be gracefully mounted/unmounted using IOS CLI.
- The USB is accessible in ROMMON and IOS applications.
- USB device must have single partition, and in ext2, Fat16, or Fat32 format only.
- The user can copy files between usbflash0: to/from flash:/bootflash:
- In both ROMMON and IOS, use **dir usbflash0:** to view USB:



Caution No hot-plug support in rommon mode. On insertion of USB, reboot (rommon1>reset) to view usb.



Caution Cisco USBs are strongly recommended and are the only ones supported. Many generic USBs may not work. Some branded USBs which comply with protocol standards such as Kingston USB3.0 may work.

USB CLI Commands:

To access the USB file system through ROMMON, use the following command:

```
ROMMON>dir usbflash0:
```

To access the USB file system through IOS, use the following command:

```
Router#dir usbflash0:
```

To plug in and unplug the USB device gracefully, disable it first:

```
Router conf t
Router(config)#platform usb disable
```

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

To gracefully activate a mounted USB in IOS:

```
Router#no platform usb disable
Router#show platform usb status
USB enabled
```

The USB port could be considered a potential security risk. You may wish to disable it if it is not in use. To gracefully remove a USB when in IOS mode:

```
Router conf t
Router(config)#platform usb disable
Jun 4 05:44:52.339: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 removed
Router#show platform usb status
USB disabled
```

To re-enable USB port:

```
Router(config)#no platform usb disable
*Jun 4 05:45:20.890: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
Router#show platform usb status
USB enabled
```



CHAPTER 22

ROM Monitor Overview and Basic Procedures

This chapter provides an overview of ROM Monitor concepts and operations, and includes the following sections:

- [ROM Monitor Overview, on page 273](#)
- [Access ROM Monitor Mode, on page 274](#)
- [Displaying the Configuration Register Setting, on page 276](#)
- [Environment Variable Settings, on page 277](#)
- [Exiting ROM Monitor Mode, on page 278](#)

ROM Monitor Overview

The *ROM Monitor* is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a router. When you connect a terminal to the router that is in ROM Monitor mode, the ROM Monitor (`rommon 1>`) prompt is displayed.

During normal operation, users do not use ROM Monitor mode. ROM Monitor mode is used only in special circumstances, such as reinstalling the entire software set, resetting the router password, or specifying a configuration file to use at startup.

The *ROM Monitor software* is known by many names. It is sometimes called *ROMMON* because of the CLI prompt in ROM Monitor mode. The ROM Monitor software is also called the *boot software*, *boot image*, or *boot helper*. Although it is distributed with routers that use the Cisco IOS XE software, ROM Monitor is a separate program from the Cisco IOS XE software. During normal startup, the ROM Monitor initializes the router, and then control passes to the Cisco IOS XE software. After the Cisco IOS XE software takes over, the ROM Monitor is no longer in use.

Rommon mode only allows for image boot via Flash: or USB (`usbflash0:`). There is no option to netboot.

Rommon mode has limitations on the USB variants it supports.



Note Cisco USBs are strongly recommended, and test validation support is claimed for only Cisco USBs. Many generic USBs may not work. Some branded USBs which comply with protocol standards such as Kingston USB3.0 may work.

Environmental Variables and the Configuration Register

Two primary connections exist between ROM Monitor and the Cisco IOS XE software: the ROM Monitor environment variables and the configuration register.

The ROM Monitor environment variables define the location of the Cisco IOS XE software and describe how to load it. After the ROM Monitor has initialized the router, it uses the environment variables to locate and load the Cisco IOS XE software.

The *configuration register* is a software setting that controls how a router starts up. One of the primary uses of the configuration register is to control whether the router starts in ROM Monitor mode or Administration EXEC mode. The configuration register is set in either ROM Monitor mode or Administration EXEC mode as needed. Typically, you set the configuration register using the Cisco IOS XE software prompt when you need to use ROM Monitor mode. When the maintenance in ROM Monitor mode is complete, you change the configuration register so the router reboots with the Cisco IOS XE software.

Accessing ROM Monitor Mode with a Terminal Connection

When the router is in ROM Monitor mode, you can access the ROM Monitor software only from a terminal connected directly to the console port of the card. Because the Cisco IOS XE software (EXEC mode) is not operating, nonmanagement interfaces are not accessible. Basically, all Cisco IOS XE software resources are unavailable. The hardware is available, but no configuration exists to make use of the hardware.

Network Management Access and ROM Monitor Mode

It is important to remember that ROM Monitor mode is a router mode, not a mode within the Cisco IOS XE software. It is best to remember that ROM Monitor software and the Cisco IOS XE software are two separate programs that run on the same router. At any given time, the router runs only one of these programs, .

One area that can be confusing when using ROM Monitor and the Cisco IOS XE software is the area that defines the IP configuration for the Management Ethernet interface. Most users are comfortable with configuring the Management Ethernet interface in the Cisco IOS XE software. When the router is in ROM Monitor mode, however, the router does not run the Cisco IOS XE software, so that Management Ethernet interface configuration is not available.

When you want to access other devices, such as a TFTP server, while in ROM Monitor mode on the router, you must configure the ROM Monitor variables with IP access information.

Access ROM Monitor Mode

The following sections describe how to enter the ROMMON mode.

Checking the Current ROMMON Version

To display the version of ROMmon running on a router, use the **show rom-monitor** command . To show all variables that are set in ROMmon, use **show romvar**.

```
Router#show rom-monitor r0
System Bootstrap, Version 2.1(REL), RELEASE SOFTWARE
Copyright (c) 1994-2019 by cisco Systems, Inc
```

```
Router# show romvarROMMON variables:
PS1 = rommon ! >
```



```
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
THRPUT = 50
LICENSE_BOOT_LEVEL = network-essentials,network-stack:esg;
RET_2_RTS =
BSI = 0
RET_2_RCALTS =
RANDOM_NUM = 1027275747
```

Router# **reload**

Default manufacturing config-register value in rommon> is 0x102 [baud rate 9600]. If you would like to change the config-register value, it must be changed separately in both rommon> and IOS modes.

```
rommon 1 > set
PS1=rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
LICENSE_SUITE =
RET_2_RTS =
Diagnostic = 1
THRPUT =
USER_BOOT_PARAM = DEBUG_CONF=/bootflash/debug.conf
EULA_ACCEPTED = TRUE
BOOT_WDOG = DISABLE
LICENSE_BOOT_LEVEL =
BOOT = bootflash:sparrow_crashkernel.bin,1;
CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 1662155698
```

Commonly Used ROM Monitor Commands

The following table summarizes the commands commonly used in ROM Monitor. For specific instructions on using these commands, refer to the relevant procedure in this document.

Table 16: Commonly Used ROM Monitor Commands

ROMMON Command	Description
boot image	Manually boots a Cisco IOS XE software image.
boot image -o config-file-path	Manually boots the Cisco IOS XE software with a temporary alternative administration configuration file.
confreg	Changes the config-register setting.
dev	Displays the available local storage devices.
dir	Displays the files on a storage device.
reset	Resets the node.
set	Displays the currently set ROM Monitor environmental settings.
sync	Saves the new ROM Monitor environmental settings.
unset	Removes an environmental variable setting.

ROMMON Command Examples

The following example shows what appears when you enter the ? command on a router:

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
dev                  list the device table
dir                  list files in file system
help                 monitor builtin command help
history              monitor command history
meminfo              main memory information
repeat               repeat a monitor command
reset                system reset
set                  display the monitor variables
showmon              display currently selected ROM monitor
sync                 write monitor environment to NVRAM
token                display board's unique token identifier
unalias              unset an alias
unset                unset a monitor variable
```

Changing the ROM Monitor Prompt

You can change the prompt in ROM Monitor mode by using the **PS1=** command as shown in the following example:

```
rommon 8 > PS1="ESR6300 rommon ! > "
ESR6300 rommon 9 >
```

Changing the prompt is useful if you are working with multiple routers in ROM Monitor at the same time. This example specifies that the prompt should be “ESR6300 rommon ”, followed by the line number, and then followed by “>” by the line number.

Displaying the Configuration Register Setting

To display the current configuration register setting, enter the **confreg** command without parameters as follows:

```
rommon > confreg
Configuration Summary
(Virtual Configuration Register: )
enabled are:
[ 0 ] break/abort has effect
[ 1 ] console baud: 9600
boot:..... the ROM Monitor
do you wish to change the configuration? y/n [n]:
```

The configuration register setting is labeled *Virtual Configuration Register* . Enter the **no** command to avoid changing the configuration register setting.

Environment Variable Settings

The ROM Monitor environment variables define the attributes of the ROM Monitor. Environmental variables are entered like commands and are always followed by the equal sign (=). Environment variable settings are entered in capital letters, followed by a definition. For example:

```
IP_ADDRESS=10.0.0.2
```

Under normal operating conditions, you do not need to modify these variables. They are cleared or set only when you need to make changes to the way ROM Monitor operates.

This section includes the following topics:

Frequently Used Environmental Variables

The following table shows the main ROM Monitor environmental variables. For instructions on how to use these variables, see the relevant instructions in this document. The ESR6300 boot loader does not support netboot, so any setting like environment variables IP_ADDRESS, IP_SUBNET_MASK, DEFAULT_GATEWAY, TFTP_SERVER, TFTP_FILE are not used.

Table 17: Frequently Used ROM Monitor Environmental Variables

Environmental variable	Description
BOOT =path/file	Identifies the boot software for a node. This variable is usually set automatically when the router boots.

Displaying Environment Variable Settings

To display the current environment variable settings, enter the **set** command :

```
rommon 1 > showmon
System Bootstrap, Version 1.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

ESR 6300-K9 platform with 4188160 Kbytes of main memory

MCU Version - Bootloader: 4, App: 4
MCU is in application mode.
```

Entering Environment Variable Settings

Environment variable settings are entered in capital letters, followed by a definition. The following example shows the environmental variables that can be configured in ROMmon mode.:

```
rommon 1> confreg 0x0
rommon 1> BOOT_WDOG = DISABLE
rommon 1> BOOT = ESR6300-K9_image_name
```

Saving Environment Variable Settings

To save the current environment variable settings, enter the **sync** command:

```
rommon > sync
```



Note Environmental values that are not saved with the **sync** command are discarded whenever the system is reset or booted.

Exiting ROM Monitor Mode

To exit ROM Monitor mode, you must change the configuration register and reset the router.

Procedure

	Command or Action	Purpose
Step 1	confreg Example: rommon 1> confreg	Initiates the configuration register configuration prompts.
Step 2	Respond to each prompt as instructed.	See the example that follows this procedure for more information.
Step 3	reset Example: rommon 2> reset	Resets and initializes the router.

Configuration Example

```
rommon 3 > confreg
      Configuration Summary
      (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
boot: ..... the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
enable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
disable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]:
change the boot characteristics? y/n [n]:
      Configuration Summary
```

```
(Virtual Configuration Register: 0x0)
enabled are:
[ 0 ] break/abort has effect
[ 1 ] console baud: 9600
boot: ..... the ROM Monitor
do you wish to change the configuration? y/n [n]:
```

Upgrading the ROMMON for a Router

ROMMON upgrade on the ESR6300 router is automatically done when the image is booted. The latest version of the ROMMON is bundled with the IOS XE image. An algorithm detects if the current running version is older than the bundled version, if so, it is automatically upgraded. If the current running version is equal to the bundled version no upgrade is executed. For every successful upgrade, the router is automatically rebooted in order for the new version to get loaded and executed.:

-
- Step 1** (Optional) Run the **show rom-monitor slot** command on the router to see the current release numbers of ROMMON on the hardware. See the [Checking the Current ROMMON Version, on page 274](#) for information about interpreting the output of the command that you run.
- Step 2** If autoboot has not been enabled by using the **config-register 0x2102** command, run the **boot filesystem:/file-location** command at the ROMMON prompt to boot the Cisco IOS XE image, where *filesystem:/file-location* is the path to the consolidated package file. The ROMMON upgrade is not permanent for any piece of hardware until the Cisco IOS XE image is booted.
- Step 3** Run the **enable** command at the user prompt to enter the privileged EXEC mode after the boot is complete.
- Step 4** Run the **show rom-monitor slot** command to verify whether the ROMMON has been upgraded.
-



CHAPTER 23

Device Zeroization

This section contains the following topics:

- [Push Button, on page 281](#)
- [Device Zeroization, on page 282](#)

Push Button

There is no actual button on the ESR6300, and the system integrator must configure their platform with a Push Button. Reset on an ESR6300 does not cause the device to reboot, but initiates the configured level of zeroization.

- When the system is running in IOS mode, pressing this push button for 4+ seconds will cause files erase in flash, and will reset to factory-default mode on boot up.

The button must be pressed while the system is turned on at the same time.

The push button must continue to be held for more than 4 seconds after the power is turned on.

Config-reg setting is in NVRAM, and not changed by the button push.

Pressing the push button when in rommon mode has no effect.

Pressing the push button when in IOS mode causes a syslog message to appear and triggers a reload.

Pressing the push button for more than 4+ seconds after power up displays the following message when reset has been triggered:

```
System Bootstrap, Version 1.4(DEV) [vandvisv-vandvisv 113], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2019 by cisco Systems, Inc.
Compiled at Mon Jun 3 10:56:19 2019 by vandvisv
ESR-6300-CON-K9 platform with 4194304 Kbytes of main memory
MCU Version - Bootloader: 8, App: 10
MCU is in application mode.
Reset button push detected
```

How the router boots up depends on the following conditions:

- If there is a golden image in flash, the router will bootup with this image by default.
- If a golden image is not found, the router will be in rommon> mode as expected. Or, based on config-reg entry, may boot up first image in the flash:

Microcontroller Unit (MCU)

The MCU is part of the ESR6300 hardware. It performs the following functions:

- Monitors the Push button status at power up
- Monitors the system hardware watchdog output
- Maintains Reset Reason register
- Controls the SYS LED

The MCU versions are displayed using **show version**. Details on MCU version and upgrade status are also stored in Flash: as `boothelper.log`. The MCU is automatically upgraded by the software.

```
Router#show ver | i MCU
MCU bootloader version: 8
MCU application version: 10

Router#cat flash:boothelper.log
Logging at Fri Nov 15 05:00:54 Universal 2019
boot loader upgrade enabled
Bootloader is up-to-date
Current MCU App version is 10
MCU firmware is up-to-date
```

In the event the MCU Application is corrupt, or does not match the Release Notes version, this has to be repaired. Steps to recover from this state: Reload router, hit Ctrl+C to break into rommon mode.

```
Rommon>set MCU_UPGRADE=IGNORE - Ignore MCU firmware upgrade errors.
Rommon>sync
Rommon>reset
Rommon>boot bootflash:<image>
```

Once the MCU successfully upgrades, you can disable/unset this IGNORE option in rommon. Details on other MCU setting rommon options follow: (there are no available IOS configuration options or linux shell mode troubleshooting measures)

```
set MCU_UPGRADE=SKIP - Prevents MCU firmware upgrade from taking place.
set MCU_UPGRADE=FORCE - Forces MCU firmware upgrade to take place.
unset MCU_UPGRADE - Normal operation. Allows automatic upgrade
```

Device Zeroization

Zeroization consists of erasing any and all potentially sensitive information in the device.

This includes erasure of Main memory, cache memories, and other memories containing packet data, NVRAM, and Flash memory. The process of zeroization is launched upon the initiation of a user command and a subsequent trigger.

By default, the router will have the zeroization feature disabled. SPI: Flash, I2C, and ACT2 are not impacted by this feature.

When zeroization is functionally active, SYS LED indicates blinking yellow until the router reloads.

Zeroization can be triggered by the push button, or software-triggered by a privilege 15 user with console access. There is no remote access for security reasons. On triggering zeroization, the eMMC, NVRAM will be erased completely.

The zeroization process starts as soon as the push button is pressed down or the command is triggered.. The CLI command, "service declassify", is used to set the desired action in response to push button press. To prevent accidental erasure of the system configuration/image, the default setting is set to "no service declassify".



Note For complete details on how the process of zeroization works, see the [Cisco Embedded Service 6300 Series Router Hardware Technical Guide](#).

Zeroization Trigger

Zeroization can be triggered by either software or by the push button. In either case, there are a series of commands that need to be entered.

