

# Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide

**First Published:** 2021-07-09

**Last Modified:** 2026-09-28

**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

© 2021–2026 Cisco Systems, Inc. All rights reserved.

# Full Cisco Trademarks with Software License

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

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

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

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

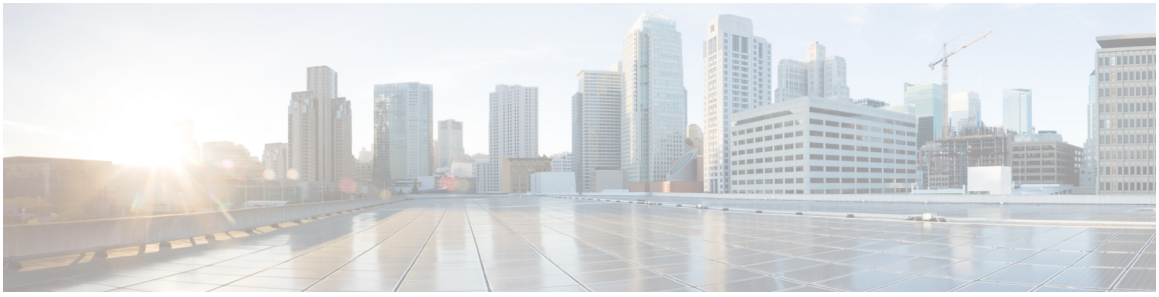
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

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

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

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



# CONTENTS


**Full Cisco Trademarks with Software License** iii

CHAPTER 1

**Overview** 1

Cisco Catalyst IR8140 Heavy Duty Series routers 1

Access CLI using a router console 2

Access the router using the console interface 3

Initial bootup security 4

Change the default password 4

Telnet and HTTP protocols 5

Remote console CLI access methods 6

Router console connections 6

Set up the IR8140H to run SSH 6

Access a console interface using telnet 8

CLI sessions 9

Change CLI session timeout 9

Lock a CLI session 10

CHAPTER 2

**New Features** 13

New features for Cisco IOS XE 26.2.1 13

New features for Cisco IOS XE 26.1.1 13

New features for Cisco IOS XE 17.18.2 13

New Features for Cisco IOS XE 17.16.1a 14

New Features for Cisco IOS XE 17.15.1a 14

New Features for Cisco IOS XE 17.14.1a 14

New features for Cisco IOS XE 17.8.1 14

IKEv2 for WPAN support 14
WPAN high availability support 14
Yang model for WPAN 15
Yang model for BBU 15
Yang model for GPS 16
Itron CAM Module support 16

CHAPTER 3 Using Cisco IOS XE software 17
Command modes 17
Keyboard shortcuts 19
CLI command forms 20
Using the history buffer to recall commands 20
Configuration files management 21
Saving configuration changes 21
Filter output from the show and more commands 21
Information about platforms and Cisco software images 22
Cisco feature navigator 23
Getting help 23
Finding command options examples 23
Software advisor 27
Software release notes 27

CHAPTER 4 Basic router configuration 29
IR8140H interface names 29
Verify basic configuration of router 30
Configure global parameters 36
Configure Gigabit Ethernet interface 37
Configure sub-interface on GigabitEthernet0/0/0 38
Configure a loopback interface 39
Cisco Discovery Protocol for security 40
Configure command-line access 40
Configure a static route 42
Configuring dynamic routes 44
Configure routing information protocol 44

Enhanced interior gateway routing protocol 45
Modular QoS CLIs 46
Configuring VLANs 46

CHAPTER 5 Configuring Secure Shell 47
Secure Shell 47
Prerequisites for configuring Secure Shell 47
Restrictions for configuring Secure Shell 47
SSH and router access 48
SSH servers, integrated clients, and supported versions 48
SSH configuration guidelines 49
How to Configure Secure Shell 49
Set up the IR8140H to run SSH 49
Configure the SSH server 51
SSH configuration and status commands 52
Configure the router for local authentication and authorization 52
Secure copy 54
Prerequisites for secure copy 54
Restrictions for configuring secure copy 55
Configure secure copy server 55
Additional references 56

CHAPTER 6 Software installation reference 57
Software installation requirements 57
Cisco software licenses 57
Consolidated packages 58
Network-Essentials packages 58
Network-Advantage packages 58
Related documentation 59
Install Cisco IOS XE release 59
ROMMON image software packages 61
File systems 61
Autogenerated file directories and files 62
Flash storage 63

Related documentation 63

CHAPTER 7 Software Maintenance Upgrade 65

Software Maintenance Upgrade package 65

SMU workflow requirements 66

Install a patch image 66

Uninstall patch image using rollback 68

Uninstall the patch image using deactivate, commit, and remove commands 70

CHAPTER 8 Smart Licensing Using Policy (SLP) 73

Smart licensing using policy on Cisco routers 73

CHAPTER 9 Battery Backup Unit (BBU) 75

Battery Backup Units 75

BBU mode configurations 75

Enable BBU 76

Disable BBU 76

Reset BBU 77

Enable or disable transportation mode on the router 78

Upgrade the BBU 79

CHAPTER 10 Tamper detection 83

Tamper detection scenarios 83

CHAPTER 11 Power Over Ethernet (PoE) 85

Power over Ethernet 85

Device detection and power allocations 85

Power budget calculation for router connected modules 86

Key considerations 86

Configure PoE using CLI 87

Verify PoE configuration 87

Debugging commands for PoE 89

CHAPTER 12 **Support for IRMH-5GS6-RC-GL UIM** 91

Support for IRMH-5GS6-RC-GL UIM 91

CHAPTER 13 **12V DC output for third party device** 93

12V DC outputs 93

CHAPTER 14 **NTP timing based on GPS clock** 95

Configure NTP using GPS time 95

CHAPTER 15 **vCPU and RAM distribution** 97

Introduction 97

Distribution of vCPU and RAM resources for Cisco IOx applications 97

Higher CPU and RAM allocation for IOx applications 98

Configure data plane heavy template 98

Verify the active vCPU and RAM distribution 99

Configure the Service Plane Heavy Template 100

Verify the active vCPU and RAM distribution 100

CHAPTER 16 **Cellular pluggable interface modules** 103

CHAPTER 17 **Configuring Cisco Resilient Mesh and the WPAN Module** 111

Cisco Resilient Mesh and WPAN modules 111

Configure the WPAN interface 112

Enable dot1x, mesh-security and DHCPv6 113

Configure IEEE154 settings 114

Configure group multicast 115

Configure RPL 116

Configure the power outage server 117

Configuring Cisco Resilient Mesh Security 117

Configure mesh key 117

Cisco Resilient Mesh Security configuration example 118

Verifying Cisco Resilient Mesh Security configuration 119

IPv6 multicast agents 121
Configure IR8100 as PIM6 router 122
Configure DTLS relay for EST 123
TLS Support Matrix 124
Mesh stack modes 124
Configure CG-Mesh stack mode 125
Configure Wi-SUN stack mode 126
Modulation and data rate 127
Limited Function Nodes 130
Direct parenting of LFN support in Wi-SUN mesh deployment 133
Verify WPAN 133
IR8100 basic WPAN configurations 134
Example of IR8100 configuration settings for CR-Mesh 135
ASR configuration example for CR-Mesh 139
Check and upgrade the WPAN firmware version 144
Upgrade WPAN firmware 145
Upgrade WPAN firmware (CG-Mesh to WiSUN) 146

CHAPTER 18 **DHCP Option 82** 147
DHCP Option 82 147
Prerequisites 148
Key considerations 149
Limitations 149
DHCP Option 82 packet flow 149
Hexadecimal pattern and suboption decoding 150
Configure DHCP Option 82 on server 151
Configure DHCP address pool 153
Configure DHCP relay agent 154
Configure relay chaining on relay agents 156
Verify DHCP Option 82 157
Debug DHCP Option 82 logs 157

CHAPTER 19 **IKEv2 and IPsec PFS Post Quantum Cryptography** 159
IKEv2 and IPsec PFS Post Quantum Cryptography 159

Benefits of PQC 160
Prerequisites 160
Limitations 160
Phased migration in Hub-and-Spoke deployments 161
ML-KEM algorithm and parameter sets 161
PFS negotiation behavior 162
Configure an IKEv2 proposal for PQC 162
Configure Perfect Forward Secrecy with PQC 164
Verify the PQC hybrid key exchange 165
Troubleshooting PQC hybrid key exchange 166

CHAPTER 20 **Post Quantum Cryptography for SSHv2 sessions** 167
Implementation of Post Quantum Cryptography 167
Overview 168
Factors to consider for deploying PQC 168
Protocol requirements 168
Restrictions for PQC 168
PQC negotiation scenarios 169
Configure PQC for SSHv2 sessions 169
Verify PQC for SSHv2 sessions 170
Key elements of PQC 170
Supported platforms 172

CHAPTER 21 **System messages** 173
Information about process management 173
How to Find Error Message Details 173

CHAPTER 22 **Environmental monitoring** 179
Environmental monitoring 179
Environmental monitoring 179
Environmental monitoring and reporting functions 179
Environmental monitoring functions 180
Environmental Reporting Functions 181
Additional references 187

Technical assistance 187

CHAPTER 23 **IOx application hosting 189**

Application hosting 189

Application hosting 189

Application hosting 189

IOx framework 190

Cisco application hosting 190

IOXMAN 190

Application hosting on the IR8100 industrial integrated services router 191

VirtualPortGroup 192

vNICs 193

Configure application hosting 194

Enable IOx 194

Configure a VirtualPortGroup to a Layer 3 data port 195

Install and uninstall apps 197

Override the app resource configuration 198

Verify the application hosting configuration 199

Configuration examples for application hosting 201

Example: Enable IOx 201

VirtualPortGroup configuration to a Layer 3 data port example 201

App installation and uninstallation commands 201

App resource configuration override example 201

Native docker support 202

Enable signed verification for Cisco signed applications 203

Cisco Cyber Vision and Edge Intelligence 203

Cisco ThousandEyes Enterprise Agent 204

CHAPTER 24 **Cisco SD-WAN support 205**

Cisco SD-WAN overview 205

Related documentation 206

CHAPTER 25 **ROM Monitor overview 207**

ROM Monitor overview and basic procedures 207

ROM Monitor 207
Access ROM Monitor mode 208
Check the current ROMmon version 208
Commonly used ROM Monitor commands 210
Examples 210
Change the ROM Monitor prompt 210
Display the configuration register setting 211
Environment variable settings 211
Frequently used environmental variables 212
Display environment variable settings 212
Environment variable settings 213
Save environment variable settings 213
Exit ROM Monitor mode 213
Configuration example 214
Upgrade the ROMmon for a router 214

CHAPTER 26 **WAN Monitoring** 217
WANMon 217
Built-in recovery actions 217
Prerequisites 218
Guidelines and limitations 219
Configure WANMon 219
Verify WANMon configuration 221
Configuration examples 221
WANMon cellular interface configuration example 221
Multiple WAN link monitoring example 222

CHAPTER 27 **Yang data models** 223
Support for YANG data models 223

CHAPTER 28 **Process health monitors** 225
Control plane resources 225
System process monitors 225
View Cisco IOS process resource 226

Overall Control Plane resources 227
Monitoring hardware using alarms 229
Router design and monitoring hardware 229
BootFlash Disk Monitoring 229
Approaches for monitoring hardware alarms 229
Viewing the console or syslog for alarm messages 229
Network management system alerts a network administrator when an alarm is reported through SNMP 229

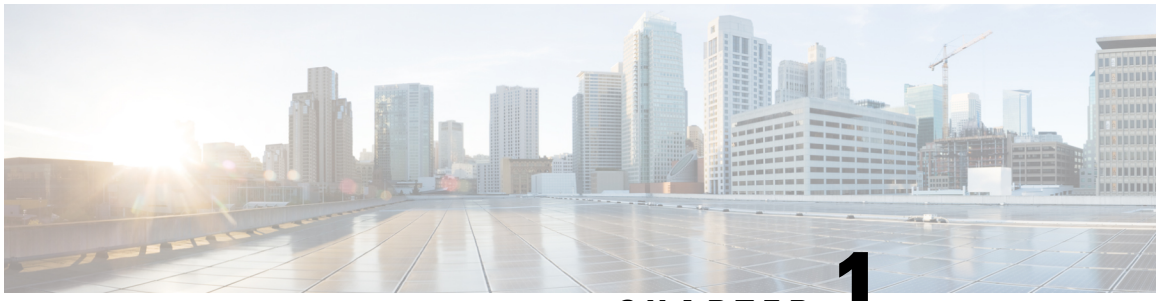
CHAPTER 29 **Unified Threat Defence** 231
Unified threat defense 231
Unified threat defense restrictions 232
License requirements for UTD features 232
References for unified threat defense configuration on IR8140 232

CHAPTER 30 **Cisco Network Plug and Play Agent** 233
Prerequisites for Cisco Network Plug and Play Agent 233
Restrictions for Cisco Network Plug and Play Agent 234
Information About Cisco Network Plug and Play Agent 234
Cisco Network Plug and Play Deployment Solution 234
Cisco Network Plug and Play Features 235
Cisco Network Plug and Play Agent Services and Capabilities 236
Software Maintenance Upgrade 238
Cisco Network Plug and Play Agent 239
Cisco Network Plug and Play Server 239
Cisco Network Plug and Play Agent Deployment 240
Cisco Network Plug and Play Agent Network Topology 241
Cisco Network Plug and Play Agent Initialization 241
Cisco Network Plug and Play Agent Deployment Solutions 242
Cisco Network Plug and Play Agent Discovery Process 242
Plug-n-Play Agent Deployment Protocol 247
Plug-n-Play Agent Security 248
Security Methods for the PnP Discovery Process 249
Self-Signed Certificate Based Authentication 249

Mobile Device Based Secured Installation 249
CA-Signed Certificate based Authentication 250
DHCP Option based Discovery over an IPv4 Network 250
DHCP Option based Discovery over an IPv6 Network 251
DNS-based Discovery 252
DNS-based Discovery over an IPv6 Network 253
Cisco Cloud Redirection over an IPv4 and IPv6 Network 253
Cisco Network PnP Discovery Over 4G Interface 254
Cisco Network PnP Discovery over a Management Interface 255
Cisco PnP over an EtherChannel 255
Security Methods for Post-PnP Discovery Process 255
Certificate Install Service 255
SUDI-based PnP Application Level Authentication 256
SUDI-based Client Certificate Validation 256
SUDI-based Serial Number 256
SUDI-Based Device Authentication 256
How to Configure Cisco Network Plug and Play Agent 258
Configuring Cisco Network Plug and Play Agent Profile 258
Configuring Network Plug and Play Agent Device 259
Configuring Cisco Network Plug and Play Reconnect Factor 259
Configuring Cisco Network Plug and Play HTTP Transport Profile 260
Configuring Cisco Network Plug and Play HTTPS Transport Profile 262
Configuring Backup Cisco Network Plug and Play Device 263
Configuring Backup Cisco Network Plug and Play Reconnect Factor 264
Configuring Backup Cisco Network Plug and Play HTTP Transport Profile 265
Configuring Backup Cisco Network Plug and Play HTTPS Transport Profile 266
Configuring Cisco Network Plug and Play Agent Tag 268
Troubleshooting and Debugging 269
Glossary 270
Additional References for Open Plug-n-Play Agent 270

CHAPTER 31 **Troubleshooting** 273
Troubleshooting 273
Diagnostic mode 273

Recommendation: prepare information before contacting support 274
Show interfaces troubleshooting command 274
Software upgrade methods 275
Change the configuration register 275
Configure the configuration register for autoboot 276
Reset the router 277
Recover a lost password 278
Reset the configuration register value 279
Configure a console port transport map 280
View console port, SSH, and telnet handling configurations 281
Factory reset commands 283



CHAPTER 1

# Overview

This document outlines the core characteristics and functional capabilities of the system to facilitate effective configuration and management.


- Cisco Catalyst IR8140 Heavy Duty Series routers, on page 1
- Access CLI using a router console, on page 2
- **Initial bootup security** , on page 4
- Remote console CLI access methods, on page 6
- CLI sessions, on page 9


# Cisco Catalyst IR8140 Heavy Duty Series routers

A Cisco Catalyst IR8140 Heavy Duty Router (IR8140H) is a next-generation, modular, IP66/67-rated industrial router that:

- is designed for outdoor use,
- features four external module slots plus two onboard WAN ports, and
- is available in two models: IR8140H-P-K9 (supports Power over Ethernet) and IR8140H-K9 (does not support PoE).

### Key points to consider

Consider these points before using this guide:

- The terms IR8140H , IR8100 , and router are used throughout this document in text and CLI examples to refer to the Cisco Catalyst IR8140 Heavy Duty Series Router, unless otherwise noted.
- The documentation set for this product strives to use bias-free language. For 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.

### Supported modules

The IR8140H Series features four external module slots plus two onboard WAN ports and supports:

- 60W PSU,
- GNSS onboard transceiver,
- 900MHz WPAN – OFDM/FSK,
- 4G/LTE IRMH modules, mSATA module,
- 1x 1GbE SFP WAN and 1x 1GbE Cu WAN,
- PoE (15W) – Supported only on the IR8140H-P-K9 PID,
- 12VDC_OUT port (Only available when PoE is not in use),
- Battery Backup Units (BBUs) – Up to 3,
- 2x Alarm ports (Digital IO).

# Access CLI using a router console

Cisco IR8140H routers have an RJ45 RS232 serial console port located on the CPU module. The default baud rate is 9600. You can use any RJ45 console cable that is available in the market.

On a device fresh from the factory, you are greeted with a System Configuration Dialog. 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.

**Note** Autoinstall will terminate if any input is detected on console.

### Procedure

**Step 1** Connect the RJ45 console cable to the router's RS232 serial console port on the CPU module.

**Step 2** Open a terminal emulator on your computer and configure it to use 9600 baud rate.

**Step 3** Power on the router and observe the console output. The System Configuration Dialog details are displayed as given in the example.

**Example:**

```
--- System Configuration Dialog ---
            Would you like to enter the initial configuration dialog? [yes/no]:
            WARNING: ** NOTICE ** This is the final IOS XE release to provide support for
the H.323 protocol. Consider switching to SIP for multimedia applications before upgrading
 to 17.6.1.
            *Jan 27 23:51:55.579: %TAMPER_ALARM-0-TAMPER_ALARM_ASSERT: Tamper alarm slot
(Tamper alarm slot 2) asserted
            *Jan 27 23:51:55.579: %TAMPER_ALARM-0-TAMPER_ALARM_ASSERT: Tamper alarm slot
(Tamper alarm slot 3) asserted
            Autoinstall trying DHCPv6 on GigabitEthernet0/0/0,GigabitEthernet0/0/1
```

```
            Autoinstall trying DHCPv4 on GigabitEthernet0/0/0,GigabitEthernet0/0/1
            AUTO IP is starting!!!!
            start Autoip process
            Acquired IPv4 address 192.168.0.202 on Interface GigabitEthernet0/0/0
            Received following DHCPv4 options:
            dns-server-ip : 192.168.0.2
            si-addr : 192.168.0.2
            hostname : Router
            stop Autoip process
            Press RETURN to get started!
            *Jan 27 23:53:08.903: %SYS-5-USERLOG_NOTICE: Message from tty0(user id: ):
Device in day0 workflow, some non user-configured options may be enabled by default
            *Jan 27 23:53:08.920: %SYS-5-CONFIG_P: Configured programmatically by process
PnP Agent Discovery from console as vty0
            OK to enter CLI now...
            pnp-discovery can be monitored without entering enable mode
            Entering enable mode will stop pnp-discovery
            *Jan 27 23:53:08.921: %PNP-6-HTTP_CONNECTING: PnP Discovery trying to connect
to PnP server (https://devicehelper.cisco.com.:443/pnp/HELLO)
            *Jan 27 23:53:29.880: %PNP-6-HTTP_CONNECTED: PnP Discovery connected to PnP
server (https://devicehelper.cisco.com.:443/pnp/HELLO)
            *Jan 27 23:53:30.893: %PNP-6-PNP_SUDI_UPDATE: Device SUDI
[PID:IR8140H-P-K9,SN:FDO2438J8UN] identified
          *Jan 28 00:02:43.494: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config
 Wizard)
            Interface IP-Address OK? Method Status Protocol
            GigabitEthernet0/0/0 192.168.0.202 YES DHCP up up
            GigabitEthernet0/0/1 unassigned YES unset administratively down down
            WPAN0/1/0 unassigned YES unset up up
            Router#
```

**Step 4** Press the **RETURN** key to get started and access the CLI prompt.

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

# Access the router using the console interface

Use this task to access the router's console interface and enter privileged EXEC mode to manage and configure the device through the CLI.

**Procedure**

**Step 1** Use the **enable** command to enable the router and enter privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Enter your system password when prompted. Skip this step if the enable password has not been configured. Once your password is accepted, the privileged EXEC mode prompt is displayed.

**Example:**

```
Password: enablepass
```

**Note** 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** Use the **quit** command to exit the console session.

**Example:**

```
Router> quit
```

### Initial bootup security

This reference provides guidance on enforcing default password changes and managing Telnet and HTTP access during initial device configuration.