```
Router#config terminal
Router(config)#service declassify {erase-nvram | erase-all}
```

In the above example, erase-nvram will wipe only nvram, while erase-all will wipe bootflash: and nvram as well.

To confirm if the feature is enabled:

```
Router#show declassify
Declassify facility: Enabled=Yes In Progress=No
                    Erase flash=Yes Erase nvram=Yes
  Declassify Console and Aux Ports
  Shutdown Interfaces
  Reload system
```

To remove the feature, use the following command:

```
Router(config)#no service declassify
```

To Trigger Zeroization

To trigger the zeroization from the command line:

```
Router#declassify trigger
```

To trigger the zeroization from the push button, press and hold the button for 4+ seconds. When the system auto reloads, it will come up in ROMMON mode: "\$\$" with bootflash: wiped clean.

Important Notice about Zeroization

eMMC is a managed NAND. This means that our router system does not interact with the flash memory directly. The flash controller presents a block-style interface to our system, and it handles the flash management (analogous to the Flash Translation Layer). Our embedded router system cannot access the raw flash directly.

The JEDEC standard has commands that are supposed to remove data from the raw flash. In Cisco's implementation, the "Erase" and "Sanitize" commands are used. The eMMC standard JESD84-B51 defines "Sanitize" as follows:

The Sanitize operation is a feature ... that is used to remove data from the device according to Secure Removal Type. The use of the Sanitize operation requires the device to physically remove data from the unmapped user address space.

After the sanitize operation is completed, no data **should exist** in the unmapped host address space.



Warning Zeroization does NOT erase removable media such as SD Card and USB Storage. This media must be removed from the system and erased or destroyed using procedures that are outside the scope of this document.

Zeroize does a very thorough wipe of all non-protected parts of the eMMC flash using the best technology designed by the flash manufacturer today and can do so using the push of a button without the need for a console, ssh, or management session of any kind. It is the integrator's and end user's responsibility to determine the suitability regardless of the CLI keyword used to enable the feature.



Note While Cisco IOS and Cisco IOS-XE use the command line text of “declassify” in the command line interface (CLI) to enable the zeroize feature, in no way does this represent any specific endorsement or acknowledgment of a Government approved flash erasure methodology.

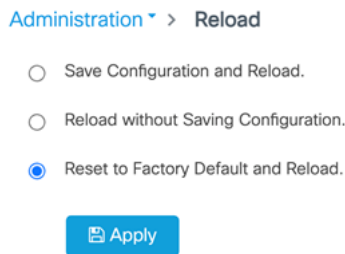
Declassification procedures are unique to each Government organization. Cisco solely provides the technical detail of the erasure operation here, not the policy distinction or any specific recommendation per classification.

Please refer to your respective Government Agency policies, procedures, and recommendations for the handling of sensitive data to see if this procedure meets with those requirements.

WARNING!

The CLI **service declassify erase-all** is literally a **software self-destruct mechanism** intended for defense and intelligence environments that attempts to wipe clean, all of the writable non-volatile storage on the device to clear the device configuration, other stored configurations and all security credentials including any additional license keys.

Please do not use this feature in lieu of doing a **write erase** from the CLI or from the Administration page, Reload option of the WebUI. Invoke the reload with the **Reset to Factory Default and Reload** option and click **Apply**. See the following figure.



If **service declassify erase-all** is invoked, after restoring the IOS-XE image and device configuration, you must re-license the device using the standard Cisco Smart Licensing procedures which ultimately require a Cisco Smart Account and access to the internet or a satellite license server.

Command Line Interface

There are two levels of zeroization actions, **erase-nvram** and **erase-all**. The following CLI shows the options:

```
device(config)#service declassify ?
erase-nvram    Enable erasure of device configuration as zeroization action. Default is no
erasure.
erase-all     Enable erasure of both flash and nvram file systems as part of zeroization.
Default is no erasure
```

The perma-locked bootable image(s) in the flash file system will still be available and can be used for booting the device.

The “erase-all” level of zeroization process erases the entire flash file system. This also wipes out all files and perma-locked bootable image(s). All interfaces are shut down before this process. Here, erasure of individual files in the flash file system is not possible and the only option is to erase the entire flash file system. This also erases packet data, ASIC data and processors related caches along with scrubbing Main memory.

With any level of zeroization, the device always fall back to the ROMMON prompt on the console after the erasure of configuration files or flash file system.

Zeroization Support in bootloader

The zeroization process may take several minutes, depending on several system parameters such as the size of DDR memory, EMMC disk size, etc.

It is possible that the zeroization may get interrupted by a power cycle before it completes. Since the primary OS image on EMMC itself gets purged during zeroization, it becomes impossible to continue zeroization after a power cycle. To solve this, zeroization support has been in the bootloader and will run it to completion even if it gets interrupted by power cycles.

Troubleshooting Zeroization

The following table shows troubleshooting tips for zeroization:

Table 18:

Symptoms	Troubleshooting
Upon zeroization, some files are still left behind in the bootflash:	In that case, collect logs to pass on to Cisco support/engineering teams for further debugging. Upon zeroization, the ideal state of the router should be in rommon mode displayed as \$. When executing \$dir bootflash:, the partition should not even be mounted.
How do you know if zeroization was triggered if the router is in \$\$ prompt?	Symptoms are bootflash: unmounted, router should be stuck in rommon and environment variables [rommon>set] should be wiped clean. There is no syslogging or reset reason displayed.

Symptoms	Troubleshooting
<p>Zeroization does not take effect on trigger.</p>	<p>Check MCU version: show ver I MCU. MCU application version should reflect the latest as per the Release Notes. If it is anything else, likely Application is corrupt and we need to re-trigger MCU upgrade.</p> <p>Capture the output from show platform declassify. Ensure you have actually enabled zeroization, before executing declassify trigger.</p> <p>Ensure you have privilege 15 to trigger zeroization.</p> <p>Ensure you are on console access. SSH/telnet remote session zeroization trigger is considered a security issue and is therefore disabled.</p>



CHAPTER 24

Call Manager Express

This section contains the following topics:

- [Call Manager Express Overview, on page 287](#)
- [SCCP Configuration Example, on page 287](#)
- [SCCP Show Command Example, on page 288](#)
- [SIP Configuration Example, on page 289](#)
- [Debug Commands, on page 290](#)
- [SIP Show Command Example, on page 290](#)

Call Manager Express Overview

Cisco Unified Communications Manager Express (formerly known as Cisco Unified Call Manager Express) is a call-processing application in Cisco IOS software that enables Cisco routers to deliver key-system or hybrid PBX functionality for enterprise branch offices or small businesses.

The Network-Advantage license is required for the CME feature on the ESR6300:

IP Phones are powered by ESR6300 LAN ports PoE/PoE+ and can negotiate power if they support the CDP/LLDP protocols.

There are several sources of information available for Call Manager Express:

- [Product Marketing Information](#)
- [Cisco Unified Communications Manager Express System Administrator Guide](#)
- [All of the Support Information](#)
- [Basic Configuration Guide for CUCME/CME](#)
- [Cisco Unified Communications Manager Express FAQ](#)

SCCP Configuration Example

Generate configuration files for SCCP Phones:

```
telephony-service
max-ephones 24
```

```

max-dn 200
ip source-address 192.168.8.15 port 2000
load 7945 term45.default.loads
!
!
ephone-dn 8
number 1008
name sccp-08
!
!
ephone-dn 9
number 1009
name sccp-09
!
ephone 8
device-security-mode none
mac-address 00A3.D1F3.6FAD
type 7945
button 1:8
!
!
ephone 9
device-security-mode none
mac-address 00A3.D1F3.6FC0
type 7945
button 1:9

```

SCCP Configuration tftp-server:

```

tftp-server bootflash:term45.default.loads
tftp-server bootflash:SCCP45.9-4-2SR3-1S.loads
tftp-server bootflash:cvm45sccp.9-4-2ES26.sbn
tftp-server bootflash:cnu45.9-4-2ES26.sbn
tftp-server bootflash:apps45.9-4-2ES26.sbn
tftp-server bootflash:jar45sccp.9-4-2ES26.sbn
tftp-server bootflash:dsp45.9-4-2ES26.sbn
!

```

SCCP Show Command Example

The following are two examples of SCCP:

```

Router#sh telephony-service ephone
Number of Configured ephones 2 (Registered 0)
ephone 8
Device Security Mode: Non-Secure
mac-address 00A3.D1F3.6FAD
type 7945
button 1:8
keepalive 30 auxiliary 30
actual keepalive 30 auxiliary 30
multicast-moh
max-calls-per-button 8
busy-trigger-per-button 0
Always send media packets to this router: No
Preferred codec: g711ulaw
conference drop-mode never
conference add-mode all
conference admin: No
privacy: Yes
privacy button: No

```

```

user-locale US
network-locale US
lpcor type:
lpcor (incoming):                (outgoing):
!
ephone 9
Device Security Mode: Non-Secure
mac-address 00A3.D1F3.6FC0
type 7945
button 1:9
keepalive 30 auxiliary 30
actual keepalive 30 auxiliary 30
multicast-moh
max-calls-per-button 8
busy-trigger-per-button 0
Always send media packets to this router: No
Preferred codec: g711ulaw
conference drop-mode never
conference add-mode all
conference admin: No
privacy: Yes
privacy button: No
user-locale US
network-locale US
lpcor type:
lpcor (incoming):                (outgoing):
!
Router#sh telephony-service ephone-dn

ephone-dn 8
number 1008
name sccp-08
preference 0 secondary 9
huntstop
call-waiting beep
no cti notify
no cti watch
ephone-dn 9
number 1009
name sccp-09
preference 0 secondary 9
huntstop
call-waiting beep
no cti notify
no cti watch

```

SIP Configuration Example

Generate Configuration Profiles for SIP Phones:

```

voice register global
mode cme
source-address 192.168.8.16 port 5060
max-dn 20
max-pool 15
load 8845 sip8845_65.12-5-1SR2-2.loads
tftp-path flash:
file text
create profile sync 0095724401230545
ntp-server 192.168.8.15 mode unicast
auto-register
!

```

```

voice register dn 2
number 202
call-forward b2bua busy 100
  call-forward b2bua noan 100 timeout 20
allow watch
name SIP-PHONE2
label 4085252002
voice register pool 2
busy-trigger-per-button 2
id mac 0045.1D86.F992
type 8845
number 1 dn 2
dtmf-relay sip-notify
codec g711ulaw

```

SIP Configuration TFTP-Server:

```

tftp-server flash:vc48845_65.12-5-1SR2-2.sbn
tftp-server flash:fb18845_65.BEV-01-006.sbn
tftp-server flash:kern8845_65.12-5-1SR2-2.sbn
tftp-server flash:rootfs8845_65.12-5-1SR2-2.sbn
tftp-server flash:sb28845_65.BEV-01-015.sbn
tftp-server flash:sip8845_65.12-5-1SR2-2.loads
!

```

Debug Commands

Two commands that are helpful in debugging are:

```

router#debug ccsip message
router#debug voice register event
router#
000313: *Jun 18 02:54:31.888: voice_reg_process_bulk_registration: preparing unsolicited
sharedln registration for 6010@28.18.88.70
000314: *Jun 18 02:54:31.888: voice_reg_process_bulk_registration: preparing unsolicited
sharedln registration for 6779@28.18.88.70
000315: *Jun 18 02:54:31.888: voice_reg_process_bulk_registration: preparing unot presence
registration for watcher [sip:6010@28.18.88.70] presentity [sip:6777@28.18.88.1]
000316: *Jun 18 02:54:31.888: voice_reg_process_bulk_registration: preparing unot presence
registration for watcher [sip:6010@28.18.88.70] presentity [sip:6506777@28.18.88.1]

```

SIP Show Command Example

The following are two examples of SIP:

```

Router#sh voice register global
CONFIG [Version=12.6]
=====
Version 12.6
Mode is cme
Auto-registration is enabled
Max-pool is 15
Max-dn is 20
Outbound-proxy is enabled and will use global configured value
Security Policy: DEVICE-DEFAULT
Forced Authorization Code Refer is enabled
Source-address is 192.168.8.16 port 5060
Load 8845 is sip8845_65.12-5-1SR2-2.loads

```



```
NTP Server Address is 192.168.8.15
NTP Server Mode is: unicast
Time-format is 12
Total SIP phones registered: 1
Total Registration Statistics
  Registration requests : 8
  Registration success  : 2
  Registration failed   : 0
  unRegister requests  : 1
  unRegister success    : 1
  unRegister failed     : 0
  Auto-Register requests : 0
  Attempts to register
    after last unregister : 0
  Last register request time : 11:29:38.113 PDT Mon Jul 8 2019
  Last unregister request time : 07:16:06.845 PDT Wed Jul 3 2019
  Register success time      : 11:29:38.113 PDT Mon Jul 8 2019
  Unregister success time    : 07:16:06.845 PDT Wed Jul 3 2019
```

```
Router#sh voice register dn 2
Dn Tag 2
Config:
  Number is 202
  Preference is 0
  Huntstop is disabled
  Name SIP-PHONE2
  Allow watch is enabled
  Auto answer is disabled
  Label is 4085252002
  call-forward b2bua busy 100
  call-forward b2bua noan 100 timeout 20
  Pool 2 has this DN configured for line 1
```




CHAPTER 25

Troubleshooting

This chapter contains the following topics:

- [Getting Started with Troubleshooting, on page 293](#)
- [Understanding Diagnostic Mode, on page 293](#)
- [Before Contacting Cisco or Your Reseller, on page 294](#)
- [show interfaces Troubleshooting Command, on page 294](#)
- [Software Upgrade Methods, on page 294](#)
- [Recovering a Lost Password, on page 295](#)

Getting Started with Troubleshooting

Before troubleshooting a software problem, you must connect a PC to the router via the console port. With a connected PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface by using Telnet. The Telnet option assumes that the interface is up and running.

Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.
- Provide methods of restarting the IOS or other processes.

- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

show interfaces Troubleshooting Command

Use the **show interfaces** command to display the status of all physical ports and logical interfaces on the router.

The ESR6300 supports the following interfaces:

GigabitEthernet combo ports 0/0/0 and 0/0/1

Gigabit Ethernet LAN ports g0/1/0-4

Pluggable Cellular Module 0/3/0 and 0/3/1

Software Upgrade Methods

Several methods are available for upgrading software on the Cisco ESR6300 Routers, including:

- Copy the new software image to flash memory over LAN or WAN when the existing Cisco IOS software image is in use.
- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.

- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.

Recovering a Lost Password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value.
5. If you have performed a **write erase**, or used the reset button, you will need to add the license.

```
Router#config term
Router#license smart reservation
```



Note Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.



Tip See the “Hot Tips” section on Cisco.com for additional information on replacing enable secret passwords.

Change the Configuration Register

To change a configuration register, follow these steps:

Step 1 Connect a PC to the CONSOLE port on the router.

Step 2 At the privileged EXEC prompt (*router_name #*), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

Example:

```
Router# show version
Cisco IOS XE Software, Version 17.01.01
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 19-Nov-19 06:19 by mcpre
```

```
(output omitted for brevity)
Configuration register is 0x2102
Router#
```

Step 3 Record the setting of the configuration register.

Step 4 To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Configuring the Configuration Register for Autoboot



Note Altering the configuration register is only for advanced troubleshooting and should only be done with guidance from Cisco support.

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the **config-reg 0x0** command.
- From the ROMMON prompt, use the **confreg 0x0** command.



Note Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

Reset the Router

To reset the router, follow these steps:

Step 1 If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (I) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

Note Some terminal keyboards have a key labeled *Break*. If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

Step 2 Press break. The terminal displays the following prompt:

Example:

```
rommon 2>
```

Step 3 Enter **confreg 0x142** to reset the configuration register:

Example:

```
rommon 2> confreg 0x142
```

Step 4 Initialize the router by entering the **reset** command:

Example:

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

Example:

```
--- System Configuration Dialog ---
```

Step 5 Enter **no** in response to the prompts until the following message is displayed:

Example:

```
Press RETURN to get started!
```

Step 6 Press **Return**. The following prompt appears:

Example:

```
Router>
```

Step 7 Enter the **enable** command to enter enable mode. Configuration changes can be made only in enable mode:

Example:

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

Example:

```
Router#
```

Step 8 Enter the **show startup-config** command to display an enable password in the configuration file:

Example:

```
Router# show startup-config
```

What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

Reset the Password and Save Your Changes

To reset your password and save the changes, follow these steps:

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **enable secret** command to reset the enable secret password in the router:

Example:

```
Router(config)# enable secret  
password
```

Step 3 Enter **exit** to exit global configuration mode:

Example:

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

Step 4 Save your configuration changes:

Example:

```
Router# copy running-config startup-config
```

Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

Step 1 Enter the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

Example:

```
Router(config)# config-reg  
value
```

Step 3 Enter **exit** to exit configuration mode:

Example:

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

Note To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

Step 4 Reboot the router, and enter the recovered password.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

Procedure

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>transport-map type console transport-map-name</p> <p>Example:</p> <pre>Router(config)# transport-map type console consolehandler</pre>	<p>Creates and names a transport map for handling console connections, and enters transport map configuration mode.</p>
Step 4	<p>connection wait [allow [interruptible] none [disconnect]]</p> <p>Example:</p> <pre>Router(config-tmap)# connection wait none</pre>	<p>Specifies how a console connection will be handled using this transport map.</p> <ul style="list-style-type: none"> • allow interruptible—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting. <p>Note Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.</p> <ul style="list-style-type: none"> • none—The console connection immediately enters diagnostic mode.
Step 5	<p>(Optional) banner [diagnostic wait] banner-message</p> <p>Example:</p> <pre>Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X Router(config-tmap)#</pre>	<p>(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.</p> <ul style="list-style-type: none"> • diagnostic—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration. <p>Note Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> • wait—Creates a banner message seen by users waiting for Cisco IOS VTY to become available. • <i>banner-message</i>—Banner message, which begins and ends with the same delimiting character.
Step 6	<p>exit</p> <p>Example:</p> <pre>Router(config-tmap)# exit</pre>	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	<p>transport type console console-line-number input transport-map-name</p> <p>Example:</p> <pre>Router(config)# transport type console 0 input consolehandler</pre>	<p>Applies the settings defined in the transport map to the console interface.</p> <p>The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the transport-map type console command.</p>

Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [all | name transport-map-name | type [console]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: console port (consolehandler):

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode
```

```
Router# show transport-map type console
Transport Map:
Name: consolehandler
```

```
REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

```
Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
```

```
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

Using the factory reset Commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
*Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.

***Return to ROMMON Prompt
```



CHAPTER 26

System Messages

This chapter contains the following sections:

- [Information About Process Management, on page 303](#)
- [How to Find Error Message Details, on page 303](#)

Information About Process Management

You can access system messages by logging in to the console through Telnet protocol and monitoring your system components remotely from any workstation that supports the Telnet protocol.

Starting and monitoring software is referred to as process management. The process management infrastructure for a router is platform independent, and error messages are consistent across platforms running on Cisco IOS XE. You do not have to be directly involved in process management, but we recommend that you read the system messages that refer to process failures and other issues.

How to Find Error Message Details

To show further details about a process management or a syslog error message, enter the error message into the Error Message Decoder tool at: <https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>.

For example, enter the message `%PMAN-0-PROCESS_NOTIFICATION` into the tool to view an explanation of the error message and the recommended action to be taken.

The following are examples of the description and the recommended action displayed by the Error Message Decoder tool for some of the error messages.

```
Error Message: %PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]
```

Explanation	Recommended Action
-------------	--------------------

The process lifecycle notification component failed, preventing proper detection of a process start and stop. This problem is likely the result of a software defect in the software subpackage.

Note the time of the message and investigate the kernel error message logs to learn more about the problem and see if it is correctable. If the problem cannot be corrected or the logs are not helpful, copy the error message exactly as it appears on the console along with the output of the **show tech-support** command and provide the gathered information to a Cisco technical support representative.

Error Message: %PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])

Explanation	Recommended Action
A process important to the functioning of the router has failed.	Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac . With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss . If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/ , or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the show logging and show tech-support commands and your pertinent troubleshooting logs.

Error Message: %PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])

Explanation	Recommended Action
-------------	--------------------

A process that does not affect the forwarding of traffic has failed.

Note the time of the message and investigate the kernel error message logs to learn more about the problem. Although traffic will still be forwarded after receiving this message, certain functions on the router may be disabled because of this message and the error should be investigated. If the logs are not helpful or indicate a problem you cannot correct, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <http://www.cisco.com/cisco/psn/bssprt/bss>. If you still require assistance, open a case with the Technical Assistance Center at: <http://tools.cisco.com/ServiceRequestTool/create/>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: %PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])

Explanation

The process has failed as the result of an error.

Recommended Action

This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <http://www.cisco.com/tac>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <http://www.cisco.com/cisco/psn/bssprt/bss>. If you still require assistance, open a case with the Technical Assistance Center at: <http://tools.cisco.com/ServiceRequestTool/create/>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: %PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.

Explanation	Recommended Action
A process failure is being ignored due to the user-configured debug settings.	If this behavior is desired and the debug settings are set according to a user's preference, no action is needed. If the appearance of this message is viewed as a problem, change the debug settings. The router is not expected to behave normally with this debug setting. Functionalities such as SSO switchover, router reloads, FRU resets, and so on will be affected. This setting should only be used in a debug scenario. It is not normal to run the router with this setting.

Error Message: %PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])

Explanation	Recommended Action
The process was restarted too many times with repeated failures and has been placed in the hold-down state.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac . With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss . If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/ , or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the show logging and show tech-support commands and your pertinent troubleshooting logs.

Error Message: %PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]

Explanation	Recommended Action
The route processor is being reloaded because there is no ready standby instance.	Ensure that the reload is not due to an error condition.

Error Message: %PMAN-3-RELOAD_RP : Reloading: [chars]

Explanation	Recommended Action
-------------	--------------------

The RP is being reloaded.

Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: %PMAN-3-RELOAD_SYSTEM : Reloading: [chars]

Explanation	Recommended Action
The system is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: %PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]

Explanation	Recommended Action
The executable file used for the process is bad or has permission problem.	Ensure that the named executable is replaced with the correct executable.

Error Message: %PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>

Explanation	Recommended Action
The executable file used for the process is missing, or a dependent library is bad.	Ensure that the named executable is present and the dependent libraries are good.

Error Message: %PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]

Explanation	Recommended Action
The executable file used for the process is empty.	Ensure that the named executable is non-zero in size.

Error Message: %PMAN-5-EXITACTION : Process manager is exiting: [chars]

Explanation	Recommended Action
The process manager is exiting.	Ensure that the process manager is not exiting due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: %PMAN-6-PROCSHUT : The process [chars] has shutdown

Explanation	Recommended Action
The process has gracefully shut down.	No user action is necessary. This message is provided for informational purposes only.

Error Message: %PMAN-6-PROCSTART : The process [chars] has started

Explanation	Recommended Action

The process has launched and is operating properly. No user action is necessary. This message is provided for informational purposes only.

Error Message: %PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless

Explanation	Recommended Action
The process has requested a stateless restart.	No user action is necessary. This message is provided for informational purposes only.



CHAPTER 27

Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

- [Monitoring Control Plane Resources, on page 309](#)
- [Monitoring Hardware Using Alarms, on page 314](#)
- [Approaches for Monitoring Hardware Alarms, on page 315](#)

Monitoring Control Plane Resources

The following sections explain the details of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

- [Avoiding Problems Through Regular Monitoring, on page 309](#)
- [Cisco IOS XE Process Resources, on page 309](#)
- [Overall Control Plane Resources, on page 313](#)

Avoiding Problems Through Regular Monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. It also establishes a baseline for a normal system load. You can use this information as a basis for comparison, when you upgrade hardware or software to see if the upgrade has affected resource usage.

Cisco IOS XE Process Resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the **show memory** command and the **show process cpu** command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do not include information for resources on the entire platform. When the **show memory** command is used in a system with 4 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

Router# **show memory**

Tracekey : 1#33e0077971693714bd2b0bc347d77489
Address Bytes Prev Next Ref PrevF NextF what Alloc PC

Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7F68ECD010 728952276 281540188 447412088 445683380 234766720
lsmpi_io 7F6852A1A8 6295128 6294304 824 824 412
Dynamic heap limit(MB) 200 Use(MB) 0

Processor memory

```
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68ECD010 0000000568 00000000 7F68ECD2A0 001 ----- *Init* :400000+60E37C4
7F68ECD2A0 0000032776 7F68ECD010 7F68ED5300 001 ----- Managed Chunk Q
:400000+60D12A8
7F68ED5300 0000000056 7F68ECD2A0 7F68ED5390 001 ----- *Init* :400000+3B0C610
7F68ED5390 0000012808 7F68ED5300 7F68ED85F0 001 ----- *Init* :400000+B8A5D64
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68ED85F0 0000032776 7F68ED5390 7F68EE0650 001 ----- List Elements
:400000+60A4A9C
7F68EE0650 0000032776 7F68ED85F0 7F68EE86B0 001 ----- List Headers :400000+60A4AD8
7F68EE86B0 0000032776 7F68EE0650 7F68EF0710 001 ----- IOSXE Process S
:400000+11924CC
7F68EF0710 0000032776 7F68EE86B0 7F68EF8770 001 ----- IOSXE Queue Pro
:400000+1192510
7F68EF8770 0000065544 7F68EF0710 7F68F087D0 001 ----- IOSXE Queue Bal
:400000+1192554
7F68F087D0 0000000328 7F68EF8770 7F68F08970 001 ----- *Init* :400000+B89E1D8
7F68F08970 0000000328 7F68F087D0 7F68F08B10 001 ----- *Init* :400000+B89E1D8
7F68F08B10 0000000328 7F68F08970 7F68F08CB0 001 ----- *Init* :400000+B89E1D8
7F68F08CB0 0000000360 7F68F08B10 7F68F08E70 001 ----- Process Events
:400000+60F9CD4
7F68F08E70 0000000056 7F68F08CB0 7F68F08F00 001 ----- SDB String :400000+605981C
7F68F08F00 0000000080 7F68F08E70 7F68F08FA8 001 ----- Init :400000+60599E4
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68F08FA8 0000036872 7F68F08F00 7F68F12008 001 ----- *Init* :400000+11891E8
7F68F12008 0000010008 7F68F08FA8 7F68F14778 001 ----- Platform VM Pag
:400000+11AD244
7F68F14778 0000002008 7F68F12008 7F68F14FA8 001 ----- *Init*
iosd_crb_sparrow_unix:7F8EB59000+5CC1C
7F68F14FA8 0000200712 7F68F14778 7F68F46008 001 ----- Interrupt Stack
:400000+11891E8
7F68F46008 0000003008 7F68F14FA8 7F68F46C20 001 ----- Watched Semapho
:400000+60FE448
7F68F46C20 0000000328 7F68F46008 7F68F46DC0 001 ----- *Init* :400000+B89E1D8
7F68F46DC0 0000000096 7F68F46C20 7F68F46E78 001 ----- Init :400000+60599E4
7F68F46E78 0000000216 7F68F46DC0 7F68F46FA8 001 ----- *Init* :400000+60ED228
7F68F46FA8 0000036872 7F68F46E78 7F68F50008 001 ----- *Init* :400000+11891E8
7F68F50008 0000000896 7F68F46FA8 7F68F503E0 001 ----- Watched Message
:400000+60FE4A8
7F68F503E0 0000002008 7F68F50008 7F68F50C10 001 ----- Watcher Message
:400000+60FE4D8
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68F50C10 0000000360 7F68F503E0 7F68F50DD0 001 ----- Process Events
:400000+60F9CD4
7F68F50DD0 0000000184 7F68F50C10 7F68F50EE0 001 ----- *Init* :400000+60ED918
7F68F50EE0 0000000112 7F68F50DD0 7F68F50FA8 001 ----- *Init* :400000+60B57CC
7F68F50FA8 0000036872 7F68F50EE0 7F68F5A008 001 ----- *Init* :400000+11891E8
7F68F5A008 0000002336 7F68F50FA8 7F68F5A980 001 ----- Process Array
:400000+6102A4C
7F68F5A980 0000000184 7F68F5A008 7F68F5AA90 001 ----- *Init* :400000+60ED918
```