- Enforce Changing Default Password
- Telnet and HTTP

# Change the default password

When the router is first booted after a factory reset or when it is new, you will receive a prompt on the console to enter the initial configuration dialog. Cisco recommends using the enable secret command instead of the enable password command for improved encryption.

### Procedure

**Step 1** Enter your response to the initial configuration dialog prompt on the console. If you choose no, the router proceeds with auto-install attempts and then prompts you to set the enable secret password.

**Example:**

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

**Step 2** Use the **enable secret** command to enter a new password when prompted to set the password.

**Example:**

```
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.
            ------------------------------------------------
            secret should be of minimum 10 characters with
            at least 1 upper case, 1 lower case, 1 digit and
            should not contain [cisco]
            ------------------------------------------------
            Enter enable secret: **********
            Confirm enable secret: **********
```

**Note** The initial dialog forces you to set a new enable password using the enable secret command. The password must be at least 10 characters, include upper and lower case letters, at least one digit, and must not contain the word "cisco". If a weak password is entered, you will be prompted again until a strong password is provided. You must enter the password twice for confirmation.

**Step 3** Save the configuration and complete the setup process by selecting option 2 to save the configuration to NVRAM and exit.

**Example:**

```
The following configuration command script was created:
            enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
            !
            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!
            Router> en
            Password:
            Router# sh run | inc sec
            enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
            Router#
```

**Note** After you save the configuration, you can access privileged EXEC mode using the new enable secret password. When you enter the password, it is masked, and the configuration will be encrypted and saved to NVRAM.

The router is now secured with a strong enable secret password, and the configuration is saved. You can proceed to further configure the router as needed.

# Telnet and HTTP protocols

Telnet and HTTP protocols are remote access protocols that:

- have modified default boot configurations as of release 17.5.1,
- are automatically configured during factory reset or initial boot processes, and
- include changes to telnet, HTTP server, HTTP client, SSH, and HTTPS server settings.

### Default configuration changes

For devices after a factory reset or when they are new from the factory, these events take place:

- Disable telnet.

- Disable http server.
- HTTP client works.
- Enable SSH.
- Enable https server.

# Remote console CLI access methods

A remote console CLI access method is a network-based approach that:

- enables remote access to the IR8100H CLI via Telnet or SSH,
- provides Telnet functionality that is disabled by default for security reasons, and
- offers SSH as the preferred and more secure method for remote CLI access.

## Router console connections

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

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.

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 .

## Set up the IR8140H to run SSH

To set up your device to run SSH, follow this procedure.

**Note** Configure user authentication for local or remote access. This step is required.

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Note** Enter password if prompted.

**Step 2** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **hostname** *hostname* command to configure a hostname for your device.

**Example:**

```
Router(config)# hostname your_hostname
```

**Note** You can follow this procedure only if you are configuring the device as an SSH server.

**Step 4** Use the **ip domain-name** *domain_name* command to configure a host domain for your device.

**Example:**

```
Router(config)# ip domain-name your_domain_name
```

**Step 5** Use the **crypto key generate rsa** command to enable the SSH server for local and remote authentication on the device and generate an RSA key pair.

**Example:**

```
Router(config)# crypto key generate rsa
```

**Note** You must follow this procedure only if you are configuring the device as an SSH server. Generating an RSA key pair for the device automatically enables SSH. A minimum modulus size of 1024 bits is recommended. 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.

**Step 6** Use the **end** command to exit to privileged EXEC mode.

**Example:**

```
Router(config)# end
```

**Step 7** Use the **show running-config** command to verify your entries.

**Example:**

```
Router# show running-config
```

**Step 8** (Optional) Use the **copy running-config startup-config** command to save your entries in the configuration file.

**Example:**

```
Router# copy running-config startup-config
```

# Access a console interface using telnet

Use this task to access a device's console interface using Telnet for CLI management and configuration.

**Procedure**

**Step 1** Use the **connect** *host* [*port*] [*keyword*] or **telnet** *host* [*port*] [*keyword*] command from your terminal or PC to connect to the router. 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.

**Example:**

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

**Note** For more information about these commands, see the Cisco IOS Terminal Services Command Reference document.

**Step 2** Enter your login password at the prompt. If no password is configured, press Return.

**Example:**

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

**Step 3** Use the **enable** command from user EXEC mode to enable the router and enter privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 4** Enter your system password at the password prompt.

**Example:**

```
Password: enablepass
```

**Step 5** The privileged EXEC mode prompt is displayed once the enable password is accepted.

**Example:**

```
Router#
```

**Step 6** Enter the necessary commands to complete specific tasks using the CLI access in privileged EXEC mode.

**Step 7** Use the **exit** or **logout** command to exit the Telnet session.

**Example:**

```
Router# logout
```

# CLI sessions

A CLI session is a command-line interface connection that:

- enables user access to system configuration and management functions,
- provides mechanisms to control user access and protect system resources, and
- prevents conflicts during concurrent user interactions.

### CLI session management features

CLI sessions include the following management features:

- **Inactivity timeout**: Can be configured and enforced to automatically end idle sessions.
- **Session locking**: Prevents two users from overwriting each other's changes.
- **Reserved capacity**: Spare capacity is reserved for CLI session access to ensure users can connect even when the system is under load.

# Change CLI session timeout

Setting the CLI session timeout increases the security of a CLI session by automatically ending idle sessions after a specified period of inactivity.

### Procedure

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **line console** *console-number* command to access the configuration mode for the console line of the router.

**Example:**

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

**Step 3** Use the **session-timeout** [*minutes*] command to set the session timeout. The value of *minutes* sets the amount of time that the CLI waits before timing out. Specify a value of 0 for *minutes* to disable session timeout.

**Example:**

```
Router(config-line)# session-timeout 10
```

**Step 4** Use the **show line console** *console-number* command to verify the value to which the session timeout has been set, which is shown as the value for idle session.

**Example:**

```
Router# show line console 0
```

# Lock a CLI session

To configure a temporary password on a CLI session, use the lock command in EXEC mode. The line is first configured as lockable, and then the lock command is used to assign a temporary password.



**Note** Before you can use the lock command, you need to configure the line using the lockable command.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **line console** *line-number* command to enter the line upon which you want to be able to use the lock command.

**Example:**

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

**Step 3** Use the **lockable** command to enable the line to be locked.

**Example:**

```
Router(config)# lockable
```

**Step 4** Use the **exit** command to exit the configuration mode.

**Example:**

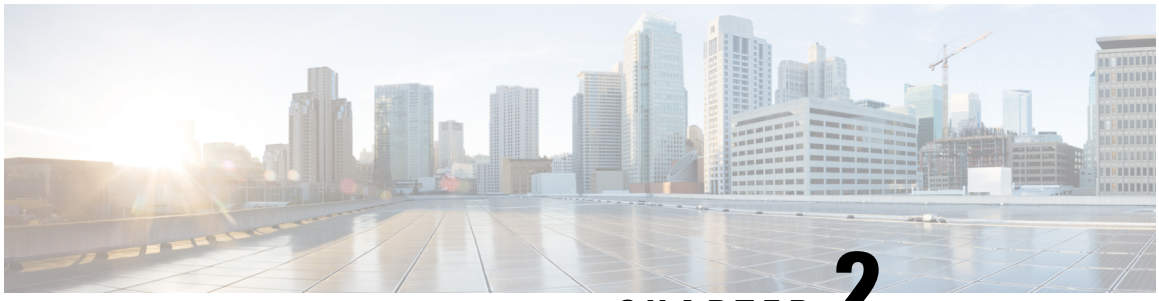
```
Router(config)# exit
```

**Step 5** Use the **lock** command to lock the CLI session. The system prompts you for a password, which you must enter twice.

**Example:**

```
Router# lock
Password: <password>
```

```
Again: <password>
Locked
```



CHAPTER 2

# New Features

This document provides an overview of the new features available in the system.


- New features for Cisco IOS XE 26.2.1, on page 13
- New features for Cisco IOS XE 26.1.1, on page 13
- New features for Cisco IOS XE 17.18.2, on page 13
- New Features for Cisco IOS XE 17.16.1a, on page 14
- New Features for Cisco IOS XE 17.15.1a, on page 14
- New Features for Cisco IOS XE 17.14.1a, on page 14
- New features for Cisco IOS XE 17.8.1, on page 14


## New features for Cisco IOS XE 26.2.1

This reference identifies the new features available in Cisco IOS XE 26.2.1 release.

New features in this release are:

- DHCP Option 82
- IKEv2 and IPsec PFS Post Quantum Cryptography
- Post Quantum Cryptography for SSHv2 sessions

## New features for Cisco IOS XE 26.1.1

This reference identifies the new features available in Cisco IOS XE 26.1.1 release.

New features in this release are:

- Power Over Ethernet (PoE)
- Unified Threat Defence

## New features for Cisco IOS XE 17.18.2

New features in this release are:

- Cisco ThousandEyes Enterprise Agent
- Common HSEC License

# New Features for Cisco IOS XE 17.16.1a

This document outlines the new features available in the Cisco IOS XE 17.16.1a release.

- Monitoring Radio Signal Parameters and GPS Coordinates of Cellular Telemetry using Syslog Messages

# New Features for Cisco IOS XE 17.15.1a

This document lists the new features available in the Cisco IOS XE 17.15.1a release.

This new feature is available in this release:

- Higher CPU and RAM Allocation for IOx Applications

# New Features for Cisco IOS XE 17.14.1a

This document lists the new features available in the Cisco IOS XE 17.14.1a release.

- Direct Parenting of LFN Support in Wi-SUN Mesh Deployment

# New features for Cisco IOS XE 17.8.1

This reference provides information about the new features available in Cisco IOS XE 17.8.1 release.

## IKEv2 for WPAN support

IKEv2 for WPAN support is a routing capability that:

- enables IKEv2 dynamic routing from Cisco IOS-XE Release 17.8.1 on the IR8140H router,
- allows redistribution of WPAN external routes (such as MAP-T routes) into IKEv2, and
- supports both spoke and hub distribution models.

## WPAN high availability support

WPAN high availability support is a redundancy feature that:

- enables high availability for WPAN between two IR8140H routers, each with one WPAN module,
- uses HSRP to track state between the two routers, and

- synchronizes WPAN state (RPL routes, mesh-security sessions and keys, multicast sequence numbers) between the two routers using a reliable UDP based protocol.

### WPAN high availability limitations

WPAN HA has specific implementation constraints:

- WPAN HA will not integrate with the rest of the IOS XE HA infrastructure. It is specific to WPAN.
- WPAN HA will only be supported between two IR8140 routers with a single WPAN interface each.
- This feature cannot be used together with the Dual WPAN interface feature.



**Note** WPAN HA will not integrate with the rest of the IOS XE HA infrastructure. It is specific to WPAN. WPAN HA will only be supported between two IR8140 routers with a single WPAN interface each. This feature cannot be used together with the Dual WPAN interface feature.

# Yang model for WPAN

A Yang model for WPAN is an operational model that provides Yang operational model support for information available through WPAN show commands.

### Available commands

Yang operational model support includes commands for:

- The WPAN interface (for example, **show wpan 0/X/0**)
- RPL commands (for example, **show wpan 0/X/0 rpl**)
- meshsec (for example, **show mesh-security**)

Cisco IOS-XE Yang Data Models are found here:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.8.1 release is found under 1781.

# Yang model for BBU

A Yang model for BBU is a data model that:

- provides operational model support for Battery Backup Unit (BBU) information,
- enables access to BBU information currently available via show commands, and
- follows Cisco IOS-XE Yang Data Model standards.

### Yang model availability

The Yang operational model support has been added for the Battery Backup Unit (BBU) information currently available via show commands. For example, **show platform hardware battery**.

For more details on Cisco IOS-XE Yang Data Models, see
https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.8.1 release is found under 1781.

# Yang model for GPS

A Yang model for GPS is an operational model that provides structured access to GNSS information through standardized data formats instead of traditional show commands.

### Yang model implementation details

Yang operational model support will be added for GNSS information currently available via show commands.

For example, **show platform hardware gnss**

Cisco IOS-XE Yang Data Models are found here:

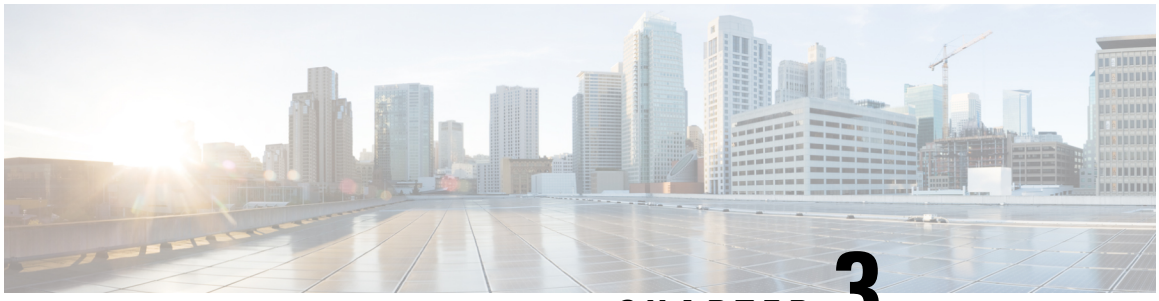
https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.8.1 release is found under 1781.

# Itron CAM Module support

The IR8140 supports third party modules from Cisco IOS-XE Release 17.8.1.

Before inserting the 3rd-party module, use the CLI **hw-module subslot 0/1 3rdparty-mode** to configure the slot as 3rd-party mode, to avoid delays during boot caused by the system looking for ACT2, which does not exist on a 3rd-party module.



CHAPTER 3

# Using Cisco IOS XE software

This reference outlines the fundamental components and operational capabilities of the Cisco IOS XE software.


- Command modes , on page 17
- Keyboard shortcuts, on page 19
- CLI command forms, on page 20
- Using the history buffer to recall commands, on page 20
- Configuration files management, on page 21
- Saving configuration changes, on page 21
- Filter output from the show and more commands, on page 21
- Information about platforms and Cisco software images, on page 22


## Command modes

The command modes available in Cisco IOS XE are the same as those in traditional Cisco IOS. Access Cisco IOS XE software using the CLI, which is divided into several modes. The commands available depend on the current mode. To see the available commands for each mode, you can enter a question mark **?** at the CLI prompt.

### EXEC mode

After logging in to the CLI, you enter user EXEC mode, which provides access to a limited set of commands. To access all commands, enter privileged EXEC mode using a password.

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.

**Note**

- Most EXEC commands are one-time commands such as the **show** commands which display important status information, and **clear** commands clear counters or interfaces.
- The EXEC commands are not saved when the software reboots.
- From privileged EXEC mode, you can run any EXEC command or enter the global configuration mode.

### Configuration mode

Configuration modes allow you to change the running configuration. If you later save the running configuration to the startup configuration, these changed commands are retained when the software reboots. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and other modes, such as protocol-specific modes.

### ROM monitor mode

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 may enter ROM monitor mode.

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

***Table 1: 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** 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.<br>To return to privileged EXEC mode, use the **end** command. |

| Command Mode | Access Method | Prompt | Exit Method |
|---|---|---|---|
| Diagnostic | The router boots up or accesses diagnostic mode in these scenarios:<br>• In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload.<br>• A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode.<br>• 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.<br>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. |
| 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. |

# 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.

***Table 2: Keyboard shortcuts***

| Key Name | Purpose |
|---|---|
| **Ctrl-B** or the **Left Arrow** key [1] | Move the cursor back one character. |

| Key Name | Purpose |
|---|---|
| **Ctrl-F** or the **Right Arrow** key [1] | Move the cursor forward one character. |
| **Ctrl-A** | Move the cursor to the beginning of the command line. |
| **Ctrl-E** | Move the cursor to the end of the command line. |
| **Esc B** | Move the cursor back one word. |
| **Esc F** | Move the cursor forward one word. |

# CLI command forms

Most configuration commands have a **no** form. Use the **no** form to disable a function. Use the command without **no** to enable or re-enable a disabled function or to enable a function that is already disabled by default.

As an example, IP routing is enabled by default. If you want to disable IP routing, you can use the **no ip routing** command and to re-enable IP routing, you can 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, you can enter **default ?** in the appropriate command mode.

# Using the history buffer to recall commands

The history buffer stores the last 20 commands entered, which can be accessed through history substitution commands.

***Table 3: History substitution commands***

| Command | Purpose |
|---|---|
| **Ctrl-P** or the **Up Arrow** key [1] | 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. |

| Command | Purpose |
|---|---|
| [1] The arrow keys function only on ANSI-compatible terminals such as VT100s. | |

# Configuration files management

The startup configuration file is stored in the nvram: file system. The running configuration files are stored in the system: file system. "Several other Cisco router platforms use this configuration file storage setup.

IOS XE encrypts the configuration file. For more information about encryption, see https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html.

As part of routine maintenance on any Cisco router, you must back up the startup configuration file. Copy the startup configuration file from NVRAM to one of the router's other file systems and to a network server. Backing up the startup configuration file makes it easy to recover if the file in NVRAM becomes unusable.
.

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

For more information on managing configuration files, see Cisco IOS XE Configuration Fundamentals Configuration Guide .

# Saving configuration changes

This task saves the configuration to the NVRAM using the **copy running-config startup-config** command.

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.

# Filter output from the show and more commands

Use the pipe character (|) with specific keywords to filter or search through the output of `show` and `more` commands.

Follow these steps to filter output from the show and more commands.

### Procedure

Use the **show** *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression* command to filter or search through the output of a show or more command.

**Note**

- 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 regular expression is case sensitive.
- 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 display only the output lines in which the expression `protocol` appears:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is up, line protocol is up
1401 unknown protocol drops
GigabitEthernet0/0/1 is up, line protocol is up
3073 unknown protocol drops
WPAN0/1/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/2/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/2/1 is up (spoofing), line protocol is up (spoofing)
0 unknown protocol drops
Cellular0/3/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/3/1 is down, line protocol is down
0 unknown protocol drops
Loopback1 is up, line protocol is up
0 unknown protocol drops
Tunnel1 is up, line protocol is up
Tunnel protocol/transport GRE/IP
0 unknown protocol drops
Tunnel2 is up, line protocol is up
Tunnel protocol/transport GRE/IP
0 unknown protocol drops
VirtualPortGroup1 is up, line protocol is up
0 unknown protocol drops
```

# Information about platforms and Cisco software images

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

For more information about Cisco IOS-XE configuration guides, see 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 determine if a feature is included in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html.

# Cisco feature navigator

You can 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.

# Getting help

Provides instructions for accessing context-sensitive help and command completion features within the CLI.

| 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.<br>**Note**<br>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 ?** | Lists the keywords or arguments that you must enter next on the command line.<br>**Note**<br>There is a space between the command and the question mark. |

## Finding command options examples

This section provides information about how to display the syntax for a command, including optional or required keywords and arguments, by using the question mark (?) at the configuration prompt.

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.

***Table 4: Finding command options***

| Command | Comment |
|---|---|
| `Router> enable`<br>`Password: <password>`<br>`Router#` | Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a " # " from the " > ", for example, `Router>` to `Router#` |
| `Router# configure terminal`<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`Router(config)#` | Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router (config)#` |
| `Router(config)# interface GigabitEthernet ?`<br>`<0-0> GigabitEthernet interface number`<br>`Router(config)# interface GigabitEthernet 0/?`<br>`<0-0> Port Adapter number`<br>`Router (config)# interface GigabitEthernet 0/0/?`<br>`<0-1> GigabitEthernet interface number`<br>`Router (config)# interface GigabitEthernet 0/0/0?`<br>`. <0-1>`<br>`Router(config-if)#` | Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.<br>Enter **?** to display what you must enter next on the command line.<br>When the <cr> symbol is displayed, you can press **Enter** to complete the command.<br>You are in interface configuration mode when the prompt changes to `Router(config-if)#` |

| Command | Comment |
| --- | --- |
| Router(config-if)# ?<br>Interface configuration commands:<br>. . .<br>ip Interface Internet Protocol<br>config commands<br>keepalive Enable keepalive<br>lan-name LAN Name command<br>llc2 LLC2 Interface Subcommands<br>load-interval Specify interval for load calculation<br>for an interface<br>locaddr-priority Assign a priority group<br>logging Configure logging for interface<br>loopback Configure internal loopback on an<br>interface<br>mac-address Manually set interface MAC address<br>mls mls router sub/interface commands<br>mpoa MPOA interface configuration commands<br>mtu Set the interface Maximum Transmission Unit (MTU)<br>netbios Use a defined NETBIOS access list<br>or enable name-caching<br>no Negate a command or set its defaults<br>nrzi-encoding Enable use of NRZI encoding<br>ntp Configure NTP<br>. . .<br>Router(config-if)# | 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. |

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

| Command | Comment |
|---|---|
| Router(config-if)# **ip address** **172.16.0.1 255.255.255.0 ?**<br>  secondary  Make this IP address a secondary address<br>  <cr><br>Router(config-if)# **ip address** **172.16.0.1 255.255.255.0** | Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.<br>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** .<br><cr> is displayed. Press **Enter** to complete the command, or enter another keyword. |
| Router(config-if)# **ip address** **172.16.0.1 255.255.255.0**<br>Router(config-if)# | Press **Enter** to complete the command. |

# Software advisor

Cisco maintains the Software Advisor tool. See Tools and Resources. You can 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.

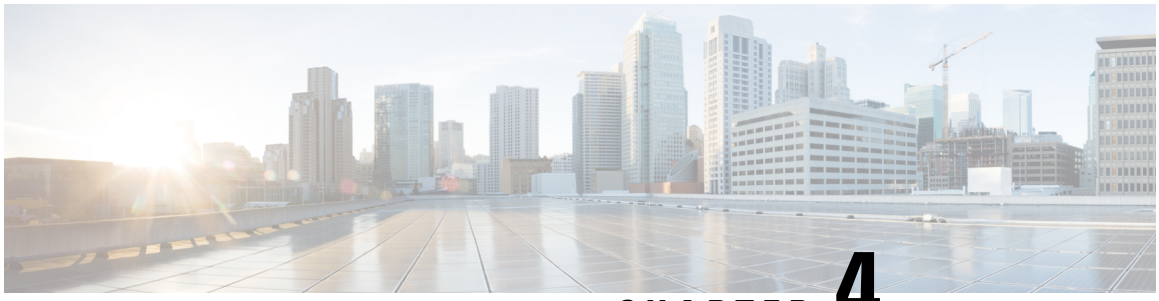
You must be a registered user on Cisco.com to access this tool.

# Software release notes

See the release notes for information about:

- Memory recommendations.
- Open and resolved severity 1 and 2 caveats.

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, see Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.



CHAPTER 4

# Basic router configuration

This chapter contains these sections:


- IR8140H interface names, on page 29
- Verify basic configuration of router, on page 30
- Configure global parameters, on page 36
- Configure Gigabit Ethernet interface, on page 37
- Configure sub-interface on GigabitEthernet0/0/0, on page 38
- Configure a loopback interface, on page 39
- Cisco Discovery Protocol for security, on page 40
- Configure command-line access, on page 40
- Configure a static route, on page 42
- Configuring dynamic routes, on page 44
- Modular QoS CLIs, on page 46
- Configuring VLANs, on page 46


## IR8140H interface names

The supported hardware interfaces and their naming conventions are as given in the table.

***Table 5: IR8140H hardware interfaces and naming conventions***

| Hardware interface | Naming convention |
|---|---|
| Gigabit Ethernet ports | GigabitEthernet0/0/0<br>GigabitEthernet0/0/1 |
| Cellular Interface | Cellular0/2/0<br>Cellular0/2/1<br>Cellular0/3/0<br>Cellular0/3/1 |
| mSATA SSD | msata |
| GPIO | alarm contact 1-2 |

| Hardware interface | Naming convention |
|---|---|
| WPAN | Wpan0/1/0 |

# Verify basic configuration of router

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.

### Procedure

Use the **show running-config** command to view the initial configuration.

**Example:**

```
IR8140H# show running-config
Building configuration...
Current configuration : 16150 bytes
!
! Last configuration change at 19:21:02 UTC Thu Nov 19 2020
!
version 17.5
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname IR8140H
!
boot-start-marker
boot system bootflash:/ir8100-universalk9.BLD_POLARIS_DEV_LATEST_20201108_112843.SSA.bin
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
aaa session-id common
!
ip domain name cisco.com
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
chat-script hspa-R7 "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
```

```
!
crypto pki trustpoint TP-self-signed-1536777273
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1536777273
 revocation-check none
 rsakeypair TP-self-signed-1536777273
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint LDevID
 enrollment retry count 4
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password
 fingerprint 7107DAB5FBDAC555893B7C047D202B5676F6C9AB
 subject-name serialNumber=PID:IR8140H-P-K9 SN:FDO2420J78D,CN= IR8140H
 revocation-check none
 rsakeypair LDevID 2048
!
crypto pki profile enrollment LDevID
 enrollment url  http://172.27.127.21/certsrv/mscep/mscep.dll
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = sit-dc-sit-dc-ca
!
crypto pki certificate chain TP-self-signed-1536777273
 certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31353336 37373732 3733301E 170D3230 31313137 32323237
  33325A17 0D333031 31313732 32323733 325A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 35333637
  37373237 33308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
  0A028201 01008D4E BBE387AB 5FE56CF9 77532A82 554176A9 3F13D193 729E1C9D
  0E9AC390 D66E845E 78AFEBFE 09DD0848 15DE936F E18FB64D 85E97E52 87412474
  DE16C42B 3101B84E 8C4F14C4 67EF8867 4AEE4996 6229CFBD 15556C90 F37C1C3D
  4D77A046 5934F3C9 6A98DDEE E4413E33 0F260D52 2EBB88C6 C0A1D9DC 633D13BB
  0DAC3ACD 6C980F61 C6521868 52EA0150 95C33DB0 26C0AB56 6CB67AD1 401CBBDD
  D1994822 1337B943 019F9EDF 4FC72749 01B66A31 ACD60696 14AF9A68 3D7578F1
  7BFE63CE A0D4A2F3 DA577B90 15C875EA F175CA24 B17E15A7 9C892E54 1D960D71
  907D4D23 2CE67E1A 720AA7A6 9EE1EFEE 12A26353 B258FECB CBAC3FF2 95DAC73D
  BBEC1F9E E1030203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
  301F0603 551D2304 18301680 14A1A44D ABD867DC 26C5B2F2 3A8D9504 807FFA9C
  E6301D06 03551D0E 04160414 A1A44DAB D867DC26 C5B2F23A 8D950480 7FFA9CE6
  300D0609 2A864886 F70D0101 05050003 82010100 267416FA CF69B1CD 96825C67
  483D698D 2B2838E5 94CDA5ED DA5E6BC0 E45739F9 676A4828 32FA2FDE C613BE3D
  6B00BA4B 97F52155 966726BE B02D6E48 685190E6 2AF094BC E2A4C087 B5F2449B
  4BFF2329 FD4D222D C11C3F73 727FD13C 901C51D0 3F08C6BA C6415D2F 078907E5
  D8CCCB8F E28D9485 D2AA4F6D 300A7A2D 289F5E49 79637E6D 7B678332 EEFF2E80
  E344AB7C F0FC70D5 694C0CC3 DB9F62E5 2A050979 E9171466 81CC91BA A99AB7C7
  12CACA37 D196D178 E349C627 597CFA9C 49132F8A 17C2F471 7E9D80E5 B7D5E673
  A225E086 F6E523AC 0C565E9A 3A7E1610 4275D2B7 9AFD5703 F5E1A8E0 94E53C1B
  ADF8644D EF0541A8 E98A1F41 A3A6F208 920EAE57
        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 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 LDevID
 certificate 5B00005DA8024836ED49AF77AE000000005DA8
  308205B1 30820499 A0030201 0202135B 00005DA8 024836ED 49AF77AE 00000000
  5DA8300D 06092A86 4886F70D 01010B05 00305F31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
  13107369 742D6463 2D534954 2D44432D 43413020 170D3230 31313139 31383531
  30395A18 0F323036 30313130 39313835 3130395A 30463128 30260603 55040513
  1F504944 3A495238 31343048 2D502D4B 3920534E 3A46444F 32343230 4A373844
  311A3018 06035504 030C1143 41424F5F 5349545F 43656C6C 756C6172 30820122
  300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00BC58AA
  810C8701 09F8B90F 2DE268BF 0CA253E8 605494F2 6A6E7FA9 387ED47B BA89C51B
  D549F4A5 16A64C04 C443A752 719A7624 DEB96B0F 898CECB5 05F7E32C 83D2FB4D
  1E87F7C0 4CCE92FC 152579FB F1974517 A2B4B05A 2B72CCF8 6FE2583F D25AE93E
  8C695806 13146E94 5B97810F 4BC6E125 78A14A68 24682979 B4ACC67D 7F58D50E
  3170D595 6DE90AD2 9CC37663 6FD9CE7B 5EB425D9 6220E0B4 705ECD1A AEA21BA6
  2071DDAB 21E4D3DC 7E83C843 D8532C6E 41939E56 A510B8F5 0A04CA8F 3F0F6EAE
  596E54C5 5FBFD7E2 70975CB7 5D081F63 F236C694 E7A4CCDD CB1FB336 CB07DD66
  52CC830D F82A684C B74FEC5D 849E0E58 6FA575D1 9F7477BD 04B1354F 77020301
  0001A382 027B3082 0277300B 0603551D 0F040403 0204F030 1D060355 1D0E0416
  04147B0F 6A00A9E8 A6DBB59A 33FD0F6C E0D9913A 7E31301F 0603551D 23041830
  16801422 A59DB25D 909EDA07 4C0039B5 9575B3F8 898F5330 81D50603 551D1F04
  81CD3081 CA3081C7 A081C4A0 81C18681 BE6C6461 703A2F2F 2F434E3D 7369742D
  64632D53 49542D44 432D4341 2C434E3D 7369742D 64632C43 4E3D4344 502C434E
  3D507562 6C696325 32304B65 79253230 53657276 69636573 2C434E3D 53657276
  69636573 2C434E3D 436F6E66 69677572 6174696F 6E2C4443 3D736974 2D64632C
  44433D63 6973636F 2C44433D 636F6D3F 63657274 69666963 61746552 65766F63
  6174696F 6E4C6973 743F6261 73653F6F 626A6563 74436C61 73733D63 524C4469
  73747269 62757469 6F6E506F 696E7430 81CA0608 2B060105 05070101 0481BD30
  81BA3081 B706082B 06010505 07300286 81AA6C64 61703A2F 2F2F434E 3D736974
  2D64632D 5349542D 44432D43 412C434E 3D414941 2C434E3D 5075626C 69632532
  304B6579 25323053 65727669 6365732C 434E3D53 65727669 6365732C 434E3D43
  6F6E6669 67757261 74696F6E 2C44433D 7369742D 64632C44 433D6369 73636F2C
  44433D63 6F6D3F63 41436572 74696669 63617465 3F626173 653F6F62 6A656374
  436C6173 733D6365 72746966 69636174 696F6E41 7574686F 72697479 303B0609
  2B060104 01823715 07042E30 2C06242B 06010401 82371508 8593BB6B 85858C6C
  8289810E 86C7AC03 E7EF037D 84B1A57E B4FB3402 01640201 07301D06 03551D25
  04163014 06082B06 01050507 03010608 2B060105 05070302 30270609 2B060104
  01823715 0A041A30 18300A06 082B0601 05050703 01300A06 082B0601 05050703
```

```
  02300D06 092A8648 86F70D01 010B0500 03820101 007D1625 49EB4FA2 199A95B5
  F6E4AD0C 4D410FCB D8EDF68A D7688929 E9F54074 1EBEE52C FEC28615 7E8180D2
  20614BD2 FC5CB729 8480F6C4 5344435E A16A27B8 2D063A7E 0F2E5717 30FBE32C
  4365B580 3FF828F1 006AA660 FFD06854 DCB5808E 8A4B233B 2A2F9ED8 5C2178C8
  C57F0AEC FB6F78DF C47540CE 26CC41C0 F28DF410 A12A1EC0 EBFA6584 3823620E
  63841662 995759C0 5F066DC0 F1E90319 CB0CC687 B25115C1 B0E41D2B D96A84FE
  E0CC0784 135BCB64 F899761D 95A6ACA0 C0B8347F 148D1D94 C6194166 60C752D1
  A788C236 524599E0 90B650A8 B2DE7861 B2CABBAA 43531F78 20C0626A 010E4C67
  DD1A5E64 BBAE382B C38AA018 737F81DA 3A80726E 4C
        quit
 certificate ca 118989AFB1C4AD944B97A1CD898BD73B
  3082039B 30820283 A0030201 02021011 8989AFB1 C4AD944B 97A1CD89 8BD73B30
  0D06092A 864886F7 0D01010B 0500305F 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31163014
  060A0992 268993F2 2C640119 16067369 742D6463 31193017 06035504 03131073
  69742D64 632D5349 542D4443 2D434130 20170D31 38303932 35313134 3735335A
  180F3230 36383039 32353131 35373533 5A305F31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
  13107369 742D6463 2D534954 2D44432D 43413082 0122300D 06092A86 4886F70D
  01010105 00038201 0F003082 010A0282 010100AF 6FB5E529 DEF701CD E5ACB737
  D2790873 875E9DBB 53ADAFC2 94C3D991 EC658A69 B1AB69BA C32307BE BF9D225D
  4FEADF33 F396AB70 A4E49526 AE637FE4 6BA0BB32 C98528D0 94658C48 DBE550A1
  ECA35F7A 4279F16C 5F3C2B11 185F95BB 9D68B2C9 82ECB523 BC3E5833 436BD1D1
  AE9616BD 1E0FC85D 67EF135B 6BC68840 3103DA89 923156FC EADD0914 3DD1F75E
  B166E550 A9F0FBEA 80DDE1F4 1B4D7789 3872EEA0 5B375344 03CDDFBA 72DC6F53
  6C3D25A3 BF8E215F 8D55C8D1 D0C279ED 9E061673 3FC6F225 6C405AA3 E6B96310
  4C2798A9 EC561A29 FF875907 B3527352 61A09CF2 D7916631 1F5215E5 6077E8C4
  A5042B6E 3039B222 BCFA1133 53FA51AD 2E972D02 03010001 A351304F 300B0603
  551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
  0E041604 1422A59D B25D909E DA074C00 39B59575 B3F8898F 53301006 092B0601
  04018237 15010403 02010030 0D06092A 864886F7 0D01010B 05000382 01010039
  6F03857F 8B5F0A38 E6DFA0E9 8598FE40 9231C4DF 5D747EA8 B968606B DD1593A8
  2348303C 7948DD69 1FDEA891 2A249CCC 9B9C9071 D51B1AC6 EF1567EF 64E8C11A
  85BDA86C AC45954E 7A86861C 1D7C622B 2211652C C8CC6359 09000B78 0E6ABF6E
  06D4247B 572E91B2 1216BC9A 5D715B8D E3220C4B 4B6B1B1A 3AA4B2CB 67F7F6B5
  2B3D9820 0E5A50A3 123E41F5 3C0D46E0 63E7212B 4730D9DA 4E0E8227 AEEAE386
  3C1A1B3A C680B486 5F71B0B5 80C82F6C 58126809 39193ABF D145BA7D 4D695762
  5DB055D4 077E779D AEA96655 576B3085 0CD9E01F 6805EF8B 494EE44B 16ACEED8
  F6529B1F AA324C9F 464FA153 9DAF12C1 74872179 1DA83009 26D36774 77C52F
        Quit
!
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2441J91D
license boot level network-advantage
memory free low-watermark processor 47507
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_IPv4_LAN
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
```

```
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 dpd 120 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 dpd 60 10 periodic
crypto ikev2 client flexvpn FlexVPN_Client_2
  peer 1 103.0.0.254
  client connect Tunnel2
!
crypto ikev2 client flexvpn FlexVPN_Client_1
  peer 1 102.0.0.254
  client connect Tunnel1
!
!
controller Cellular 0/2/0
!
controller Cellular 0/3/0
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
!
interface Loopback1
 ip address 12.12.12.12 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel source Cellular0/2/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel2
 ip unnumbered Loopback1
 tunnel source Cellular0/3/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup1
 ip address 192.168.11.1 255.255.255.0
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip address 172.27.127.74 255.255.255.128
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
```

```
!
interface Cellular0/2/0
 ip address negotiated
 ip access-group 1 out
 ip tcp adjust-mss 1460
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/2/1
 no ip address
!
interface Cellular0/3/0
 ip address negotiated
 ip access-group 1 out
 ip tcp adjust-mss 1460
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer-group 2
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/3/1
 no ip address
!
interface WPAN0/1/0
 no ip address
 arp timeout 0
 no mop enabled
 no mop sysid
!
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip route 102.0.0.0 255.255.255.0 Cellular0/2/0 192.168.5.1
ip route 103.0.0.0 255.255.255.0 Cellular0/3/0 192.168.4.1
ip route 192.168.4.0 255.255.255.0 Cellular0/3/0
ip route 192.168.5.0 255.255.255.0 Cellular0/2/0
!
ip access-list standard FlexVPN_Client_IPv4_LAN
 10 permit 192.168.11.0 0.0.0.255
 20 permit 12.12.12.12
!
!
ip access-list standard 1
 10 permit any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
!
snmp-server enable traps wpan
!
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
line vty 0 4
 transport input ssh
line vty 5 14
 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
app-hosting appid iperf
 app-vnic gateway0 virtualportgroup 1 guest-interface 0
  guest-ipaddress 192.168.11.2 netmask 255.255.255.0
 app-default-gateway 192.168.11.1 guest-interface 0
end
```

# Configure global parameters

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

### Procedure

**Step 1** Use the **configure terminal** command to enter the global configuration mode when using the console port.

**Example:**

```
Router> enable
Router# configure terminal
Router(config)#
```

**Step 2** Connect to the router with a remote terminal.

**Example:**

```
telnet router-name or address
Login: login-id
Password: *********
Router> enable
```

**Step 3** Use the **hostname** *name* command to specify the name for the router.

**Example:**

```
Router(config)# hostname Router
```

Specifies the name for the router.

**Step 4** Use the **enable password** *password* or **enable secret password** *password* command to specify a password to prevent unauthorized access to the router

**Example:**

```
Router(config)# enable password cr1ny5ho
```

**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.

# Configure Gigabit Ethernet interface

The router features two Gigabit Ethernet (GE) ports that can be used to enable WAN connectivity to a primary substation or a control center.

- One GigE Copper port (RJ45) on the midplane board. It supports standard 3-speed (10/100/1000) Ethernet features including auto-MDIX.
- One SFP socket. It supports standard 1000Base-X or 100Base-FX Ethernet over single-mode or multi-mode fiber.

To configure the Gigabit Ethernet interface, follow these steps:

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Step 2** Use the **ipv6 unicast-routing** command to enable forwarding of IPv6 unicast data packets.

**Example:**

```
Router#configure terminal
Router(config)# ipv6 unicast-routing
```

**Step 3** Use the **interface GigabitEthernet** *slot/bay/port* command to enter the configuration mode for an interface on the router.

**Example:**

```
Router(config)# interface GigabitEthernet 0/0/0
```

Enters the configuration mode for an interface on the router.

**Step 4** Use the **ip address** *ip-address mask* command to set the IP address and subnet mask for the specified interface.

**Example:**

```
Router(config-if)# ip address 192.168.12.2 255.255.255.0
```

**Note** You can use this step if you are configuring an IPv4 address.

**Step 5** Use the **ip address** *ipv6-address/prefix* command to set the IPv6 address and prefix for the specified interface.

**Example:**

```
Router(config-if)# ipv6 address 2001.db8::ffff:1/128
```

**Note** 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**, For more information, see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html.

**Step 6** Use the **no shutdown** command to enable the interface and change its state from administratively down to administratively up.

**Example:**

```
Router(config-if)# no shutdown
```

**Step 7** Use the **exit** command to exit the configuration mode of the interface and return to the global configuration mode.

**Example:**

```
Router(config-if)# exit
```

# Configure sub-interface on GigabitEthernet0/0/0

Cisco IOS XE supports sub-interfaces and dot1q configuration on the g0/0/0 interface.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router> enable
Router# configure terminal
Router(config)#
```

**Step 2** Use the **interface** *g0/0/0.***?** command to enter the sub-interface mode.to configure a sub-interface and dot1q encapsulation on the GigabitEthernet0/0/0 interface.

**Example:**

```
Router(config)#interface g0/0/0.? <1-4294967295>  GigabitEthernet interface number
Router(config-subif)#
```

**Step 3** Use the **encapsulation ?** command to configure the sub-interface and **dot1q** encapsulation on the GigabitEthernet0/0/0 interface.

**Example:**

```
Router(config-subif)# encapsulation ? dot1Q IEEE 802.1Q Virtual LAN
```

# Configure 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**

**Step 1** Use the **configure terminal** command to enter the global configuration mode

**Step 2** Use the **interface** *type number* command to enter the configuration mode on the loopback interface.

**Example:**

```
Router(config)# interface Loopback 0
```

**Step 3** (Option 1) Use the **ip address** *ip-address mask* command to set the IP address and subnet mask on the loopback interface.

**Example:**

```
Router(config-if)# ip address 10.108.1.1 255.255.255.0
```

**Note** If you are configuring an IPv6 address, you can use the **ipv6 address** *ipv6-address/prefix* command.

**Step 4** (Option 2) Use the **ipv6 address** *ipv6-address/prefix* command to set the IPv6 address and prefix on the loopback interface.