```

7F68F5AA90 0000000184 7F68F5A980 7F68F5ABA0 001 ----- *Init* :400000+60ED918
7F68F5ABA0 0000000184 7F68F5AA90 7F68F5ACB0 001 ----- *Init* :400000+60ED918
7F68F5ACB0 0000000184 7F68F5ABA0 7F68F5ADC0 001 ----- *Init* :400000+60ED918
7F68F5ADC0 0000000184 7F68F5ACB0 7F68F5AED0 001 ----- *Init* :400000+60ED918

```

The **show process cpu** command displays Cisco IOS CPU utilization average:

```

Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 0 17 0 0.00% 0.00% 0.00% 0 Chunk Manager
2 552 1205 458 0.00% 0.00% 0.00% 0 Load Meter
3 0 1 0 0.00% 0.00% 0.00% 0 PKI Trustpool
4 0 1 0 0.00% 0.00% 0.00% 0 Retransmission o
5 0 1 0 0.00% 0.00% 0.00% 0 IPC ISSU Dispatc
6 36 13 2769 0.00% 0.00% 0.00% 0 RF Slave Main Th
7 0 1 0 0.00% 0.00% 0.00% 0 EDDRI_MAIN
8 0 1 0 0.00% 0.00% 0.00% 0 RO Notify Timers
9 4052 920 4404 0.23% 0.09% 0.06% 0 Check heaps
10 12 101 118 0.00% 0.00% 0.00% 0 Pool Manager
11 0 1 0 0.00% 0.00% 0.00% 0 DiscardQ Backgro
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
12 0 2 0 0.00% 0.00% 0.00% 0 Timers
13 0 163 0 0.00% 0.00% 0.00% 0 WATCH_AFS
14 0 2 0 0.00% 0.00% 0.00% 0 ATM AutoVC Perio
15 0 2 0 0.00% 0.00% 0.00% 0 ATM VC Auto Crea
16 76 3024 25 0.00% 0.00% 0.00% 0 IOSXE heartbeat
17 0 13 0 0.00% 0.00% 0.00% 0 DB Lock Manager
18 0 1 0 0.00% 0.00% 0.00% 0 DB Notification
19 0 1 0 0.00% 0.00% 0.00% 0 IPC Apps Task
20 0 1 0 0.00% 0.00% 0.00% 0 ifIndex Receive
21 36 1210 29 0.00% 0.00% 0.00% 0 IPC Event Notifi
22 72 5904 12 0.00% 0.00% 0.00% 0 IPC Mcast Penden
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
23 0 1 0 0.00% 0.00% 0.00% 0 Platform appsess
24 0 101 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
25 16 1210 13 0.00% 0.00% 0.00% 0 IPC Service NonC
26 0 1 0 0.00% 0.00% 0.00% 0 IPC Zone Manager
27 64 5904 10 0.00% 0.00% 0.00% 0 IPC Periodic Tim
28 76 5904 12 0.00% 0.00% 0.00% 0 IPC Deferred Por
29 0 1 0 0.00% 0.00% 0.00% 0 IPC Process leve
30 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat Manager
31 8 346 23 0.00% 0.00% 0.00% 0 IPC Check Queue
32 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat RX Cont
33 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat TX Cont
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
34 48 606 79 0.00% 0.00% 0.00% 0 IPC Keep Alive M
35 28 1210 23 0.00% 0.00% 0.00% 0 IPC Loadometer
36 0 1 0 0.00% 0.00% 0.00% 0 IPC Session Deta
37 0 1 0 0.00% 0.00% 0.00% 0 SENSOR-MGR event
38 4 606 6 0.00% 0.00% 0.00% 0 Compute SRP rate
39 0 1 0 0.00% 0.00% 0.00% 0 MEMLEAK PROCESS
40 0 1 0 0.00% 0.00% 0.00% 0 ARP Input
41 112 6331 17 0.00% 0.00% 0.00% 0 ARP Background
42 0 2 0 0.00% 0.00% 0.00% 0 ATM Idle Timer
43 0 1 0 0.00% 0.00% 0.00% 0 ATM ASYNC PROC
44 0 1 0 0.00% 0.00% 0.00% 0 CEF MIB API
--More--
...
show process cpu platform sorted

CPU utilization for five seconds: 11%, one minute: 12%, five minutes: 12%

```

```

Core 0: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 1: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 2: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 42%, one minute: 42%, five minutes: 42%
Pid PPid 5Sec 1Min 5Min Status Size Name
-----

```

```

18246 17700 34% 34% 34% S 272500 qfp-ucode-sparr
18297 16477 1% 1% 1% S 165768 fman_fp_image
9992 9121 1% 1% 1% S 743608 linux_iosd-imag
27122 26048 0% 0% 0% S 8460 nginx
26048 25864 0% 0% 0% S 19252 nginx
25928 1 0% 0% 0% S 2960 rotee
25864 1 0% 0% 0% S 3532 pman.sh
24212 2 0% 0% 0% S 0 kworker/u8:0
19648 8282 0% 0% 0% S 220 sleep
19635 10903 0% 0% 0% S 212 sleep
18121 17675 0% 0% 0% S 10968 ngiolite
17979 1 0% 0% 0% S 1660 rotee
17863 2 0% 0% 0% S 0 kworker/1:0
17859 1 0% 0% 0% S 2836 rotee
17737 17095 0% 0% 0% S 56828 iomd
17700 13380 0% 0% 0% S 3556 pman.sh
17675 12798 0% 0% 0% S 3524 pman.sh
17518 16854 0% 0% 0% S 15024 hman
17312 1 0% 0% 0% S 2828 rotee
17095 12798 0% 0% 0% S 3568 pman.sh
17085 1 0% 0% 0% S 2876 rotee
16942 2 0% 0% 0% S 0 kworker/0:1
16892 14768 0% 0% 0% S 108952 cpp_cp_svr
16854 13380 0% 0% 0% S 3568 pman.sh
16716 1 0% 0% 0% S 2996 rotee
16664 15963 0% 0% 0% S 51096 cpp_sp_svr
16477 13380 0% 0% 0% S 3540 pman.sh
16326 15536 0% 0% 0% S 39852 cpp_ha_top_leve
16270 1 0% 0% 0% S 2972 rotee
15963 13380 0% 0% 0% S 3528 pman.sh
15779 15163 0% 0% 0% S 55208 cpp_driver
15730 1 0% 0% 0% S 1640 rotee
15536 13380 0% 0% 0% S 3528 pman.sh
15412 1 0% 0% 0% S 1716 rotee
15274 14681 0% 0% 0% S 15004 hman
15163 13380 0% 0% 0% S 3624 pman.sh
15083 14361 0% 0% 0% S 26792 cman_fp
15057 1 0% 0% 0% S 1660 rotee
14891 1 0% 0% 0% S 2868 rotee
14768 13380 0% 0% 0% S 3568 pman.sh
14722 14127 0% 0% 0% S 27536 cmcc
14717 14108 0% 0% 0% S 15220 btman
14681 12798 0% 0% 0% S 3572 pman.sh
14627 1 0% 0% 0% S 2996 rotee
14361 13380 0% 0% 0% S 3596 pman.sh
14338 1 0% 0% 0% S 2984 rotee
14314 1 0% 0% 0% S 2824 rotee
14155 13577 0% 0% 0% S 15128 btman
14127 12798 0% 0% 0% S 3612 pman.sh
14108 13380 0% 0% 0% S 3572 pman.sh
13813 13380 0% 0% 0% S 252 inotifywait
--More--

```

Overall Control Plane Resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the **show platform software status control-processor brief** command (summary view) or the **show platform software status control-processor** command (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational, but that the operating level should be reviewed. Critical implies that the router is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

The following sections describe the fields in the **show platform software status control-processor** command output.

Load Average

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

Memory Utilization

Memory utilization is represented by the following fields:

- Total—Total system memory
- Used—Consumed memory
- Free—Available memory
- Committed—Virtual memory committed to processes

CPU Utilization

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts

- SIRQ—System Interrupts
- IOWait—Percentage of time CPU was waiting for I/O

show platform software status control-processor Command

The following are some examples of using the **show platform software status control-processor** command:

```
Router# show platform software status control-processor
RP0: online, statistics updated 4 seconds ago
Load Average: healthy
1-Min: 0.29, status: healthy, under 5.00
5-Min: 0.51, status: healthy, under 5.00
15-Min: 0.54, status: healthy, under 5.00
Memory (kb): healthy
Total: 4038072
Used: 2872136 (71%), status: healthy
Free: 1165936 (29%)
Committed: 2347228 (58%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.00, System: 0.70, Nice: 0.00, Idle: 97.88
IRQ: 0.30, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.70, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.30, SIRQ: 0.20, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.20, System: 1.11, Nice: 0.00, Idle: 98.27
IRQ: 0.40, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 8.23, System: 24.37, Nice: 0.00, Idle: 58.00
IRQ: 9.26, SIRQ: 0.11, IOWait: 0.00
```

```
Router# show platform software status control-processor brief
Load Average
Slot Status 1-Min 5-Min 15-Min
RP0 Healthy 0.28 0.46 0.52

Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
RP0 Healthy 4038072 2872672 (71%) 1165400 (29%) 2349820 (58%)

CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOWait
RP0 0 0.70 0.20 0.00 98.58 0.30 0.20 0.00
1 1.10 0.90 0.00 97.59 0.30 0.10 0.00
2 0.40 1.31 0.00 97.87 0.40 0.00 0.00
3 8.00 26.55 0.00 56.33 8.99 0.11 0.00
```

Monitoring Hardware Using Alarms

This section contains the following:

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use **show** commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Oct 6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded
[free space is 1429020 kB] - Please clean up files on bootflash.
```

Approaches for Monitoring Hardware Alarms

This section contains the following:

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

Enabling the logging alarm Command

The **logging alarm** command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC4133 (required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)



CHAPTER 28

Environmental Monitoring

This chapter contains the following sections:

- [Environmental Monitoring](#), on page 317
- [Environmental Monitoring](#), on page 317
- [Environmental Monitoring and Reporting Functions](#), on page 318
- [Environmental Monitoring Functions](#), on page 318
- [Environmental Reporting Functions](#), on page 319
- [SNMP Polling of Temperature OID](#), on page 325
- [Technical Assistance](#), on page 326
- [Additional References](#), on page 326

Environmental Monitoring

This chapter contains the following sections:

Environmental Monitoring

The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. The following are some of the key functions of the environmental monitoring system:

- Monitoring temperature of CPUs and Motherboard
- Recording abnormal events and generating notifications
- Monitoring Simple Network Management Protocol (SNMP) traps
- Generating and collecting Onboard Failure Logging (OBFL) data
- Sending call home event notifications
- Logging system error messages
- Displaying present settings and status

Environmental Monitoring and Reporting Functions

Monitoring and reporting functions allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

- [Environmental Monitoring Functions, on page 318](#)
- [Environmental Reporting Functions, on page 319](#)

Environmental Monitoring Functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

The router is expected to meet the following environmental operating conditions

- Non-operating Temperature: -40F to +185F (-40C to +85C)
- Non-operating Humidity: 5 to 95% relative humidity (non-condensing)
- Operating Temperature:
 - 40F to +185F (-40C to +85C) as measured at the center of the top surface of the –CON SKU thermal plate.
 - Temperature range of a completed solution depends on the enclosure thermal design characteristics used by the integrator.
 - If –NCP SKU is used, integrator is responsible for designing a thermal solution that meets the component level requirements provided in this document.
- Operating Humidity: 95% +/- 5% RH
- Operating Altitude: -15,000ft (4,572m)

The following table displays the levels of status conditions used by the environmental monitoring system.

Table 19: Levels of Status Conditions Used by the Environmental Monitoring System

Status Level	Description
Normal	All monitored parameters are within normal tolerance.
Warning	The system has exceeded a specified threshold. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
Critical	An out-of-tolerance temperature or voltage condition exists. Although the system continues to operate, it is approaching shutdown. Immediate operator action is required.

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

Temperature and Voltage Exceed Max/Min Thresholds

The following example shows the warning messages indicating the maximum and minimum thresholds of the temperature or voltage:

```
Warnings :
-----
For all the temperature sensors (name starting with "Temp:") above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

Environmental Reporting Functions

You can retrieve and display environmental status reports using the following commands:

- **show diag all eeprom**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform**
- **show platform diag**
- **show platform software status control-processor**
- **show diag slot R0 eeprom detail**
- **show version**
- **show power**

These commands show the current values of parameters such as temperature and voltage.

The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are shown below:

show diag all eeprom: Example

```
Router#show diag all eeprom
MIDPLANE EEPROM data:

Product Identifier (PID) : ESR-6300-NCP-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC23032UUN
Top Assy. Revision : 01
Hardware Revision : 0.2
Asset ID :
CLEI Code : UNASSIGNED
External PoE Module POE0 EEPROM data is not initialized
```

Internal PoE is not present

Slot R0 EEPROM data:

Product Identifier (PID) : ESR-6300-NCP-K9
 Version Identifier (VID) : V00
 PCB Serial Number : FOC23032UUN
 Top Assy. Revision : 01
 Hardware Revision : 0.2
 CLEI Code : UNASSIGNED
 Slot F0 EEPROM data:

Product Identifier (PID) : ESR-6300-NCP-K9
 Version Identifier (VID) : V00
 PCB Serial Number : FOC23032UUN
 Top Assy. Revision : 01
 Hardware Revision : 0.2
 CLEI Code : UNASSIGNED
 Slot 0 EEPROM data:

Product Identifier (PID) : ESR-6300-NCP-K9
 Version Identifier (VID) : V00
 PCB Serial Number : FOC23032UUN
 Top Assy. Revision : 01
 Hardware Revision : 0.2
 CLEI Code : UNASSIGNED
 SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : ESR-6300-2x1GE
 Version Identifier (VID) : V01
 PCB Serial Number :
 Top Assy. Part Number : 68-2236-01
 Top Assy. Revision : A0
 Hardware Revision : 2.2
 CLEI Code : CNUIAHSAAA
 SPA EEPROM data for subslot 0/1:

Product Identifier (PID) : ESR-6300-ES-4
 Version Identifier (VID) : V01
 PCB Serial Number :
 Top Assy. Part Number : 68-2236-01
 Top Assy. Revision : A0
 Hardware Revision : 2.2
 CLEI Code : CNUIAHSAAA
 SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 0/5 is not available

show environment: Example

```
Router#show environment
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0
```

Slot Sensor Current State Reading Threshold (Minor, Major, Critical, Shutdown)

```
-----
R0 Temp: LM75BXXX Normal 45 Celsius (75 ,80 ,90 ,na )(Celsius)
```

show environment all: Example

```
Router#show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: LM75BXXX R0 Normal 45 Celsius
```

show inventory: Example

```
Router#show inventory
+++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++

NAME: "Chassis", DESCR: "Embedded Services Router with 2 Gigabit Ethernet routed ports,4
Gigabit Ethernet switched ports, no cooling plate"
PID: ESR-6300-NCP-K9 , VID: V00 , SN: FOC23032UUN

NAME: "Power Supply Module 0", DESCR: "External Power Supply Module"
PID: PWR-12V , VID: , SN:

NAME: "module 0", DESCR: "Cisco ESR-6300-NCP-K9 Fixed and pluggable Interface Module
controller"
PID: ESR-6300-NCP-K9 , VID: , SN:

NAME: "NIM subslot 0/1", DESCR: "ESR-6300-ES-4"
PID: ESR-6300-ES-4 , VID: V01 , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 2 port Gigabitethernet Module"
PID: ESR-6300-2x1GE , VID: V01 , SN:

NAME: "module R0", DESCR: "Cisco ESR-6300-NCP-K9 Route Processor"
PID: ESR-6300-NCP-K9 , VID: V00 , SN: FOC23032UUN

NAME: "module F0", DESCR: "Cisco ESR-6300-NCP-K9 Forwarding Processor"
PID: ESR-6300-NCP-K9 , VID: , SN:
```

show platform: Example

```
Router#show platform
Chassis type: ESR-6300-NCP-K9

Slot Type State Insert time (ago)
-----
0 ESR-6300-NCP-K9 ok 07:30:08
0/0 ESR-6300-2x1GE ok 07:29:45
0/1 ESR-6300-ES-4 ok 07:29:45
R0 ESR-6300-NCP-K9 ok, active 07:31:20
F0 ESR-6300-NCP-K9 ok, active 07:31:20
P0 PWR-12V ok 07:30:46
```

show platform diag: Example

```

Router#show platform diag
Chassis type: ESR-6300-NCP-K9

Slot: 0, ESR-6300-NCP-K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:45 (07:30:11 ago)
Software declared up time : 00:01:16 (07:30:40 ago)
CPLD version :
Firmware version : 2.1(DEV) [vitu-vitu 127]

Sub-slot: 0/0, ESR-6300-2x1GE
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:02:07 (07:29:49 ago)
Logical insert detect time : 00:02:07 (07:29:49 ago)

Sub-slot: 0/1, ESR-6300-ES-4
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:02:07 (07:29:49 ago)
Logical insert detect time : 00:02:07 (07:29:49 ago)

Slot: R0, ESR-6300-NCP-K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:33 (07:31:24 ago)
Software declared up time : 00:00:33 (07:31:24 ago)
CPLD version : 00000000
Firmware version : 2.1(DEV) [vitu-vitu 127]

Slot: F0, ESR-6300-NCP-K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:33 (07:31:24 ago)
Software declared up time : 00:01:42 (07:30:14 ago)
Hardware ready signal time : 00:00:00 (never ago)
Packet ready signal time : 00:01:45 (07:30:11 ago)
CPLD version : 00000000
Firmware version : 2.1(DEV) [vitu-vitu 127]

Slot: P0, PWR-12V
State : ok
Physical insert detect time : 00:01:06 (07:30:50 ago)

Slot: GE-POE, Unknown
State : NA
Physical insert detect time : 00:00:00 (never ago)

```

show platform software status control-processor: Example

```

Router# show platform software status control-processor
RP0: online, statistics updated 9 seconds ago
Load Average: healthy
1-Min: 0.32, status: healthy, under 5.00
5-Min: 0.33, status: healthy, under 5.00

```



```

15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
Total: 3959840
Used: 2894588 (73%), status: healthy
Free: 1065252 (27%)
Committed: 2435656 (62%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 0.50, System: 0.91, Nice: 0.00, Idle: 98.07
IRQ: 0.40, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.81, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.20, SIRQ: 0.20, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.81, System: 2.65, Nice: 0.00, Idle: 95.41
IRQ: 1.12, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 7.66, System: 17.05, Nice: 0.00, Idle: 70.58
IRQ: 4.59, SIRQ: 0.10, IOWait: 0.00
Router#

```

show diag slot R0 eeprom detail: Example

```

Router#show diag slot R0 eeprom detail
Slot R0 EEPROM data:

EEPROM version : 4
Compatible Type : 0xFF
Controller Type : 3497
Hardware Revision : 0.2
PCB Part Number : 73-101841-01
Board Revision : 07
Deviation Number : 0
Fab Version : 01
PCB Serial Number : FOC23032UUN
Top Assy. Part Number : 068-102311-01
Top Assy. Revision : 01
Chassis Serial Number : FOC23032UUN
Deviation Number : 0
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Product Identifier (PID) : ESR-6300-NCP-K9
Version Identifier (VID) : V00
CLEI Code : UNASSIGNED
Manufacturing Test Data : 00 00 00 00 00 00 00 00
Field Diagnostics Data : 00 00 00 00 00 00 00 00
Chassis MAC Address : d478.9b5c.d680
MAC Address block size : 128
Asset ID :
Asset Alias :
Unknown Field (type 0086): 00 00 00 00
Asset ID :

```

show version: Example

```

Router# show version
Cisco IOS XE Software, Version 17.01.01
Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M), Version
 17.1.1, RELEASE SOFTWARE (fc1)

```

Technical Support: <http://www.cisco.com/techsupport>
 Copyright (c) 1986-2019 by Cisco Systems, Inc.
 Compiled Tue 19-Nov-19 06:19 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2019 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: IOS-XE ROMMON

Router uptime is 1 day, 49 minutes
 Uptime for this control processor is 1 day, 51 minutes
 System returned to ROM by reload
 System image file is "bootflash:c6300-universalk9.17.01.01.SPA.bin"
 Last reload reason: Reload Command

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	Technology-package Current	Technology-package Type	Technology-package Next reboot
network-stack	network-advantage	Smart License	network-advantage
dna-stack	dna-advantage	Smart License	dna-advantage

The current throughput level is 250000 kbps

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco ESR-6300-CON-K9 (1RU) processor with 705559K/6147K bytes of memory.
 Processor board ID FOC233501BF
 MCU bootloader version: 8
 MCU application version: 10
 1 Virtual Ethernet interface
 6 Gigabit Ethernet interfaces
 32768K bytes of non-volatile configuration memory.
 4194304K bytes of physical memory.

```
60542080K bytes of USB Flash at usbflash0:.
6500351K bytes of Bootflash at bootflash:.

Configuration register is 0x2102
```

show power: Example

```
Router# show power
Main PSU :
Total Power Consumption from 3.3V Line : 0.34
Total Power Consumption from 5V Line : 6.64
Configured Mode : N/A
Current runtime state same : N/A
PowerSupplySource : External PS
POE Module :
Configured Mode : N/A
Current runtime state same : N/A
Total power available : 120 Watts
```

SNMP Polling of Temperature OID

Support has been added for SNMP MIB to be able to return values from temperature sensors. The output should look similar to the **show environment** CLI.

The output of a **show environment** on an IR1101:

```
IR1101#show environment

Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0

Slot      Sensor      Current State  Reading
Threshold(Minor,Major,Critical,Shutdown)
-----
-----
R0        Temp: TS1    Normal         42    Celsius    (75 ,80 ,90 ,na ) (Celsius)
R0        Temp: TS2    Normal         37    Celsius    (75 ,80 ,90 ,na ) (Celsius)
```

The output from an snmpwalk would look similar to this:

```
[root@sg-centos-hv ~]# snmpwalk -v 2c -c public 33.33.33.204 1.3.6.1.4.1.9.9.13.1.3.1
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "Sensor 1"
SNMPv2-SMI::enterprises.9.9.13.1.3.1.3.1 = Gauge32: 48
SNMPv2-SMI::enterprises.9.9.13.1.3.1.4.1 = INTEGER: 93
SNMPv2-SMI::enterprises.9.9.13.1.3.1.5.1 = INTEGER: 0
SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.13.1.3.1.7.1 = INTEGER: 0
```

The ciscoEnvMonTemperatureStatusEntry oid is 1.3.6.1.4.1.9.9.13.1.3.1:

- ciscoEnvMonTemperatureStatusIndex (.1)
- ciscoEnvMonTemperatureStatusDescr (.2)
- ciscoEnvMonTemperatureStatusValue (.3)
- ciscoEnvMonTemperatureThreshold (.4)

- ciscoEnvMonTemperatureLastShutdown (.5)
- ciscoEnvMonTemperatureStatus (.6)

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Additional References

The following sections provide references related to the power efficiency management feature.

MIBs

MIBs	MIBs Link
CISCO-ENTITY-FRU-CONTROL-MIB	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator at: http://www.cisco.com/go/mibs.</p>



CHAPTER 29

Additional Information

This chapter contains the following sections:

- [Where to find Additional Information, on page 327](#)
- [Communications, Services, and Additional Information, on page 327](#)

Where to find Additional Information

The ESR6300 offers a rich IOS-XE feature set. This marketing data sheet provides a complete list of all of the features. <https://www.cisco.com/c/dam/en/us/products/routers/cisco-embedded-series-router-c78-742901.pdf>

Previous chapters in this guide provided an introduction to the ESR6300, as well as some of the basic configuration and feature differences for this product. The IOS-XE Operating System runs on numerous routing devices, and as such, has a wealth of additional configuration information.

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 DevNet](#).
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.