**Example:**

```
Router(config-if)# ipv6 address 2001:db8::ffff:1/128
```

**Step 5** Use the **exit** command to exit the loopback interface mode.

**Example:**

```
Router(config-if)# exit
```

**Step 6** Use the **show interface loopback** command to verify the loopback interface configuration.

**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
```

# Cisco Discovery Protocol for security

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.

# Configure 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

**Step 1** Use the **line** [ **aux** | **console** | **tty** | **vty** ] *line-number* command to enter the line configuration mode, and specify the type of line.

**Example:**

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

**Note** The example provided here specifies a console terminal for access.

**Step 2** Use the **password** *password* command to specify a unique password for the console terminal line.

**Example:**

```
Router(config-line)# password 5dr4Hepw3
```

**Step 3** Use the **login** command to enable password checking at terminal session login.

**Example:**

```
Router(config-line)# login
```

**Step 4** Use the **exec-timeout** *minutes* [ *seconds* ] command to set the interval during which the EXEC command interpreter waits until user input is detected.

**Example:**

```
Router(config-line)# exec-timeout 5 30
Router(config-line)#
```

**Note**

- 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** Use the **line** [ **aux** | **console** | **tty** | **vty** ] *line-number* command to specify a virtual terminal for remote console access.

**Example:**

```
Router(config)# line vty 0 4
Router(config-line)#
```

**Step 7** Use the **password** *password* command to specifies a unique password for the virtual terminal line.

**Example:**

```
Router(config-line)# password aldf2ad1
```

**Step 8** Use the **login** command to enables password checking at the virtual terminal session login.

**Example:**

```
Router(config-line)# login
```

**Step 9** Use the **end** command to exit line configuration mode, and returns to privileged EXEC mode.

**Example:**

```
Router(config-line)# end
```

a) Use the **show running-config** command to verify the loopback interface configuration.

**Example:**

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (
    default
                        )
topbits 1 (
    default
          )
line vty 0 4
password secret
login
!
```

**Note**

- The transport input none is the default, but if SSH is enabled this must be set to ssh.
- You do not have to input the commands marked **default**.

# Configure a static route

Static routes provide fixed routing paths through the network. They are manually configured on the router. update the static route with a new one. Static routes are private routes unless they are redistributed by a routing protocol.

**Before you begin**

To configure static routes, follow these steps.

**Procedure**

**Step 1** (Option 1) Use the **ip route** *prefix mask* { *ip-address* | *interface-type interface-number* [ *ip-address* ]} command to specify a static route for IP packets.

**Example:**

```
Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2
```

**Note** If you are configuring an IPv6 address, use the **ipv6 route** command.

**Step 2** (Option 2) Use the **ipv6 route** *prefix/mask* { *ipv6-address* | *interface-type interface-number* [ *ipv6-address* ]} command to specify a static route for IP packets.

**Example:**

```
Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0
```

**Note** See additional information for IPv6 here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html

**Step 3** Use the **end** command to exit global configuration mode and enter privileged EXEC mode.

**Example:**

```
Router(config)# end
```

After configuring static routes, the router will use the specified paths for routing IP or IPv6 packets. You can verify the configuration using the appropriate show commands.

**Step 4** Use the **show ip route** (or **show ipv6 route**) command to verify static routing configuration.

For IPv4 address:

**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
S*   0.0.0.0/0 is directly connected, GigabitEthernet0
```

For IPv6 address:

**Example:**

```
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
```

**Note**

- In the 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 need to enter the command marked **default**. This command appears automatically in the configuration file generated when you use the **running-config** command.

# 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.

For more information on Cisco IOS-XE configuration guides, see https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-amsterdam-17-3-1/model.html.

## Configure routing information protocol

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

**Procedure**

**Step 1** Use the **router rip** command to enter router configuration mode, and enable RIP on the router.

**Example:**

```
Router(config)# router rip
```

**Step 2** Use the **version** { **1** | **2** } command to specify use of RIP version 1 or 2.

**Example:**

```
Router(config-router)# version 2
```

**Step 3** Use the **network** *ip-address* command to specify a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.

**Example:**

```
Router(config-router)# network 192.168.1.1
Router(config-router)# network 10.10.7.1
```

**Step 4** Use the **no auto-summary** command to disable automatic summarization of subnet routes into network-level routes.

**Example:**

```
Router(config-router)# no auto-summary
```

**Note** It allows sub prefix routing information to pass across classful network boundaries.

**Step 5** Use the **end** command to exit router configuration mode, and enters privileged EXEC mode.

**Example:**

```
Router(config-router)# end
```

**Step 6** Use the **show ip route** command to verify RIP configuration.

**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
```

**Note** You can look for RIP routes marked with the letter R.

# 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.

- EIGRP offers improved convergence properties and operating efficiency compared to IGRP.
- IGRP is now considered obsolete.
- EIGRP uses the Diffusing Update Algorithm (DUAL) to guarantee loop-free operation and synchronize devices during topology changes.

### Convergence and Efficiency in EIGRP

EIGRP's convergence technology is based on the Diffusing Update Algorithm (DUAL), which ensures loop-free operation and device synchronization during route computations.

**Note** Devices that are not affected by topology changes are not involved in recomputations.

For more information on configuring Enhanced Interior Gateway Routing Protocol (EIGRP), see https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-10/ire-xe-16-10-book/ire-enhanced-igrp.html .

# Modular QoS CLIs

Modular QoS CLI (MQC) is a standardized approach for configuring Quality of Service (QoS) features on Cisco routing and switching platforms, including the IoT Integrated Services Router.

- MQC provides a consistent method to enable and manage QoS across Cisco devices.
- It is used on both routing and switching platforms.
- MQC is the primary interface for configuring QoS features on the IoT Integrated Services Router.

### Overview and Reference for Modular QoS CLI (MQC)

MQC is the method by which all QoS features are configured on the IoT Integrated Services Router.

For more details, see QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE 17 .

# Configuring VLANs

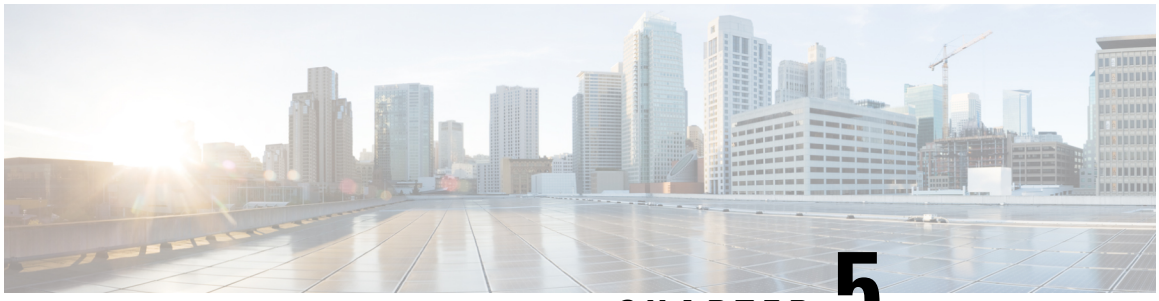
A VLAN is a switched network that is logically segmented by function or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs. However, you can group end-stations even if they are not physically located on the same LAN segment. Any device port can belong to a VLAN, 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 or a device supporting fallback bridging. In a device stack, VLANs can be formed with ports across the stack. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the device is assigned manually on an interface-by-interface basis. When you assign device interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

The device can route traffic between VLANs by using device virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.

**Note** IR8140 routers have reserved a set of VLANs 2350 to 2449 for internal platform use. It is not allowed to add the reserved VLANs. You must ensure that these VLANs are not used in the network.



CHAPTER 5

# Configuring Secure Shell

This section provides the necessary information to configure Secure Shell on network devices.


- Secure Shell, on page 47
- How to Configure Secure Shell, on page 49
- Secure copy, on page 54
- Additional references, on page 56


## 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

Secure Shell (SSH) prerequisites are the mandatory configuration and software requirements that must be met before the device can support secure remote connections.

- An RSA public/private key pair must be generated on the device.
- An IPsec encryption software image (DES or 3DES) must be installed for both the SSH server and client.
- A valid hostname and host domain must be configured using global configuration commands.

### Configuration requirements for Secure Shell

To successfully configure the device for SSH, ensure the following settings are applied:

- Configure the device identity by using the **hostname** and **ip domain-name** commands in global configuration mode.

## Restrictions for configuring Secure Shell

Provides the necessary constraints and configuration requirements for enabling secure shell on the IR8100.

These are restrictions for configuring the IR8100 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.
- This software release supports IP Security (IPSec).
- The IR8100 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.

**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.

# SSH and router access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device.

- Provides more security for remote connections than Telnet by using strong encryption.
- Supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).
- Functions consistently in both IPv4 and IPv6, supporting IPv6 addresses and secure transport.

# SSH servers, integrated clients, and supported versions

The SSH Integrated Client is an application that runs over the SSH protocol to provide device authentication and encryption.

- Enables secure, encrypted connections to Cisco or non-Cisco devices running an SSH server.
- Supports ciphers including DES, 3DES, and password authentication.
- Requires the SSH server to be enabled for client functionality.

### SSH authentication methods

The SSH client supports the following user authentication methods:

- TACACS+
- RADIUS

- Local authentication and authorization

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

# SSH configuration guidelines

An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.

## RSA Key Generation Troubleshooting

Ensure that the hostname and domain are configured correctly before generating RSA keys to avoid CLI errors or warning messages.

- 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

## Set up the IR8140H to run SSH

To set up your device to run SSH, follow this procedure.

**Note** Configure user authentication for local or remote access. This step is required.

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Note** Enter password if prompted.

**Step 2** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **hostname** *hostname* command to configure a hostname for your device.

**Example:**

```
Router(config)# hostname your_hostname
```

**Note** You can follow this procedure only if you are configuring the device as an SSH server.

**Step 4** Use the **ip domain-name** *domain_name* command to configure a host domain for your device.

**Example:**

```
Router(config)# ip domain-name your_domain_name
```

**Step 5** Use the **crypto key generate rsa** command to enable the SSH server for local and remote authentication on the device and generate an RSA key pair.

**Example:**

```
Router(config)# crypto key generate rsa
```

**Note** You must follow this procedure only if you are configuring the device as an SSH server. Generating an RSA key pair for the device automatically enables SSH. A minimum modulus size of 1024 bits is recommended. 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.

**Step 6** Use the **end** command to exit to privileged EXEC mode.

**Example:**

```
Router(config)# end
```

**Step 7** Use the **show running-config** command to verify your entries.

**Example:**

```
Router# show running-config
```

**Step 8** (Optional) Use the **copy running-config startup-config** command to save your entries in the configuration file.

**Example:**

```
Router# copy running-config startup-config
```

# Configure the SSH server

**Before you begin**

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

Follow these steps to configure the SSH server.

**Procedure**

**Step 1** Use the **configure terminal** to enter global configuration mode.

**Example:**

```
IR8100# configure terminal
```

**Step 2** Use the **ip ssh version** [ **2** ] command to optionally configure the device to run SSH Version 2.

**Example:**

```
IR8100(config)#  ip ssh version 2
```

**Note** 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 3** Use the **ip ssh** { **timeout** *seconds* | **authentication-retries** *number* } command to configures the SSH control parameters.

**Example:**

```
IR8100(config)# ip ssh timeout 90 ip ssh authentication-retries 2
```

**Note**

- 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 the connection is established, the device uses the default time-out values of the CLI-based sessions.

  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.

- Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.

- Repeat this Step 4 when configuring both parameters.

**Step 4** Use one or both commands:

- **line vty** *line_number* [ *ending line number* ]
- **transport input ssh**

**Example:**

```
IR8100(config)# line vty 1 10
```

or

```
IR8100(config-line)#  transport input ssh
```

**Note** Optionally you can configure the virtual terminal line settings.

- Enters line configuration mode to configure the virtual terminal line settings. For the *line_number* and *ending_line_number* 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 5** Use the **end** command to exit line configuration mode and return to privileged EXEC mode.

**Example:**

```
IR8100(config-line)# end
```

# SSH configuration and status commands

This topic provides information about commands for displaying the SSH server configuration and status.

***Table 6: 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. |

# Configure the router for local authentication and authorization

**Before you begin**

**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.

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:

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
IR8100# configure terminal
```

**Step 2** Use the **aaa new-model** command to enable AAA.

**Example:**

```
IR8100(config)# aaa new-model
```

**Step 3** Use the **aaa authentication login default local** command to set the login authentication to use the local username database.

**Example:**

```
IR8100(config)# aaa authentication login default local
```

**Note** The default keyword applies the local user database authentication to all ports.

**Step 4** Use the **aaa authorization exec local** command to configure user AAA authorization, check the local database, and allow the user to run an EXEC shell.

**Example:**

```
IR8100(config-line)#  aaa authorization exec local
```

**Step 5** Use the **aaa authorization network local** command to configure user AAA authorization for all network-related service requests.

**Example:**

```
IR8100(config-line)# aaa authorization network local
```

**Step 6** Use the **username** *name* **privilege** *level* **password** *encryption-type password* command to enter the local database, and establishes a username-based authentication system.

**Example:**

```
IR8100(config-line)# username your_user_name privilege 1 password 7 secret567
```

**Note** Repeat this command for each user.

**a.** For *name* , specify the user ID as one word. Spaces and quotation marks are not allowed.

**b.** (Optional) For *level* , 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.

**c.** For encryption-type, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.

**d.** For password, 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 7** Use the **end** command to exit line configuration mode and return to privileged EXEC mode.

**Example:**

```
IR8100(config-line)# end
```

# 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

These 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

This section describes the restrictions for configuring the IR1800 for secure copy (SCP).

- 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.

# Configure secure copy server

To configure the Cisco IR8100 for Secure Copy (SCP) server-side functionality, perform these steps.

**Procedure**

**Step 1** Use the **enable** command to enable privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **aaa new-model** command to set AAA authentication at login.

**Example:**

```
Router(config)# aaa new-model
```

**Step 4** Use the **aaa authentication login** { **default** | *list-name* } *method1* [ *method2...* ] command to enable the AAA access control system.

**Example:**

```
Router(config)# aaa authentication login default group tacacs+
```

**Step 5** Use the **username** *name* [ **privilege** *level* ] **password** *encryption-type encrypted-password* command to establish a username-based authentication system.

**Example:**

```
Router(config)# username superuser privilege 2 password 0 superpassword
```

**Note** You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.

**Step 6** Use the **ip scp server enable** command to enable SCP server-side functionality.

**Example:**

```
Router(config)# ip scp server enable
```

**Step 7** Use the **exit** command to exit global configuration mode and return to privileged EXEC mode

**Example:**

```
Router(config)# exit
```

**Step 8** Use the **show running-config** command to optionally display the SCP server-side functionality.

**Example:**

```
Router# show running-config
```

**Step 9** Use the **debug ip scp** command to optionally troubleshoot SCP authentication problems.

**Example:**

```
Router# debug ip scp
```

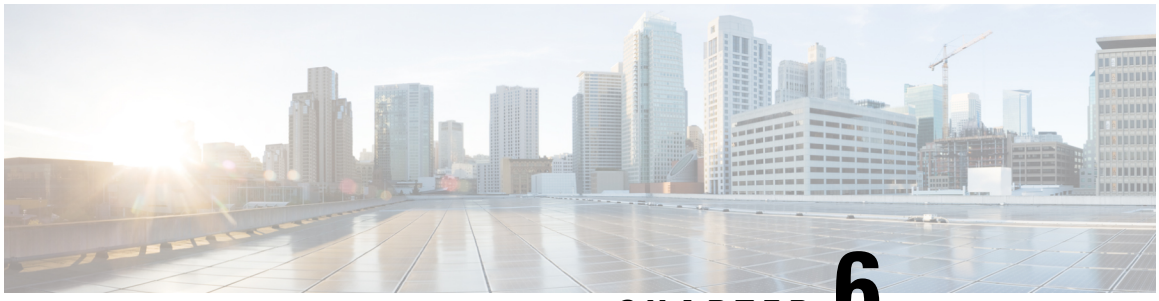
```
IR8100#   copy scp <somefile> your_username@remotehost:/ <some/remote/directory>
```

# Additional references

These sections provide references related to the SSH feature.

***Table 7: References***

| 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 6

# Software installation reference

This chapter contains the following sections:


- Software installation requirements, on page 57
- Install Cisco IOS XE release, on page 59
- ROMMON image software packages, on page 61
- File systems, on page 61
- Autogenerated file directories and files, on page 62
- Flash storage, on page 63
- Related documentation, on page 63


# Software installation requirements

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

Upgrade software during a scheduled maintenance period when service interruption is acceptable. After upgrading the software, reboot the router to apply changes.

## Cisco software licenses

Cisco software licensing is a system that enables activation and validation of Cisco IOS software feature sets through specific processes and components.

- Licenses can be used to enable consolidated packages, technology packages, or individual features.
- License files are stored in the bootflash of the router.
- The IR8100 uses Smart Licensing Using Policy (SLP) for license management.

### Understanding 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.

# Consolidated packages

Consolidated packages are image-based licenses used to activate all subsystems on the IR8100 router that correspond to a specific license. These licenses are enforced only at boot time.

- Image-based licenses help bring up all subsystems related to the license.
- Licenses are enforced only during the router's boot process.
- Not all IOS-XE features may apply to the IR8100; some features may not be implemented or appropriate for this platform.

### Available consolidated packages and feature applicability

To obtain software images for the IR8100 router, See Cisco Software Download page.

The following image-based licenses can be pre-installed on the IR8100 router:

- Network-Essentials
- Network-Advantage



**Note** All of the IOS-XE feature set may not apply to the IR8100. Some features may not have been implemented yet, or are not appropriate for this platform. Details of the Network-Essentials and Network-Advantage contents can be found in the IR8100 product data sheet.

# Network-Essentials packages

The Network-Essentials and Network-Essentials_npe technology is a baseline networking feature.

- The **Network-Essentials** technology package includes baseline features and supports security features.
- The **Network-Essentials_npe** package includes all features of Network-Essentials except payload encryption functionality.
- The **Network-Essentials_npe** is available only in the Network-Essentials_npe image and helps fulfill export restriction requirements.

### Differences between Network-Essentials and Network-Essentials_npe packages

The main difference between the Network-Essentials and Network-Essentials_npe packages is the presence or absence of payload encryption features such as IPsec and Secure VPN.

# Network-Advantage packages

**Network-Advantage** is a Cisco technology that provides advanced network features.

- The **Network-Advantage** technology package includes all crypto features.
- The **Network-Advantage_npe** package (npe = No Payload Encryption) includes all features of **Network-Advantage** except payload-encryption functionality.

- The **Network-Advantage_npe** package is available only in the **Network-Advantage_npe** image to fulfill export restriction requirements.

#### Feature differences between Network-Advantage and Network-Advantage_npe

The main difference between the **Network-Advantage** and **Network-Advantage_npe** packages is the set of payload-encryption-enabling features such as IPsec and Secure VPN.

## Related documentation

For further information on software licenses, see the Smart Licensing chapter.

# Install Cisco IOS XE release

When the device boots up with the Cisco IOS XE image for the first time, it checks the installed version of the ROMmon and upgrades it 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.

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

**Note** When the device boots up for the first time and the device requires an upgrade, the entire boot process may take several minutes. This process is longer than a normal boot because of the ROMmon upgrade.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode and set the boot system, configuration register, and exit.

**Example:**

```
Router# configure terminal
Router(config)# boot sys
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210221_233814_V17_5_0_172.SSA.bin
Router(config)# config-register 0x2102
Router(config)# exit
Router#
```

**Step 2** Use the **show romvar** command to verify the ROMmon variables and license configuration.

**Example:**

```
Router# show romvar
ROMMON variables:
PS1 = rommon ! >
THRPUT =
LICENSE_BOOT_LEVEL = network-advantage,all:IR8100;
RET_2_RTS =
CONSOLE_LOCK = 0
BOOT =
flash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210221_233814_V17_5_0_172.SSA.bin,12;
BSI = 0
```

```
RET_2_RCALTS =
RANDOM_NUM = 1294606670
```

**Step 3** Use the **show running-config | include license** command to display all lines in the running configuration that contain the word "license".

**Example:**

```
Router# show running-config | include license
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2441J91D
license boot level network-advantage
Router#
```

**Step 4** Use the **reload ?** command to display the available reload options.

**Example:**

```
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>
```

**Step 5** Use the **reload /verify** command to verify the image and reload the device.

**Example:**

```
Router# reload /verify
Verifying file integrity of
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210221_233814_V17_5_0_172.SSA.bin.....
.....Computed
Hash SHA1 : AA480FF5DDA5077A9FF99CABCB176E37E7DBD4F6
Starting image verification
Hash Computation: 100%Done!
Computed Hash SHA2: f2aaa17b3aaa4bb6573e1947976e1086
9a835fb36a48fbc3a8653224af5dab7f
383387a559ee35242830697ceae4a6c0
5add53a956a0dce109df80cb03c9c8b9
Embedded Hash SHA2: f2aaa17b3aaa4bb6573e1947976e1086
9a835fb36a48fbc3a8653224af5dab7f
383387a559ee35242830697ceae4a6c0
5add53a956a0dce109df80cb03c9c8b9
Digital signature successfully verified in file
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210221_233814_V17_5_0_172.SSA.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!
```

# ROMMON image software packages

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.

- ROMMON images are independent software packages for the ROM Monitor.
- They are separate from the main consolidated package used to boot the router.
- ROMMON images can be upgraded independently of the main software package.

### ROMMON Image Release and Upgrade Information

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 table provides a list of file systems that can be seen on the Cisco IR8100 router.

***Table 8: Router File Systems.1.a***

| File System | Description |
|---|---|
| bootflash: | Boot flash memory file system. |
| cns: | Cisco Networking Services file directory. |
| crashinfo: | Directory or Filename |
| flash: | Alias to the boot flash memory file system. |
| msata: | Directory or Filename |
| null: | Directory or Filename |

***Table 9: Router File Systems.1.b***

| File System | Description |
|---|---|
| nvram: | Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM. |
| system: | System memory file system, which includes the running configuration. |

| File System | Description |
|---|---|
| tar: | Archive file system. |
| tmpsys: | Temporary system files file system. |
| webui: | Directory or Filename |

Use the **?** help option if you find a file system that is not listed in the provided tables.

# Autogenerated file directories and files

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

***Table 10: Autogenerated files***

| File or directory | Description |
|---|---|
| crashinfo files | Crashinfo files can appear in the bootflash: file system.<br>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 | Storage area for .core files.<br>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. |
| managed directory | This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router. |
| tracelogs directory | The storage area for trace files.<br>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.<br>Trace files are not part of router operations; you can erase them without affecting the router's performance. |

### Key points about autogenerated directories

Important information about autogenerated directories include:

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

**Note** Altering autogenerating 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.

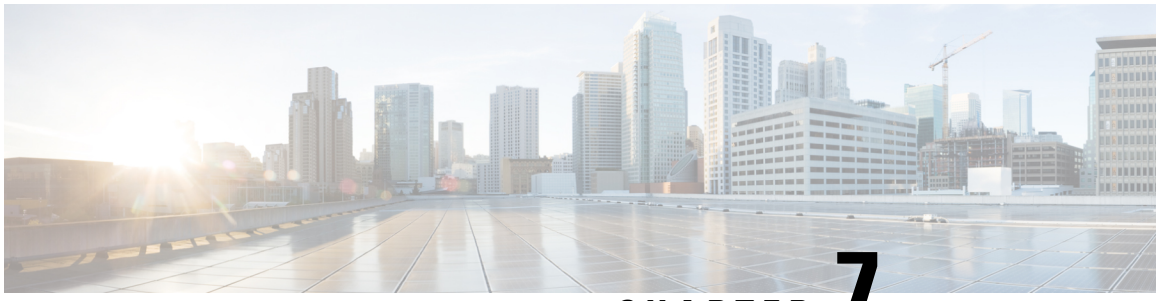
**Note** Flash storage is required for successful operation of a router.

# Related documentation

This topic provides references to further information on software licenses and feature license installation.

For more information on software licenses, see the Smart Licensing Chapter.

For further information on obtaining and installing feature licenses, see Configuring the Cisco IOS Software Activation Feature .



CHAPTER 7

# Software Maintenance Upgrade

The Software Maintenance Upgrade (SMU) is a feature used to deliver critical software fixes without requiring a full image upgrade.


- Software Maintenance Upgrade package, on page 65


# Software Maintenance Upgrade package

The Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or security resolution to a released image for a specific defect in order to respond to immediate issues. It does not contain new features.

- SMUs are provided on a per release, per component basis and are specific to the platform. SMU versions are synchronized to the package major, minor, and maintenance versions they upgrade.
- SMUs are not an alternative to maintenance releases; all defects fixed by SMUs are automatically integrated into upcoming maintenance releases.
- The Cisco IOS XE platform internally validates SMU compatibility and does not allow installation of non-compatible SMUs, based on rules and limitations for a SMU change-set.
- An SMU allows you to address network issues quickly while reducing the time and scope of required testing compared to classic IOS software.
- SMU is a method to fix bugs in an existing release and allows the application of a PSIRT fix in an existing release.
- SMU is NOT an upgrade path from release X to release Y.

### Hot Patching in SMU

The device only supports:

- The running image is modified in-place or in-service.
- This avoids downtime and interruption of service.
- The updated code to fix the defect is written in a different location, and the patch redirects the program run.

# SMU workflow requirements

The workflow for the patch requires that you complete these sequence of operations in exec mode:

1. Addition of the SMU to the file system.
2. Activation of the SMU onto the system.
3. Committing the SMU change.
4. Removal and uninstallation of the SMU.

The basic requirements for SMU are:

- The image where the defect was discovered.
- The patch file that contains the fix for the defect must be formatted as ir8100-image_name.release_version.CSCxxyyyyy.SPA.smu.bin.

# Install a patch image

**Before you begin**

**Note** Use this task as an example of a patch created as a test. Your patch will have a name associated with a CDET to be installed as a fix.

Use these steps to install the patch image:

**Procedure**

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **show power** command to verify the overall power consumption.

```
Router# show power
Main PSU :
Total Power Consumed: 11.37 Watts
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 : 30 WattsRouter#
```

**Step 3** Use the **install add file bootflash:***image-file* command to add the image.

```
Router# install add file
bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V 17_5_0_148.SSA.bin
 CSCxx12345.SSA.smu.bin
```

```
install_add: START Thu Aug  6 11:52:52 PDT 2020
cat: /tmp/patch/patch.sta: No such file or directory
install_add: Adding SMU
install_add: Checking whether new add is allowed ....
--- Starting SMU Add operation ---
Performing SMU_ADD on Active/Standby
[1] SMU_ADD package(s) on R0
[1] Finished SMU_ADD on R0
Checking status of SMU_ADD on [R0]
SMU_ADD: Passed on [R0]
Finished SMU Add operation
SUCCESS: install_add  Thu Aug  6 11:53:31 PDT 2020
Router#
```

**Step 4** Use the **install activate file bootflash:***image-file* command to activate the patch image.

```
Router# install activate file
bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V 17_5_0_148.SSA.bin
 CSCxx12345.SSA.smu.bin

install_activate: START Thu Aug  6 11:53:59 PDT 2020
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]
y
Building configuration...
[OK]Modified configuration has been saved
install_activate: Activating SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on Active/Standby
/usr/sbin/kgv_update: kgv_update [
/flash1/ir8100-universalk9.2020-08-06_10.38_shchang2.0.CSCxx12345.SSA.smu.bin, NOT slot
local is ics ] continuing ....
/usr/sbin/kgv_update: Signature validated for
/flash1/ir8100-universalk9.2020-08-06_10.38_shchang2.0.CSCxx12345.SSA.smu.bin
/usr/sbin/kgv_update: TAM hash len:32
val:4407CBB447F0EEE3B12120D902F48FBA1C0D4900EED1FB614441198BE2302934
/usr/sbin/kgv_update: PCR8 before extend ctr:2
0817449B454BF036AF9D593D726D94D8942C50A9FFE93278FDA78EA62F2989F2
/usr/sbin/kgv_update: PCR8 after extend ctr:3
EF5F579FCDFA989D044296F0584B99F719F2B6215895524B5E8AD55DF5671560
/usr/sbin/kgv_update: PCR extend successful
/usr/sbin/kgv_update: Chasfs updated for
name:bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V
17_5_0_148.SSA.bin CSCxx12345.SSA.smu.bin
hash:975352C1562A492D582D09D5EB91230863F6CC18E6F9C0EB512AF27CC0C77E2C05F29596AD34AD7808C9B39EC23D4412F0D3AFA707BC906FE03D554A845E42D4
/usr/sbin/kgv_update: Update successful for
bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V 17_5_0_148.SSA.bin
 CSCxx12345.SSA.smu.bin
[1] SMU_ACTIVATE package(s) on R0
[1] Finished SMU_ACTIVATE on R0
Checking status of SMU_ACTIVATE on [R0]
SMU_ACTIVATE: Passed on [R0]
Finished SMU Activate operation
SUCCESS: install_activate flash1/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V
 17_5_0_148.SSA.bin CSCxx12345.SSA.smu.bin
Thu Aug  6 11:55:14 PDT 2020
Router#
```

**Step 5** Use the **install commit** command to commit the installation.

```
Router# install commit
install_commit: START Thu Aug  6 11:55:29 PDT 2020
install_commit: Committing SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on Active/Standby
[1] SMU_COMMIT package(s) on R0
[1] Finished SMU_COMMIT on R0
Checking status of SMU_COMMIT on [R0]
SMU_COMMIT: Passed on [R0]
Finished SMU Commit operation
SUCCESS: install_commit flash1/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V
 17_5_0_148.SSA.bin CSCxx12345.SSA.smu.bin Thu Aug  6 11:56:08 PDT 2020
Router#
```

**Step 6** Use the **show install summary** command to display the status summary of the installation.

```
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    17.04.01.0.118999
SMU   C    bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V
17_5_0_148.SSA.bin CSCxx12345.SSA.smu.bin
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
Router#
```

**Step 7** Use the **show power** command to verify the result of the patch by showing the same command.

```
Router# show power
Main PSU :
Total Power Consumed: 11.04 Watts
Device HOT SMU works!
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 : 0 Watts
Router#
```

# Uninstall patch image using rollback

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **show install summary** command to display the install summary.

**Example:**

```
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    17.04.01.0.118999
SMU   C    bootflash:/ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V
17_5_0_148.SSA.bin CSCxx12345.SSA.smu.bin
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
Router#
```

**Step 3** Use the **install ?** command to view all the available commands.

**Example:**

```
Router# install ?
abort             Abort the current install operation
activate          Activate an installed package
add               Install a package file to the system
auto-abort-timer  Install auto-abort-timer
commit            Commit the changes to the loadpath
deactivate        Deactivate an install package
label             Add a label name to any installation point
prepare           Prepare package for operation
remove            Remove installed packages
rollback          Rollback to a previous installation point
Router# install rollback to ?
base       Rollback to the base image
committed  Rollback to the last committed installation point
id         Rollback to a specific install point id
label      Rollback to a specific install point label
```

**Step 4** Use the **install rollback to base** command to restore the image to its original version.

**Example:**

```
Router# install rollback to base
install_rollback: START Thu Aug  6 12:04:04 PDT 2020
install_rollback: Rolling back SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on Active/Standby
[1] SMU_ROLLBACK package(s) on R0
[1] Finished SMU_ROLLBACK on R0
Checking status of SMU_ROLLBACK on [R0]
SMU_ROLLBACK: Passed on [R0]
Finished SMU Rollback operation
CSCxx12345:SUCCESS
SUCCESS: install_rollback
/flash1/ir8100-universalk9.2020-08-06_10.38_shchang2.0.CSCxx12345.SSA.smu.bin Thu Aug  6
12:04:57 PDT 2020
Router#
```

**Step 5** Use the **show install summary** command to display the installed patches.

**Example:**

```
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    17.04.01.0.118999
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
Router#
```

**Note** In the above command output, the patch has been removed and the device returns to the base image version prior to the upgrade.

**Step 6** Use the **show power** command to verify the result of the patch.

**Example:**

```
Router# show power
Main PSU :
Total Power Consumed: 11.98 Watts
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 : 30 Watts
Router#
```

# Uninstall the patch image using deactivate, commit, and remove commands

**Note** In this task there are two patches installed on the devices: CSCvq11111 and CSCvt22222. but only CSCvt22222 will be removed.

**Procedure**

**Step 1** Use the **show install summary** command to display the installation and patch details.

**Example:**

```
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
--------------------------------------------------------------------------------
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvq11111.SPA.smu.bin
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
IMG   C    17.04.1
```

**Step 2** Use the **install deactivate file bootflash:** *patch-file* command to deactivate the patch.

```
Router# install deactivate file bootflash:/ir8100-universalk9.release.CSCvt22222.SPA.smu.bin
install_deactivate: START Fri Apr 24 22:54:10 UTC 2020
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Deactivate operation ---
Performing SMU_DEACTIVATE on Active/Standby
[R0] SMU_DEACTIVATE package(s) on R0
[R0] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation
SUCCESS: install_deactivate /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin Fri
 Apr 24 22:54:49 UTC 2020
```

**Step 3** Use the **show install summary** command to display the installed patches.

**Example:**

```
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
  --------------------------------------------------------------------------------
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvt11111.SPA.smu.bin
SMU   D    /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
IMG   C    17.01.1
```

**Step 4** Use the **install commit** command to save.

```
Router# install commit
install_commit: START Fri Apr 24 22:56:11 UTC 2020
install_commit: Committing SMU

*Apr 24 22:56:15.169: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commitExecuting pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on Active/Standby
  [R0] SMU_COMMIT package(s) on R0
  [R0] Finished SMU_COMMIT on R0
Checking status of SMU_COMMIT on [R0]
SMU_COMMIT: Passed on [R0]
Finished SMU Commit operation

SUCCESS: install_commit /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin Fri Apr
 24 22:56:32 UTC 2020

*Apr 24 22:56:33.342: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit SMU
```

**Step 5** Use the **show install summary** command to display the installed patches.

**Example:**

```
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
--------------------------------------------------------------------------------
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvt11111.SPA.smu.bin
SMU   I    /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
IMG   C    <release>
```

**Step 6** Use the **install remove file flash:** *patch-file* command to remove the patch.

**Example:**

```
Router# install remove file flash:ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
install_remove: START Fri Apr 24 22:57:17 UTC 2020

*Apr 24 22:57:20.775: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 remove flash:ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bininstall_remove: Removing
SMU
Executing pre scripts....
Executing pre scripts done.

--- Starting SMU Remove operation ---
Performing SMU_REMOVE on Active/Standby
  [R0] SMU_REMOVE package(s) on R0
  [R0] Finished SMU_REMOVE on R0
Checking status of SMU_REMOVE on [R0]
SMU_REMOVE: Passed on [R0]
Finished SMU Remove operation

SUCCESS: install_remove /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin Fri Apr
 24 22:57:34 UTC 2020

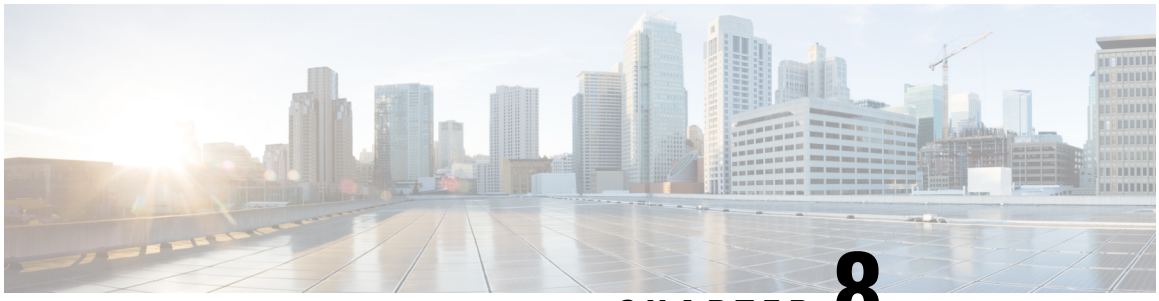
*Apr 24 22:57:34.902: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install remove flash:ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
```

Show what patches are installed:

**Step 7** Use the **show install summary** command to display the installed patches.

**Example:**

```
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
 --------------------------------------------------------------------------------
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvt11111.SPA.smu.bin
SMU   I    /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
IMG   C    <release>
```



CHAPTER 8

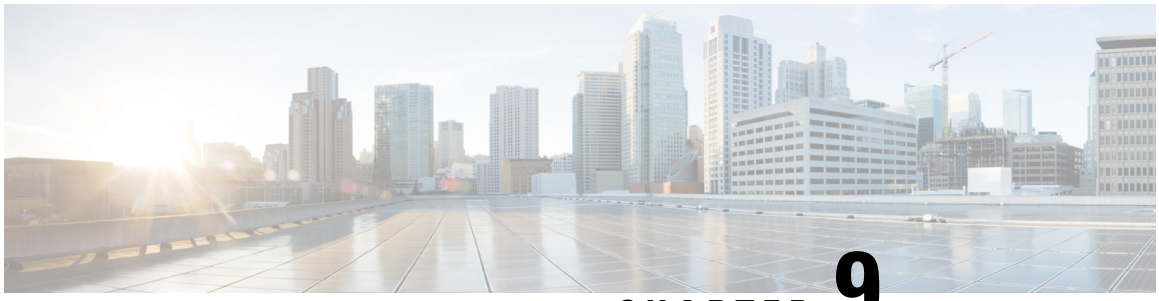
# Smart Licensing Using Policy (SLP)

This document outlines the core concepts and operational requirements for implementing Smart Licensing Using Policy.


- Smart licensing using policy on Cisco routers, on page 73


## Smart licensing using policy on Cisco routers

The Smart Licensing Using Policy chapter has been replaced by a standalone guide called Smart Licensing Using Policy on the Cisco Catalyst IR1101, IR1800, IR8140, IR8340 and ESR6300 Routers.



CHAPTER 9

# Battery Backup Unit (BBU)

This reference provides technical specifications and functional details for the Battery Backup Unit (BBU).


- Battery Backup Units, on page 75
- BBU mode configurations, on page 75
- Upgrade the BBU, on page 79


## Battery Backup Units

The integrated modular battery backup unit (BBU) is a smart charging and monitoring system for the IR8100 router.

- Supplies power to the router when AC power is turned off.
- Allows graceful shutdown of router events based on configured voltage level thresholds.
- Supports up to three BBU units installed on the system.

### Battery Backup Unit reference information

The BBU Product ID (PID) for the IR8100 is CGR-BATT-4AH.

## BBU mode configurations

The BBU (Battery Backup Unit) mode determines whether the router uses battery power when AC power is unavailable. Disabling or enabling the BBU affects battery life and system operation.

- Disabling the BBU preserves battery life during storage, shipping, or transportation.
- Disabling the BBU allows safe battery replacement in an operating router.

### BBU mode configuration details

The BBU automatically supplies power to the router when AC power is not available. You can enable or disable the BBU as needed.

**Note** When the BBU is disabled by the `request platform hardware battery disable` command, the router will shut down if not powered by AC power. The BBU cannot be charged while disabled.

# Enable BBU

To enable the BBU in the router, follow these steps.

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **request platform hardware battery enable** command to enable the battery.

**Example:**

```
Router# request platform hardware battery enable
```

**Step 3** Confirm the action when prompted.

**Example:**

```
Proceed with enabling battery?[confirm]
Battery enabled.
Router# Aug 16 22:26:01.473: %BBU-5-CLI_OK: R0/0: bbu: Command Battery enabled
```

**Step 4** Use the **show platform hardware battery unit** command to check the BBU status.

**Example:**

```
Router# show platform hardware battery unit
Battery pack state: Operational
Battery unit                 0           1           2
----------------------------+-----------+-----------+-----------
Status ...................          Idle        Idle        Full
Battery Mode .............       enabled     enabled     enabled
Charge level .............           90%         91%         96%
Capacity Remaining   (mAh)          5235        5225        5545
Full Charge Capacity (mAh)          5739        5739        5739
Voltage ............. (mV)         11736       11714       11869
Current ............. (mA)             0           0           0
Temperature ......... ('C)            30          31          31
Firmware version .........          1224        1224        1224
```

# Disable BBU

To disable the BBU in the router, follow these steps.

**Procedure**

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **request platform hardware battery disable** command to disable the BBU.

**Example:**

```
Router# request platform hardware battery disable
```

**Step 3** Confirm the action when prompted.

**Example:**

```
Router will shut down if not powered by AC Power. Proceed with disabling battery?[confirm]
Battery disabled.
Router# Aug 16 22:26:16.647: %BBU-5-CLI_OK: R0/0: bbu: Command Battery disabled
```

**Step 4** Use the **show platform hardware battery unit** command to check the BBU status.

**Example:**

```
Router# show platform hardware battery unit
Battery pack state: Operational
Battery unit                 0           1           2
----------------------------+-----------+-----------+-----------
Status ...................          Idle        Idle        Full
Battery Mode .............      disabled    disabled    disabled
Charge level .............           91%         91%         96%
Capacity Remaining   (mAh)          5236        5219        5534
Full Charge Capacity (mAh)          5739        5739        5739
Voltage ..............  (mV)        11732       11714       11869
Current ..............  (mA)            0           0           0
Temperature .........  ('C)           30          31          31
Firmware version .........          1224        1224        1224
```

# Reset BBU

To reset the BBU in the router:

**Procedure**

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **request platform hardware battery reset enable** command to disconnect the communications with the battery.

**Example:**

```
Router# request platform hardware battery reset enable
```

**Step 3** Confirm the action when prompted.

**Example:**

```
Proceed with enabling reset?[confirm]
Battery reset enabled.
```

**Step 4** Use the **request platform hardware battery reset enable** command to verify the BBU status.

**Example:**

```
Router# show platform hardware battery unit
Battery is not ready
Battery pack state: Not available
```

**Step 5** Use the **request platform hardware battery reset disable** command to reconnect communications with the battery.

**Example:**

```
Router# request platform hardware battery reset disable
```

**Step 6** Confirm the action when prompted.

**Example:**

```
Proceed with disabling reset?[confirm]
Battery reset disabled.
```

**Step 7** Use the **show platform hardware battery unit** command to verify the BBU status.

**Example:**

```
Router# show platform hardware battery unit
Battery pack state: Operational
Battery unit                 0           1
---------------------------+-----------+-----------
Status ...................          Full        Full
Battery Mode .............       enabled     enabled
Charge level .............           87%        100%
Capacity Remaining   (mAh)          5907        6875
Full Charge Capacity (mAh)          6821        6944
Voltage ..............  (mV)         11996       12244
Current ..............  (mA)             0           0
Temperature .........  ('C)            30          31
Firmware version .........          6273        6273
```

# Enable or disable transportation mode on the router

When the router has the BBU transportation mode set, inhibit discharge is enabled when AC is ON and inhibit discharge is disabled when AC is OFF. So, effectively the battery can be charged, but does not discharge. Transportation mode setting is persistent on system reload.

To enable the BBU to transportation mode in the router:

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **request platform hardware battery transportation-mode enable** command to enable the transportation-mode.

**Example:**

```
Router# request platform hardware battery transportation-mode enable
```

**Step 3** Confirm the action when prompted.

**Example:**

```
Proceed with enabling transportation-mode?[confirm]
Battery transportation-mode enabled.
```

**Step 4** Use the **show platform hardware battery unit** command to verify the BBU status.

**Example:**

```
Router# show platform hardware battery unit
Battery pack state: Operational (Transportation mode)
Battery unit                 0           1
---------------------------+-----------+-----------
Status ...................          Full        Full
Battery Mode .............       enabled     enabled
Charge level .............           87%        100%
Capacity Remaining   (mAh)          5907        6875
Full Charge Capacity (mAh)          6821        6944
Voltage ............. (mV)         11994       12245
Current ............. (mA)             0           0
Temperature ......... ('C)            30          31
Firmware version .........          6273        6273
```

**Step 5** Use the **request platform hardware battery transportation-mode disable** command to disable the transportation mode.

**Example:**

```
Router# request platform hardware battery transportation-mode disable
```

**Step 6** Confirm the action when prompted.

**Example:**

```
Proceed with disabling transportation-mode?[confirm]
Battery transportation mode disabled.
```

# Upgrade the BBU

It is recommended that you keep the software up to date to ensure that the router works with the latest features and bug fixes.

To upgrade the BBU in the router:

**Before you begin**

Ensure your device is running IOS-XE 17.9.1 or later before proceeding with the upgrade.

## Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **bbu_fw** command to create a new directory.

**Example:**

```
Router# mkdir bootflash:/bbu_fw
Create directory filename [bbu_fw]?
Created dir bootflash:/bbu_fw
```

**Step 3** Copy the firmware file (**BMZ_06273.bin.SPA**) to the **bbu_fw** directory using SCP or another file transfer method.

**Example:**

```
Router# dir bootflash:/bbu_fw
Directory of bootflash:/bbu_fw/
259127  -rw-           27624   Oct 7 2024 20:23:23 +00:00  BMZ_06273.bin.SPA7228108800
bytes total (5388279808 bytes free)
```

**Note** An image stored in a local file will be used to upgrade the BBU firmware through the cli. Prior to installation, the firmware image will be signed and verified. BBU firmware images and IR1840 images will be posted to Cisco.com. For more information, contact Cisco Support.

**Step 4** Use the **show platform hardware battery short** command to verify AC power supply is on and the firmware version is the old version ( **8302** ).

**Example:**

```
Router# show platform hardware battery short
AC power supply ......... ON
Battery present ......... YES
Battery ready ........... YES
Transportation mode ..... NO
Number of battery units . 1
Time to empty ........... 3:15
Unit#  Charge  Time to empty  State        Firmware  Battery Mode
------+-------+-------------+------------+---------+--------------------
0     37%           3:15         Idle

8302

enabled
```

**Step 5** Use the **request platform hardware battery firmware-update install** command to upgrade the firmware.

**Example:**

```
Router# request platform hardware battery firmware-update install
bootflash:/bbu_fw/BMZ_06273.bin.SPA
Proceed with bbu firmware upgrade?[confirm]
Battery firmware upgrade starting
```

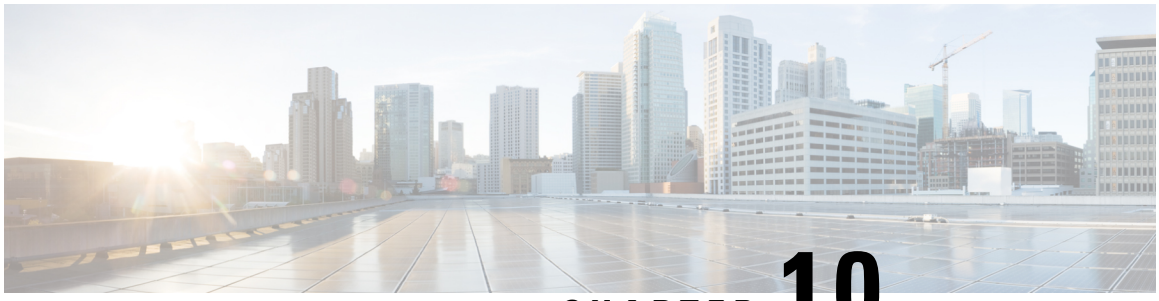
**Example:**

```
Oct  7 20:35:47.039: %BBU-5-CLI_OK: R0/0: bbu: Command Battery firmware upgrade starting
Oct  7 20:35:47.477: %BBU-7-FSM_TRANSITION: R0/0: bbu: FSM transition (3, 2) -> 2
Oct  7 20:35:48.478: %BBU-4-FW_UPGRADE_STARTED: R0/0: bbu: Firmware upgrade to version 6273
 started
Oct  7 20:35:59.637: %BBU-3-COMM_ERR: R0/0: bbu: Battery communication error: select timed
 out
Oct  7 20:36:07.598: %BBU-5-FW_UPGRADE_FINISHED: R0/0: bbu: Firmware upgrade finished
successfullyOct  7 20:36:07.599: %BBU-7-FSM_TRANSITION: R0/0: bbu: FSM transition (2, 2)
-> 0
Oct  7 20:36:14.807: %BBU-5-BBU_EVT_LOG: R0/0: bbu: Battery Event Log - BBU Event Data is
written to log file:success
Oct  7 20:36:14.811: %BBU-7-FSM_TRANSITION: R0/0: bbu: FSM transition (0, 2) -> 3
```

**Note** Do not interrupt the process until it is complete.

**Step 6** Use the **show platform hardware battery short** command to verify that the firmware upgrade is successful.

```
Router# show platform hardware battery short
AC power supply ......... ON
Battery present ......... YES
Battery ready ........... YES
Transportation mode ..... NO
Number of battery units . 1
Time to empty ........... 2:39
Unit#  Charge  Time to empty  State        Firmware  Battery Mode
------+-------+--------------+------------+---------+--------------------
0     37%           2:39     Charging
6273
enabled
```



CHAPTER 10

# Tamper detection

This reference provides information regarding the tamper detection capabilities and security monitoring functions of the hardware.


- Tamper detection scenarios, on page 83


# Tamper detection scenarios

Cisco Catalyst IR8140H routers use IR sensors and switches to detect tampering events such as module or cover removal in Unified Inventory Management (UIM) slots and the BBU unit.

- IR sensors in UIM slots detect the presence or absence of slot covers or modules.
- A switch on the BBU board monitors BBU removal in progress.
- Alarms and events are generated when tampering is detected and sent to Cisco IOT-FND.

### Tamper detection mechanisms and scenarios

Cisco Catalyst IR8140H routers provide IR sensors for cover detection in the UIM slots, and a switch on the BBU board for the BBU unit. For each UIM slot, IR8140H routers have an IR Time of Flight sensor to detect the distance to the slot cover when there is no UIM installed in the slot. If no cover is detected, an alarm syslog message is generated. If the router is registered to Cisco IOT-FND, a corresponding event is also sent to Cisco IOT-FND.

The cover detection applies for these scenarios:

- Any UIM module is removed during operation.
- The cover for an unused UIM slot is removed.
- BBU removal detected in progress (through a switch on the BBU board).

In cases where the Supervisor (CPU) module is removed or the BBU is removed (if its alarm could not be sent when the BBU removal in progress was detected), a tamper indication is stored in the flash of the secondary MCU, which allows IR8140H routers to send an alarm to Cisco IOT-FND at a later time.

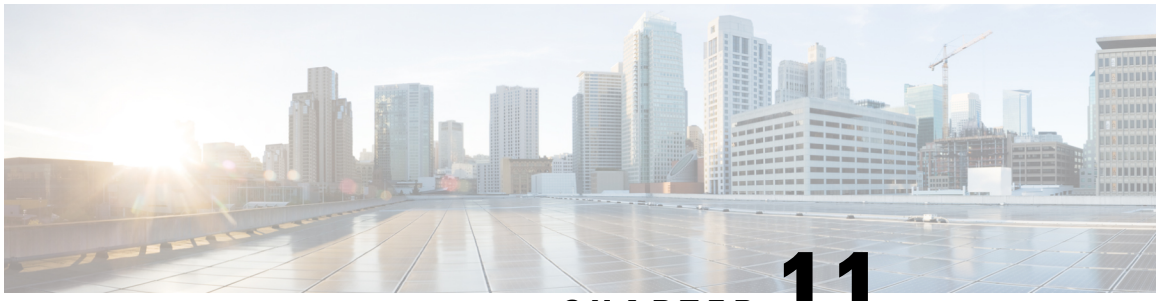
**Note** The ability to send the alarm to Cisco IOT-FND depends on the WAN interface (Ethernet or LTE connectivity) being available at the time of the occurrence of the tamper detection.

**Note** It is recommended to power down the module prior to physically removing it, using these CLI commands:

```
IR8140H(config)# hw-module subslot 0/3 shutdown unpowered
```

After inserting the replacement module, power it up using this command:

```
IR8140H(config)# no hw-module subslot 0/3 shutdown unpowered
```



CHAPTER 11

# Power Over Ethernet (PoE)

Provides information on the functionality and implementation of Power Over Ethernet to support network device connectivity.


- Power over Ethernet, on page 85
- Device detection and power allocations, on page 85
- Power budget calculation for router connected modules, on page 86
- Key considerations, on page 86
- Configure PoE using CLI, on page 87
- Verify PoE configuration, on page 87
- Debugging commands for PoE, on page 89


## Power over Ethernet

Power over Ethernet (PoE) is a network technology which allows transmission of both power and data over a single Ethernet cable. It is typically used to power up devices such as Access Points, IP Cameras and IP Phones connected to the device's Ethernet port Gi0/0/0 as per IEEE 802.3AF and AT standards.

The total PoE available power budget is fixed as 15.4 W which is used entirely by Gi0/0/0 interface. When PoE is enabled, the router detects the connected devices and allocates power based on the device types.

Starting with Cisco IOS XE Release 26.1.1, Cisco Catalyst IR8140 Heavy Duty Series Routers can provide up to 30 W of power per port to connected devices over Ethernet.

***Table 11: Feature History Table***

| Feature name | Release information | Feature description |
|---|---|---|
| Power over Ethernet Plus Support | Release 26.1.1 | Cisco Catalyst IR8140 Heavy Duty Series Routers can provide up to 30 W of power per port to connected devices over Ethernet. |

## Device detection and power allocations

After the device detection:

- The router detects a Cisco pre-standard or an IEEE-compliant power device when the PoE is enabled and the connected device is not being powered by an AC adapter.
- The router determines the power requirement based on the power classification class of the connected device.
- The router checks the available power budget to decide if it can power the port or not.
- The router initially allocates a class max power when it detects a device and then powers it on.
- Further power negotiation happens using the Cisco Discovery Protocol (CDP) / Link Layer Discovery Protocol (LLDP) protocols.



**Note** During reloading the device, the PoE ports remain powered down until the unit reboots.

# Power budget calculation for router connected modules

Starting with Cisco IOS XE Release 26.1.1, the IR8140H-P-K9 router calculates the power budget during system boot. The IR8140H-P-K9 supports 60 W of power supply.

To calculate power budget allocation for PoE:

***Table 12: Power budget calculation***

| Module | Consumed Power |
|---|---|
| System reservation | 15 W |
| SPA module (WPAN, LTE, etc.) | 5 W |
| mSATA module | 2.5 W |
| BBU | 24 W |

# Key considerations

Starting with Cisco IOS XE Release 26.1.1 consider these points:

- You must avoid online insertion and removal of modules (OIR), on the router to avoid power unavailability issues and undefined behavior of the devices.
- The power budget is calculated only once during system boot-up, based on the connected modules at a given time.
- If you power down or power up a module after system boot, the power budget allocation does not change because it is fixed at boot time.

- To manage power reliably and prevent any shortages, ensure that modules are installed or removed only before booting the system.
- Replacing a module with another module of the same type after system boot, does not affect the power budget allocation because the system retains the original allocation.

# Configure PoE using CLI

Follow this procedure to configure PoE or PoE+ for connected modules of IR8140H-P-K9 router.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the config mode.

**Example:**

```
Router#configure terminal
```

**Step 2** Use the **interface** [*interface-id*] command to enter the interface id.

**Example:**

```
Router(config-if)#interface g0/0/0
```

**Step 3** Use the **power inline** {**auto**|**never**} command to enable PoE.

**Example:**

```
Router(config-if)#power inline {auto|never}
```

**What to do next**

Verify the configuration.

# Verify PoE configuration

Follow this procedure to verify PoE or PoE+ configuration for connected modules of R8140H-P-K9 router.

**Procedure**

**Step 1** Use the **show power inline** command to verify PoE or PoE+ configuration for connected modules of router.

**Example:**

```
Router#show power inline
Available:15.4(w) Used:6.4(w) Remaining:9.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
```

```
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         6.4     IP Phone 8845       2     15.4
```

**Example:**

```
Router#show power inline
Available:31.0(w)  Used:30.0(w)  Remaining:1.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         30.0    WS-C3560CX-8PT-S    4     30.0
--------- ------ ---------- ---------- ---------- ------ -----
Totals:          1    on    30.0
```

**Step 2** Use the **show power inline** [*interface-id*] command to display power of a particular interface.

**Example:**

```
Router#show power inline Gi0/0/0
```

**Step 3** Use the **show power inline** [*interface-id*] **detail** command to display PoE status for a router for the specified interface.

**Example:**

```
Router#show power inline Gi0/0/0 detail
```

**Step 4** Use the **show power** command to display power consumption.

**Example:**

```
Router#show power
Main PSU :
  Total Power Consumed: 24.19 Watts
  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 : 15.4 Watts
```

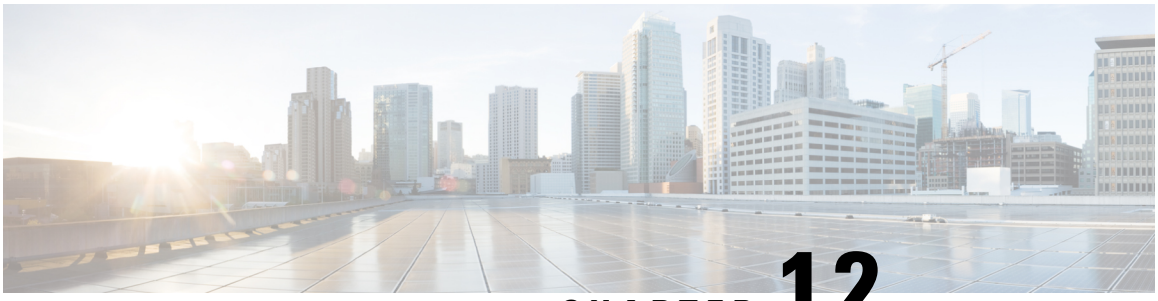
**Example:**

```
Router#show power
Main PSU :
    Total Power Consumed: 34.76 Watts
    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 : 31.0 Watts
```

# Debugging commands for PoE

The list of commands for debugging PoE are given in the table:

| Command | Description |
|---|---|
| Debug ilpower controller | Display PoE controller debug messages |
| 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 |



CHAPTER 12

# Support for IRMH-5GS6-RC-GL UIM


- Support for IRMH-5GS6-RC-GL UIM, on page 91


# Support for IRMH-5GS6-RC-GL UIM

The IRMH-5GS6-RC-GL is a 3GPP Release 17 5G Reduced Capability (RedCap) Universal Interface Module (UIM) for the Cisco Catalyst IR8140 Heavy Duty Router. It provides 5G Standalone (5G SA) RedCap and 4G LTE connectivity for industrial applications that require reliable cellular connectivity with moderate throughput.

### Benefits of the IRMH-5GS6-RC-GL UIM

The IRMH-5GS6-RC-GL UIM:

- Provides a migration path from existing LTE networks to 5G SA RedCap networks.
- Enables you to upgrade cellular technology without replacing the IR8140 router.
- Supports a broad range of LTE and 5G NR Sub-6 GHz frequency bands for deployment across multiple regions.
- Supports SGP.32-Compliant eSIM for flexible SIM profile management.
- Provides an affordable, long-term cellular connectivity option for primary or secondary WAN deployments.

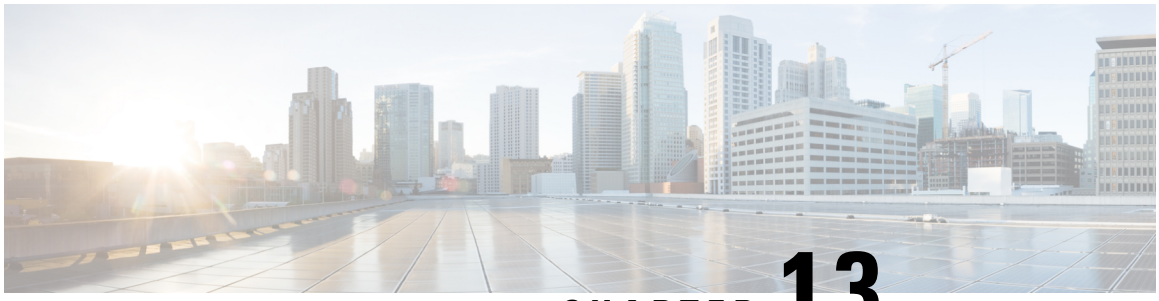
**Note** The IRMH-5GS6-RC-GL UIM supports 5G RedCap connectivity only on a 5G SA network offering RedCap service. It does not support 5G Non-Standalone (NSA) operation. When 5G SA RedCap service is unavailable, the module can use supported 4G LTE service, subject to network availability and carrier support.

### Support for QCI

Support for QoS Class Identifier and 5G QoS Identifier (5QI) on EM8695 modem is provided for:

- QCI: 1-9, 65-67, 69-76, 79, 80, 82-85.
- 5QI: 1-9, 65-67, 69-76, 79, 80, 82-85.

Support for IRMH-5GS6-RC-GL UIM



CHAPTER 13

# 12V DC output for third party device

This reference provides the technical requirements and output capabilities for the 12V DC power interface.


- 12V DC outputs, on page 93


## 12V DC outputs

The 12V DC output for 3rd party devices provides 1 Amp of power at 12V with current limiting at 1.5A and fuse protection at 5A. Output is 12V +/- 10%.

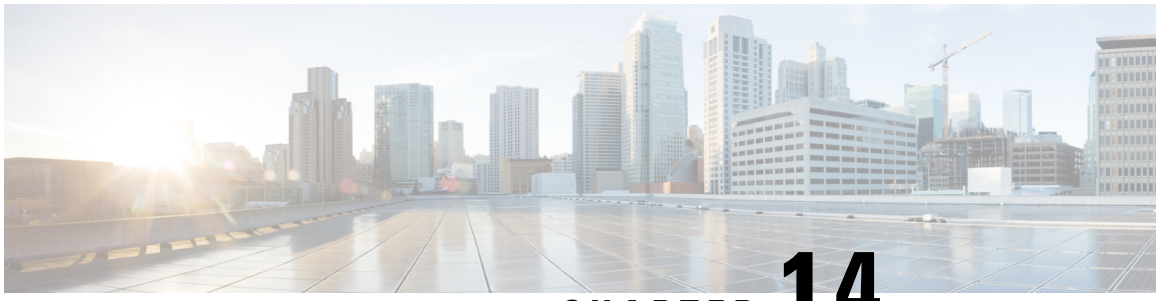
To enable 12v-output, enter the following command in global configuration mode:

```
Router(config)# platform 12v-output enable
```

To disable 12v-output, enter the following command in global configuration mode:

```
Router(config)# no platform 12v-output enable
```

**Note** PoE and 12V configuration are mutually exclusive.



CHAPTER 14

# NTP timing based on GPS clock

This reference details the configuration and operational requirements for integrating a GPS clock source with NTP to maintain accurate system time.

• Configure NTP using GPS time, on page 95

# Configure NTP using GPS time

You can configure the GPS time as the reference clock for NTP using the command **ntp refclock gps**.

The GPS time acts as a stratum 0 source, and the Cisco IOS NTP server acts as a stratum 1 device, which in turn provides clock information to its NTP clients (stratum 2 and 3).

### Procedure

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **ntp refclock gps** command to configure the NTP reference clock as GPS:

**Example:**

```
Router(config)# ntp refclock gps
```

**Step 4** Use the **ntp refclock gps** command to verify the configuration.

**Example:**

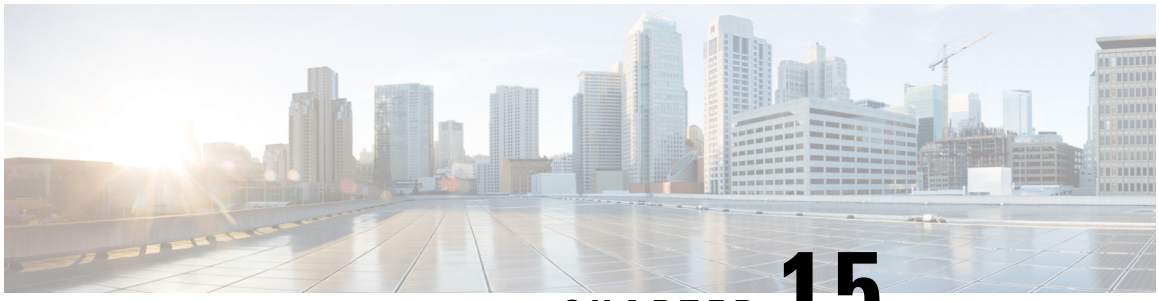
```
Router#
Sep 24 19:58:43.046 GMT: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Router# show ntp status
Clock is synchronized, stratum 1, reference is .GPS.
nominal freq is 250.0000 Hz, actual freq is 249.9970 Hz, precision is 2**10
ntp uptime is 94000 (1/100 of seconds), resolution is 4016
reference time is E31778F3.0B851ED8 (19:58:43.045 GMT Thu Sep 24 2020)
```

```
clock offset is 11.0000 msec, root delay is 0.00 msec
root dispersion is 3950.55 msec, peer dispersion is 3938.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000011995 s/s
system poll interval is 64, last update was 7 sec ago.
Router#
Router#
Router#
show ntp associations
address ref clock st when poll reach delay offset disp
*~127.127.5.1 .GPS. 0 38 64 7 0.000 11.000 1938.8
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router# show clock
20:00:43.660 GMT Thu Sep 24 2020
```

**Step 5** Use the **debug ntp refclock** command to troubleshoot the configuration.

**Example:**

```
Router# debug ntp ?
adjust NTP clock adjustments
all NTP all debugging on
core NTP core messages
events NTP events
packet NTP packet debugging
refclock NTP refclock messages
Router# debug ntp re
Router#debug ntp refclock
*Sep 24 19:58:43.045 GMT: GPS: Poll Requested
*Sep 24 19:58:43.045 GMT: GPS (19:58:43.056 GMT Thu Sep 24 2020)
*Sep 24 19:58:43.045 GMT: Valid time rcvd from GPS: 2020/09/24 19:58:43.056 (frac =
0x0E560440)
*Sep 24 19:58:43.045 GMT: RTS poll timestamp (local clock) was 0xE31778F3.0B851ED8
*Sep 24 19:58:43.045 GMT: GPS timestamp is 0xE31778F3.0E560440
*Sep 24 19:58:43.045 GMT: NTP Core(NOTICE): ntpd PPM
*Sep 24 19:58:43.046 GMT: NTP Core(NOTICE): trans state : 5
*Sep 24 19:58:43.046 GMT: NTP Core(NOTICE): Clock is synchronized.
```



CHAPTER 15

# vCPU and RAM distribution

This reference provides the configuration details for vCPU and RAM distribution across the infrastructure.


- Introduction, on page 97
- Distribution of vCPU and RAM resources for Cisco IOx applications, on page 97
- Higher CPU and RAM allocation for IOx applications, on page 98
- Configure data plane heavy template, on page 98
- Verify the active vCPU and RAM distribution, on page 99
- Configure the Service Plane Heavy Template, on page 100
- Verify the active vCPU and RAM distribution, on page 100


# Introduction

The vCPU resource allocation is a configuration process that manages how physical processor cores and memory are assigned to Cisco IOx applications.

- vCPU is also known as physical processor.

# Distribution of vCPU and RAM resources for Cisco IOx applications

Distribution of vCPU and RAM resources for Cisco IOx applications refers to the allocation of processing and memory resources to optimize application performance on Cisco Catalyst IR8100 router.

- Resource distribution enables running multiple IOx applications simultaneously.
- Templates are available for Data Plane Heavy and Service Plane Heavy configurations.
- vCPU is also known as physical processor.

### Templates for vCPU and RAM distribution

Two main templates are used to distribute vCPU and RAM resources for IOx applications on the Catalyst IR8100 router:

- **Data Plane Heavy** —Refers to a router configuration where most of the system resources are dedicated to the data plane, which is responsible for processing and forwarding network packets. This template maximizes throughput and ensures high-speed packet transfer, providing more processing power and memory to handle increased data plane load. The Data Plane Heavy template is the default for vCPU and RAM distribution in the IR8100 router.
- **Service Plane Heavy** —Refers to a router configuration where most of the system resources are allocated to the service plane, which provides network services such as Quality of Service (QoS), security functions, and load balancing. This template allocates additional vCPU and RAM to IOx applications but reduces data throughput (bandwidth).



**Note** Routers with 2 GB RAM and a single core vCPU (IOx resources) cannot run multiple IOx applications such as Unified Threat Defense and Cisco Cyber Vision.

# Higher CPU and RAM allocation for IOx applications

The IR8100 router with 8 GB RAM, starting from Cisco IOS XE Release 17.15.1, supports Data Plane Heavy and Service Plane Heavy distribution templates for hosting Cisco IOx applications.

- Allows allocation of 3 GB RAM and two vCPU cores to the IR8100 router for IOx applications.
- Supports Data Plane Heavy and Service Plane Heavy distribution templates.
- Service Plane Heavy template is recommended for hosting IOx applications.

# Configure data plane heavy template

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **platform resource data-plane-heavy** command to enable the data plane heavy template:

**Example:**

```
Router(config)# platform resource data-plane-heavy
```

**Step 3** Use the **reload** command to reboot the router and activate the data plane heavy template.

**Example:**

```
Router# reload
```

### What to do next

Verify the active vCPU and RAM distribution.

# Verify the active vCPU and RAM distribution

Follow these steps to verify the active vCPU and RAM distribution for IOx applications.

### Procedure

**Step 1** Use the **show platform software cpu allocation** command to verify the vCPU core allocation for IOx applications.

**Example:**

```
Router# show platform software cpu allocation
CPU alloc information:
Control plane cpu alloc: 0-1
Data plane cpu alloc: 2-3
Service plane cpu alloc: 0-1
Slow control plane cpu alloc:
Template used: CLI-data_plane_heavy
```

**Step 2** Use the **show app-host resource** command to verify the RAM allocation for IOx applications.

**Example:**

```
Router# show app-host resource
Resource Allocation:
CPU Quota: 33%
Memory Quota: 2048MB
Storage Total: 6350MBStorage Available: 1404MB
```

**Step 3** Use the **show app-host infra** command to verify the CPU units resource allocation for IOx applications.

**Example:**

```
Router# show app-host infraIOX version: 2.11.0.3
App signature verification: disabled
CAF Health: Stable
Internal working directory: /vol/harddisk/iox
CPU:
Quota: 33%
Available: 33%
Quota: 1617(Units)
Available: 1617(Units)
```

# Configure the Service Plane Heavy Template

### Procedure

**Step 1** Use the **platform resource service-plane-heavy** command to enable the service plane heavy template.

**Example:**

```
Router(config)# platform resource service-plane-heavy
```

**Step 2** Use the **reload** command to reboot the router and activate the service plane heavy template.

**Example:**

```
Router# reload
```

### What to do next

Verify the active vCPU and RAM distribution.

# Verify the active vCPU and RAM distribution

Use this procedure to confirm the allocation of vCPU cores, RAM, and CPU units for IOx applications on your router after applying the service plane heavy template.

### Procedure

**Step 1** Use the **show platform software cpu allocation** command to verify the vCPU cores allocation for IOx applications.

**Example:**

```
Router#show platform software cpu allocation
CPU Allocation Information:Control plane cpu alloc: 0-1
Data plane cpu alloc: 3
Service plane cpu alloc:
0-2
Template used:
CLI-service_plane_heavy
```

**Step 2** Use the **show app-host resource** command to verify the RAM allocation for IOx applications.

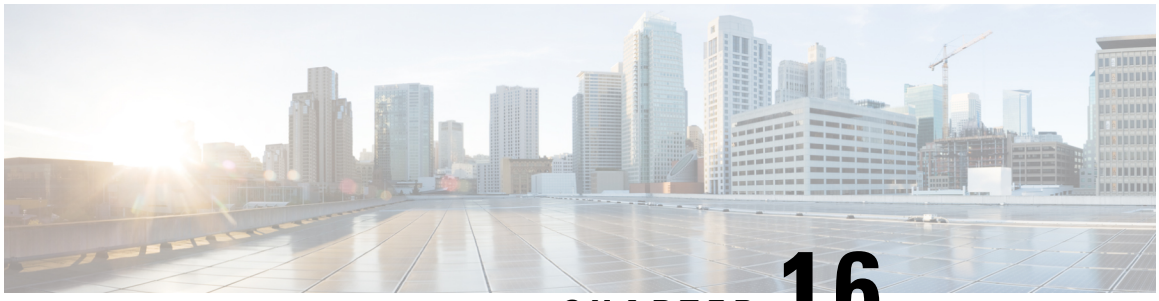
**Example:**

```
Router#show app-host resource
Resource Allocation:
CPU Quota: 38%
Memory Quota:3072MB
Storage Total: 6350MB
Storage Available: 1403MB
```

**Step 3** Use the **show app-host infra** command to verify the CPU units resource allocation for IOx applications.

**Example:**

```
Router#show app-host infra
IOX version: 2.11.0.3
App signature verification: disabled
CAF Health: Stable
Internal working directory: /vol/harddisk/iox
CPU:
Quota: 38%
Available: 38%
Quota: 1862(Units)
Available: 1862(Units)
```



CHAPTER 16

# Cellular pluggable interface modules

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 P-5GS6-R16SA-GL pluggable module, on page 103
- Galileo support on the LTE pluggable modules, on page 103
- Radio signal parameters and GPS coordinates of cellular telemetry monitoring using syslog messages, on page 105
- GPS NMEA unique identifier , on page 106
- Configure cellular modem GPS NMEA unique identifier, on page 108


# Support for P-5GS6-R16SA-GL pluggable module

From Cisco IOS-XE Release 17.18.2, the P-5GS6-R16SA-GL Pluggable Module is supported on ESR6300 routers.

Support for the P-5GS6-R16SA-GL Pluggable Module works the same way on the ESR6300 routers 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

The Cisco IOS XE 17.11.1a release introduces support for the Galileo constellation on LTE pluggable modules.

GPS was the only GNSS constellation supported in earlier releases. The Cisco IOS XE 17.11.1a release introduces support for Galileo constellation.

**Note** You can enable only one constellation at a time.

Configuration command examples:

```
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 galileo and gnss options in this CLI configure Galileo and simultaneous GNSS modes, such as GPS and Galileo.

If you disable the GPS configuration, make sure that no constellation is configured. This maintains consistency with GPS mode configuration.

Example:

```
config#


controller Cellular 0/2/0

(config-controller)# no lte gps constellation gps
```

Show commands example:

**Note** The example shows the current GNSS constellation as Galileo.

Example:

```
config#


show cellular 0/2/0 gps detail

GPS Feature =  enabled
GPS Mode Configured =  standalone
Current Constellation Configured =  galileo
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 .

# Radio signal parameters and GPS coordinates of cellular telemetry monitoring using syslog messages

Cellular telemetry is a feature that enables real-time monitoring and analysis of cellular connection performance by collecting Radio Frequency (RF) parameters and Global Positioning System (GPS) coordinates from the cellular network at a fixed interval of 60 seconds.

- Monitors key radio signal parameters such as RSSI, RSRP, RSRQ, PCI, and SNR.
- Collects GPS coordinates for location tracking.
- Facilitates troubleshooting, network optimization, and ensures reliable connectivity.

### Cellular Telemetry Reference Information

Cellular telemetry parameters that can be monitored include:

- Received Signal Strength Indicator (RSSI)
- Reference Signal Received Power (RSRP)
- Reference Signal Received Quality (RSRQ)
- Physical Cell Identity (PCI)
- Signal to Noise Ratio (SNR)
- Global Positioning System (GPS) coordinates

The Cisco Catalyst WAN Manager does not support cellular telemetry.

# Enable cellular telemetry

To enable the cellular telemetry feature in the contoller cellular interface 0/x/0 using the CLI.

### Before you begin

- Insert the cellular Pluggable Interface Module (PIM) into the IR device.
- Enable GPS in the controller for GPS coordinates to be displayed in syslogs.

### Procedure

**Step 1** Enter the global configuration mode.

**Example:**

```
Router#configure terminal
```

**Step 2** Enter the cellular configuration mode.

**Example:**

```
Router (config)#controller cellular 0/2/0
```

**Step 3** Enable the RF parameters and GPS coordinates.

**Example:**

```
Router (config-controller)#lte modem serviceability signal-parameters
Router (config-controller)#end
```

# Disable cellular telemetry

To disable the cellular telemetry feature, use the no form of the **lte modem serviceability signal-parameters** command, as shown in the example:

```
Router#Configure terminal
Router(config)#controller cellular 0/2/0
```

```
Router(config-controller)#no lte modem serviceability signal-parameters
Router(config-controller)#end
```

# Monitor cellular telemetry

You can monitor RF parameters and GPS coordinates for cellular interfaces by using the **show logging** command or check the console output.

The following example displays RF parameters and GPS coordinates at every one minute interval:

```
Router#show logging
*Sep  3 17:08:42.081: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/2/0: 4G: RSSI = -54 dBm RSRP
 = -76 dBm RSRQ = -9 dB PCI = 1 SNR = 27.4 dB
Latitude =  12 Deg 56 Min 8.9260 Sec North
Longitude =  77 Deg 41 Min 44.1641 Sec East

*Sep  3 17:09:42.080: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/2/0: 4G: RSSI = -54 dBm RSRP
 = -76 dBm RSRQ = -9 dB PCI = 1 SNR = 29.0 dB
Latitude =  12 Deg 56 Min 8.8989 Sec North
Longitude =  77 Deg 41 Min 44.1570 Sec East
```

The following example displays only RF parameters and not GPS coordinates since GPS is not enabled in the controller:

```
Router#show logging
*Sep  3 17:08:42.081: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/2/0: 4G: RSSI = -54 dBm RSRP
 = -76 dBm RSRQ = -9 dB PCI = 1 SNR = 27.4 dB

*Sep  3 17:09:42.080: %CELLWAN-2-MODEM_SIGNAL_PARAM: Cellular0/2/0: 4G: RSSI = -54 dBm RSRP
 = -76 dBm RSRQ = -9 dB PCI = 1 SNR = 29.0 dB
```

# GPS NMEA unique identifier

Starting with Cisco IOS-XE Release 26.1.1, Cisco routers can send a Unique Identifier (UID) to identify the source device when streaming NMEA GPS sentences over UDP on the Cisco IR1101 and Cisco IR1835

routers. UID streaming is supported from the Dead Reckoning (DR) module and from cellular modems that support GNSS. The UID uniquely identifies each router in GPS data processing systems.

***Table 13: Feature History Table***

| Feature name | Release information | Feature description |
|---|---|---|
| Send a UID to identify the unique source when sending GPS coordinates data | Release 26.1.1 | This feature allows you to configure Cisco routers to send a Unique Identifier (UID) while streaming NMEA GPS sentences over UDP.<br>This UID streaming is supported by both the Dead Reckoning (DR) module and cellular modems with GNSS capabilities, enabling each router to be uniquely identified in GPS data processing systems. |

### Cisco proprietary NMEA sentence format

When you configure a UID, a Cisco proprietary NMEA sentence is sent alongside the standard NMEA sentence in the same UDP packet. The format is:

```
$PCSCU,<UID>,<Source>,<Router Time>,<NMEA Sentence Time>,<NMEA Sentence Checksum>,,,,,,*95
```

- `CSC` indicates Cisco
- `U` indicates this sentence provides a unique identifier
- `<UID>` is the serial number, hostname, or custom ID
- `<Source>` indicates the origin of the NMEA stream:
  - `0`: cellular modem0
  - `1`: cellular modem1
  - `2`: DR module

For example, for cellular modem1, if you use the serial number as the UID, the Cisco proprietary NMEA sentence appears as:

```
$PCSCU,FCW2447P0EU,1,213431.100,213431.000,75,,,,,,*95
```

In this NMEA sentence

- `CSC` indicates Cisco
- `U` indicates that this sentence provides a unique identifier
- `FCW2447P0EU` indicates serial number as the UID
- `1` indicates source as cellular modem1
- `1213431.100` indicates the router time
- `213431.000` indicates the NMEA sentence time

- `75` indicates the NMEA sentence checksum

### NMEA sentence selection

By default, all NMEA sentences from the modem or DR module are sent to the configured UDP destination. To reduce UDP traffic, you can select specific NMEA sentence types to send using a hex bitmask. The table presents each NMEA sentence type and its corresponding HEX value.

*Table 14: NMEA sentence type and HEX value*

| HEX value | NMEA sentence type |
|---|---|
| **0x01** | GGA |
| **0x02** | GSA |
| **0x04** | GSV |
| **0x08** | RMC |
| **0x10** | VTG |
| **0x20** | GNS |

# Configure cellular modem GPS NMEA unique identifier

Follow these steps to configure cellular modem GPS NMEA UID.

### Procedure

**Step 1** Use the **configure terminal** command to enter the configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **controller cellular** *slot* command to enter the controller cellular configuration mode.

**Example:**

```
Router(config)# controller cellular 0/x/0
```

**Step 3** Use the **lte gps nmea uid** {**custom** *unique-identifier* **| hostname | serial-number**} command to enable the GPS NMEA UID.

UID can be any of these:

- **custom**: user-configured string of upto 50 characters.
- **hostname**: host name of the router.
- **serial-number**: serial number of the router.

When using **serial-number** or **hostname**, the UID is automatically extracted and added to the proprietary NMEA sentence. This allows uniform CLI configuration across routers.

When using a **custom ID**, each router must be configured with a *unique-identifier* value to ensure distinct identification.

**Example:**

```
Router(config-controller)# lte gps nmea uid custom 1428
```

**Example:**

```
Router(config-controller)# lte gps nmea uid hostname
```

**Example:**

```
Router(config-controller)# lte gps nmea uid serial-number
```

**Step 4** Use the **lte gps nmea ip udp** *source-address destination-address destination-port* **stream** *stream-id* command to specify the source and destination IP address.

**Example:**

```
Router(config-controller)# lte gps nmea ip udp 10.195.79.179 171.70.55.77 14013 stream 1
```

**Step 5** Use the **lte gps nmea filter** *hex-value* command to select the sentence types.

*hex-value*: HEX bitmask for NMEA message filtering (0x01:GGA, 0x02:GSA, 0x04:GSV, 0x08:RMC, 0x010:VTG, 0x20:GNS)

This example shows the HEX value if you want to send sentence type as only RMC (0x08) and GNS (0x20):

**Example:**

```
Router(config-controller)# lte gps nmea filter 28
```

This example shows the HEX value if you want to send sentence type as only GGA (0x01) and GSA (0x02):

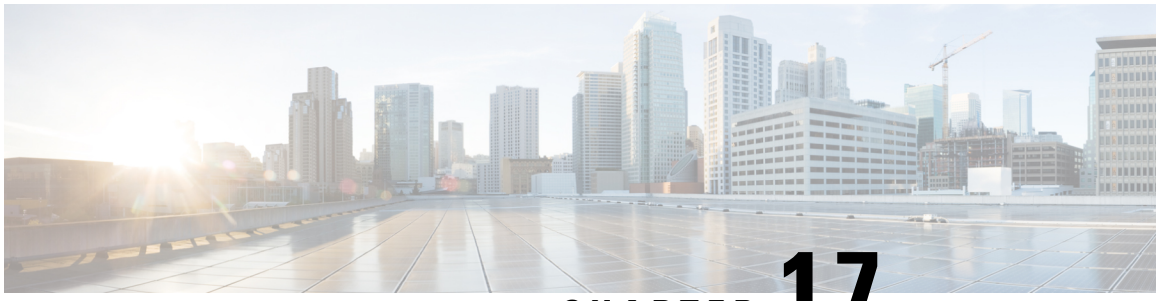
**Example:**

```
Router(config-controller)# lte gps nmea filter 03
```

**Step 6** Use the **end** command to exit the controller configuration mode and return to the privileged EXEC mode.

**Example:**

```
Router(config-controller)# end
```



CHAPTER 17

# Configuring Cisco Resilient Mesh and the WPAN Module

This document provides the necessary configuration details to establish and maintain a functional Cisco Resilient Mesh network using the WPAN module.


- Cisco Resilient Mesh and WPAN modules, on page 111
- Configure the WPAN interface, on page 112
- Configure group multicast, on page 115
- Configure RPL, on page 116
- Configure the power outage server, on page 117
- Configuring Cisco Resilient Mesh Security, on page 117
- IPv6 multicast agents, on page 121
- Configure DTLS relay for EST, on page 123
- TLS Support Matrix, on page 124
- Mesh stack modes, on page 124
- Modulation and data rate, on page 127
- Limited Function Nodes, on page 130
- Direct parenting of LFN support in Wi-SUN mesh deployment, on page 133
- Verify WPAN, on page 133
- IR8100 basic WPAN configurations, on page 134
- Example of IR8100 configuration settings for CR-Mesh, on page 135
- ASR configuration example for CR-Mesh, on page 139
- Check and upgrade the WPAN firmware version, on page 144


## Cisco Resilient Mesh and WPAN modules

A Cisco Resilient Mesh and WPAN Module is a solution for wireless personal area networking and mesh connectivity that:

- supports IEEE 802.15.4e/g standards for WPAN connectivity
- operates on Cisco IR8100 Series Routers running Cisco IOS-XE software, and
- requires configuration and management exclusively through IoT FND with no CLI or graphical user interface for direct configuration.

### Configuration and management reference

Cisco IoT FND provides the user interface for configuring and managing Cisco Resilient Mesh. Typically, Cisco IoT FND handles all configuration and management tasks by communicating with the IR8140H Series WPAN module using Cisco IOS software commands and CoAP Simple Management Protocol (CSMP) TLVs.

**Note** TIP: Cisco Resilient Mesh has no native CLI and no graphical user interface for configuration or management. Cisco IoT FND and CSMP TLVs are used for configuration and management.

For a description of Cisco Resilient Mesh operation, see Information About Cisco Resilient Mesh and WPAN.

The module serial PID is displayed in IOS-XE as IRMH-WPAN-NA:

```
Router#sh inv

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco Catalyst IR8140H Heavy Duty Series Router with PoE"
PID: IR8140H-P-K9      , VID: V00  , SN: FDO2441J91D

NAME: "Power Supply Module 0", DESCR: "60W AC Power Supply module"
PID: IRMH-PWR60W-AC    , VID: V01  , SN: LIT22503LDK

NAME: "module 0", DESCR: "Cisco Catalyst IR8140H-P-K9 Fixed and pluggable Interface Module
 controller"
PID: IR8140H-P-K9      , VID:      , SN:

NAME: "NIM subslot 0/1", DESCR: "IRMH-WPAN-NA Module"
PID: IRMH-WPAN-NA      , VID: V00  , SN: FDO24350D18
```

# Configure the WPAN interface

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **interface wpan** *slot//port* command to specify the slot and port of the WPAN module.

**Example:**

```
Router(config)# interface wpan 0/1/0
```

**Note** The WPAN slot is 1 and the port is 0/1.

# Enable dot1x, mesh-security and DHCPv6

You must enable the dot1x (802.1X), mesh-security, and DHCPv6 features to configure the WPAN interface. Follow these steps to enable dot1x, mesh-security and DHCPv6:

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **dot1x system-auth-control** command to enable 802.1X authentication globally on the router.

**Example:**

```
Router(config)# dot1x system-auth-control
```

**Step 3** Use the **interface wpan** *0/1/0* command to enter interface configuration mode and specify the WPAN interface.

**Example:**

```
Router(config)# interface WPAN 0/1/0
```

**Step 4** Use the **dot1x pae authenticator** command to enable the WPAN interface to respond to messages meant for an IEEE 802.1x authenticator.

**Example:**

```
Router(config-if)# dot1x pae authenticator
```

**Step 5** Use the **authentication host-mode multi-auth** command to set the authentication host mode.

**Example:**

```
Router(config-if)# authentication host-mode multi-auth
```

**Step 6** Use the **authentication port-control auto** command to set the authentication port control.

**Example:**

```
Router(config-if)# authentication port-control auto
```

**Step 7** Use the **ipv6 enable** command to enable IPv6 on the interface.

**Example:**

```
Router(config-if)# ipv6 enable
```

**Step 8** Use the **ipv6 dhcp relay destination** *ipv6-address* command to specify a destination address to which client messages are forwarded and to enable DHCP for IPv6 relay service on the interface.

**Example:**

```
Router(config-if)# ipv6 dhcp relay destination 2001:db8::1
```

# Configure IEEE154 settings

Follow these steps to configure WPAN radio-related settings:

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **interface wpan** *0/1/0* command to enter interface configuration mode and specify the WPAN interface.

**Example:**

```
Router(config)# interface WPAN 0/1/0
```

**Step 3** Use the **ieee154 panid** *id* command to configure the IEEE 802.15.4 Personal Area Network Identifier (PAN ID).

**Example:**

```
Router(config-if)# ieee154 panid 121
```

**Step 4** Use the **ieee154 ssid** *word* command to configure the Service Set Identifier (SSID).

**Example:**

```
Router(config-if)# ieee154 ssid myWPANssid
```

**Step 5** Use the **ieee154 notch** *x-y* command to configure the channel notch list.

**Example:**

```
Router(config-if)# ieee154 notch 10-15
```



**Note** A notch is a list of disabled channels from the 902-to-928 MHz range. Ensure your configuration complies with regional regulations.

**Step 6** Use the **show wpan 0/1/0 hardware channel-list** command in privileged EXEC mode to verify the notch configuration.

**Example:**

```
Router# show wpan 0/1/0 hardware channel-list
```

**Step 7** Use the **ieee154 phy-mode** *mode-list* command to specify the IEEE 802.15.4 PHY mode.

**Example:**

```
Router(config-if)# ieee154 phy-mode 166 165 164 163
```



**Note** The PHY mode setting selects adaptive modulation. Supported modes range from 1 to 255. Refer to the product documentation for specific modulation indices and rates supported by your hardware.

**Step 8** Use the **show wpan 0/1/0 hardware config** command in privileged EXEC mode to verify the PHY mode configuration.

**Example:**

```
Router# show wpan 0/1/0 hardware config
```

# Configure group multicast

Group multicast allows the router to forward multicast traffic to a specific group of devices, which can span multiple PANs.

**Note** This feature is not supported in Cisco Resilient Mesh Release 6.3.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ipv6 multicast-routing** command to enable IPv6 multicast routing.

**Example:**

```
Router(config)# ipv6 multicast-routing
```

**Step 3** Use the **fan-mpl domain** *domain-number* command to enable MPL.

**Example:**

```
Router(config)# fan-mpl domain 0
            Router(config-mpl)# data-imin 10000
            Router(config-mpl)# data-imax 80000
            Router(config-mpl)# data-e 1
```

**Step 4** Verify the multicast address reported by the node using the **show wpan** *interface-id* **rpl mcast-info** {**domains** | **groups**} commands.

**Example:**

```
Router# show wpan 0/1/0 rpl mcast-info domains
            Router# show wpan 0/1/0 rpl mcast-info groups
```

**Step 5** Use the **interface wpan** *interface-id* command to enter interface configuration mode, then use the **mcast-agent interface** *uplink-interface* command to add the multicast agent interface.

**Example:**

```
Router(config)# interface WPAN 0/1/0
            Router(config-if)# mcast-agent interface gi0/0/0
```

**Step 6** Use the **mcast-agent port** command to add the multicast agent port.

**Example:**

```
Router(config-if)# mcast-agent port
```

**Step 7** Use the **mcast-agent group-join** *multicast-group-address* command to add the multicast agent group.

**Example:**

```
Router(config-if)# mcast-agent group-join X:X:X:X::X
```

**Step 8** Use the **show wpan** *interface-id* **mcast-agent** {**group-join** | **interface** | **ports**} command to verify the multicast agent configuration.

**Example:**

```
Router# show wpan 0/1/0 mcast-agent group-join X:X:X:X::X
```

# Configure RPL

Resilient Mesh Endpoints perform routing at the network layer using RPL. For detailed information, refer to RFC 6550.

**Procedure**

**Step 1** Use the **interface wpan** *0/1/0* command to enter interface configuration mode.

**Example:**

```
Router(config)# interface WPAN 0/1/0
```

**Step 2** Use the **rpl** *parameter* command to configure specific RPL settings.

Available parameters include `dag-lifetime`, `dag-lifetime-unit`, `dio-dbl`, `dio-min`, `pon`, `route-poisoning`, `storing-mode`, and `version-incr-time`.

**Step 3** Use the **rpl pon instance** command to enable the Power Outage Notification (PON) instance.

**Example:**

```
Router(config-if)# rpl pon instance
```

**Note** This option is supported only in WiSUN mode. If enabled, the node uses the new PON instance for outage reports.

**Step 4** Use the **redistribute rpl** command within a routing protocol configuration to redistribute RPL routes.

**Example:**

```
Router(config)# ipv6 router ospf 100
            Router(config-rtr)# redistribute rpl metric 3
```

# Configure the power outage server

In the event of a power outage, Mesh Endpoints (MEs) perform the necessary functions to conserve energy and notify neighboring nodes of the outage. Routers relay the power outage notification to a power notification server, which then issues push notifications to customers to relate information on the outage. In most cases, the outage server is your IoT FND server.

**Procedure**

**Step 1** Use the **interface wpan** *0/1/0* command to enter interface configuration mode.

**Example:**

```
Router(config)# interface WPAN 0/1/0
```

**Step 2** Use the **outage server** *ipv6-address-or-fqdn* command to specify the IPv6 address or the fully qualified domain name (FQDN) of the power outage server.

**Example:**

```
Router(config-if)# outage server 2001:c1::8a43:e1ff:fec3:2aa
Router(config-if)# outage server fnd.cisco.com
```

# Configuring Cisco Resilient Mesh Security

Cisco Resilient Mesh security utilizes the IEEE 802.1X protocol, also known as Extensible Authentication Protocol over LAN (EAPOL), to manage authentication processes within the mesh network.



**Note** Cisco Resilient Mesh does not support TLS 1.1. If the RADIUS server does not support TLS 1.2, you must disable TLS 1.1 on the RADIUS server for compatibility.

## Configure mesh key

**Procedure**

**Step 1** Use the **mesh-security set mesh-key interface wpan** *slot/port* **key** *hex-string* command to set the mesh key.

**Example:**

```
Router# mesh-security set mesh-key interface wpan 0/1/0 key 1234567891234567
```

The hex-string must be an even number of hex digits, up to 32.

**Step 2** Use the **mesh-security set mesh-lfn-key interface wpan** *slot/port* **key** *hex-string* command to configure the mesh LFN key.

**Example:**

```
Router# mesh-security set mesh-lfn-key interface wpan 0/1/0 key 12312311
```

**Step 3** Use the **interface wpan** *slot/port* and **mesh-security mesh-key lifetime** *value* commands to configure the mesh key lifetime.

**Example:**

```
Router(config)# int wpan 0/1/0
            Router(config-if)# mesh-security mesh-key lifetime 60
```

**Note**
- The mesh-key lifetime value should be less than 120 days (10,368,000 seconds).
- This command should only be used by an expert mesh-security administrator.
- Mesh-Security configuration and keys do not appear in `show running-config` or `show startup-config` command output.

**Step 4** Use these commands to configure LFN mesh-key lifetime parameters:

**Example:**

```
Router(config-if)# mesh-security mesh-lfn-key revocation-lifetime-reduction 30
            Router(config-if)# mesh-security mesh-lfn-key rollover-ratio 180
            Router(config-if)# mesh-security mesh-lfn-key lifetime 7776000 ptk-lifetime
31104000 pmk-lifetime 46656000
```

# Cisco Resilient Mesh Security configuration example

The example shows what is required for mesh-security.

**Note** The MTU setting on the AAA server must be set to 800 bytes or lower, because IEEE802.1x implementation in RMEs limits the MTU to 800 bytes. RADIUS servers can use auth-port 1812 and acct-port 1813 instead of 1645 and 1646, respectively.

```
!
aaa new-model
!
!
aaa group server radius nps-group
 server name nps-radius
!
aaa authentication enable default none
aaa authentication dot1x default group nps-group
<...snip...>
dot1x system-auth-control
!
<...snip...>
```

```
!
!
interface Wpan0/1/0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 120 max-interval 900 suppression-coefficient 1
 ieee154 panid 7224
 ieee154 ssid migration_far2
 ieee154 txpower -30
 authentication host-mode multi-auth
 authentication port-control auto
 ipv6 address 2092:1:1:1::/64
 ipv6 enable
 ipv6 dhcp relay destination  2010:A0B0:1001:22::2
 dot1x pae authenticator
mesh-security mesh-key lifetime 259200
end
!
!
radius server nps-radius
 address ipv4 <IP address> auth-port 1645 acct-port 1646
 key <RADIUS key>
!
```

# Verifying Cisco Resilient Mesh Security configuration

**Procedure**

**Step 1** Use the **enable** command to enable the router and enter the privileged EXEC mode.

**Example:**

```
Router> enable
```

**Step 2** Use the **show dot1x all details** command to verify the 802.1X security configuration.

**Note** The output for this command shows only new or re-authentications. It does not show nodes that are in the process of warm-starting (and have cached the security credentials).

It displays the configuration and clients of the Cisco Resilient Mesh 802.1X security configuration.

**Example:**

```
Router# show dot1x all details
Sysauthcontrol                  Enabled
Dot1x Protocol Version                3
Dot1x Info for WPAN0/1/0
-----------------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
```

```
TxPeriod                  = 30
Dot1x Authenticator Client List Empty
```

**Step 3** Use the **show mesh-security keys lfn** command to verify the LFN mesh security keys.

**Example:**

```
Router# show mesh-security keys lfn
Mesh Interface: WPAN0/1/0
LFN Pairwise Master Key Lifetime : 540 Days 0 Hours 0 Minutes 0 Seconds
LFN Pairwise Temporal Key Lifetime: 360 Days 0 Hours 0 Minutes 0 Seconds
LFN Mesh Key Lifetime : 90 Days 0 Hours 0 Minutes 0 Seconds
Rollover ratio: 180
Revocation reduction: 30
LFN Key ID : 0 *
Key expiry : Wed Jun 7 11:35:37 2023
Time remaining : 81 Days 21 Hours 23 Minutes 21 Seconds
LFN Key ID : 1
Key expiry : Tue Sep 5 11:35:37 2023
Time remaining : 171 Days 21 Hours 23 Minutes 21 Seconds
```

**Step 4** Use the **show mesh-security keys** command to verify the mesh-security set-key configuration.

**Example:**

```
Router# show mesh-security keys
Mesh Interface: WPAN0/1/0
Pairwise Master Key Lifetime  : 120 Days 0 Hours 0 Minutes 0 Seconds
Pairwise Temporal Key Lifetime: 60 Days 0 Hours 0 Minutes 0 Seconds
Mesh Key Lifetime    : 30 Days 0 Hours 0 Minutes 0 Seconds
Key ID         : 3 *
Key expiry     : Sun Dec  6 20:28:12 2020
Time remaining : 0 Days 1 Hours 5 Minutes 11 Seconds
```

**Step 5** Use the **show mesh-security session all** command to verify the mesh security session details.

**Note** The output for this command shows only new or re-authentications. It does not show nodes that are in the process of warm-starting (and have cached the security credentials).

**Example:**

```
Router# show mesh-security session all
MAC Address               State                    Mesh Keys
00:07:81:08:00:3C:25:03  Encryption Enabled       11..
00:17:3B:0B:00:21:00:2F  Encryption Enabled       .1..
00:07:81:08:00:3C:22:02  Encryption Enabled       11..
00:07:81:08:00:3C:25:02  Encryption Enabled       11..
00:07:81:08:00:3C:22:0A  Encryption Enabled       11..
00:07:81:08:00:3C:22:06  Encryption Enabled       11..
00:07:81:08:00:3C:24:05  Encryption Enabled       ....
00:07:81:08:00:3C:24:08  Encryption Enabled       ....
00:07:81:08:00:3C:23:01  Encryption Enabled       11..
```

**Step 6** Use the **show mesh-security interface wpan <slot>/<port>** command to verify the mesh security interface status.

# IPv6 multicast agents

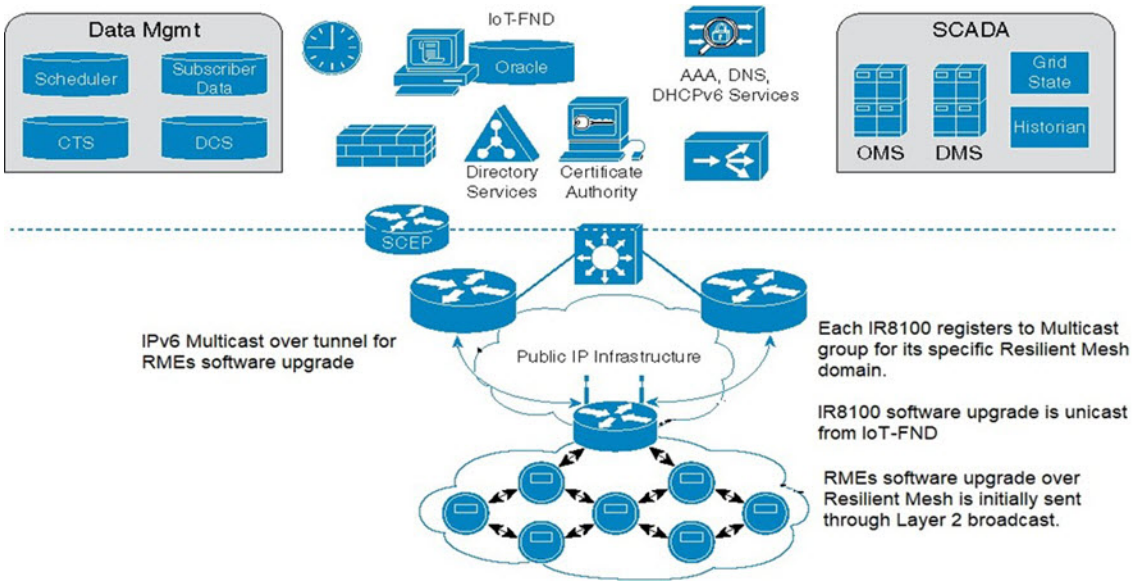
An IPv6 multicast agent is a network configuration component that

- enables multicasting traffic between IoT FND, or the Advanced-Metering Infrastructure (AMI) application server in a Network Operations Center (NOC), and the Cisco Resilient Mesh network
- requires proper configuration on the head-end router (Cisco ASR 1000) as well as on IoT FND and the AMI head-end server, and
- facilitates IPv6 multicast communication for software upgrades, demand reset messages, demand response messages, targeted pings, and meter group operations.

## IPv6 multicast configuration characteristics

The IPv6 FAN with a multicast configuration displays the following architecture:

***Figure 1: IPv6 FAN with multicast configuration***



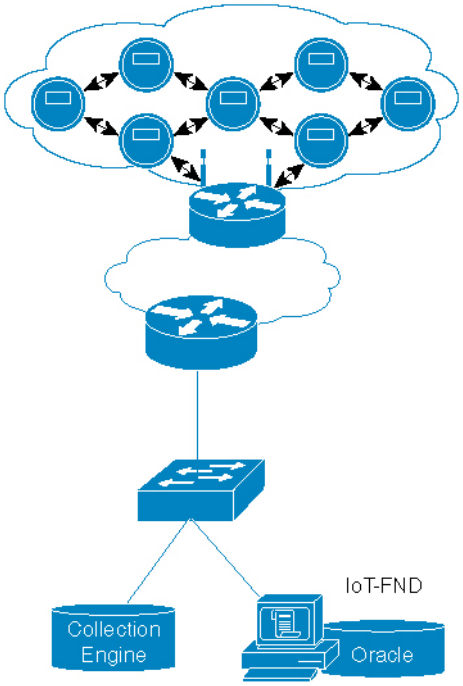

The IPv6 multicast configuration has the following characteristics:

- IPv6 Multicast is used between the IoT FND or CE and the Cisco Resilient Mesh endpoints when performing:
  - Software upgrade of the endpoints
  - Demand reset messages
  - Demand response messages (there could be more than one group for this per meter)
  - Targeted pings (group of meters on a given feeder, for example)
  - Group of meters with the same read time/cycle
- Each PAN is a multicast group with the unicast-prefix-based multicast address (RFC 3306)

- The head-end router routes (PIMv6 SSM) all multicast traffic to the unicast-prefix-based multicast address to the IR8100 (MLDv2)
- IR8100 multicast agent receives the multicast

The multicast operation in an IPv6 FAN operates as follows:

***Figure 2: Multicast operation overview in IPv6 FAN***




There are two ways to forward multicast traffic to an IR8100 running Cisco IOS-XE from the head-end:

- Configure the IR8100 as a multicast client where the tunnel is configured with **ipv6 mld join-group**.

  For this method, configure the IR8100 tunnel interface with MLD as follows:

```
Router (config)# interface Tunnel100
Router (config-if)# ipv6 mld join-group ff38:40:2001:0db8:beef:cafe:0:1
```

- Enable IPv6 multicast routing on the and configure it as a PIM6 router. This is the preferred method and is shown in the next section.

**Note** Note: In above example, the IP address is constructed from the the IPv6 subnet of WPAN.

# Configure IR8100 as PIM6 router

The preferred method of forwarding multicast traffic to the IR8100 is to enable IPv6 multicast routing and configure the device as a PIM6 router. Because the unicast-prefix-based multicast address is required for WPAN, it must be configured under loopback0, and the IR8100 must be configured to become a PIM-neighbor with the ASR head-end.

**Procedure**

**Step 1** Use the **ipv6 multicast-routing** command to enable IPv6 multicast routing.

**Example:**

```
Router(config)# ipv6 multicast-routing
```

**Step 2** Use the **interface loopback 0** and **ipv6 mld join-group** *multicast-address* commands to configure MLD under loopback0.

**Example:**

```
Router(config)# interface loopback 0
Router(config-if)# ipv6 mld join-group ff38:40:2001:0db8:beef:cafe:0:1
```

**Step 3** Use the **ipv6 pim rp-address** *address* command to configure the IPv6 PIM Rendezvous Point (RP).

**Example:**

```
Router(config)# ipv6 pim rp-address 2333::1
```

**Step 4** Configure the ASR/CSR head-end to support the PIM neighbor relationship.

**Example:**

```
ipv6 pim rp-address 2001:DB9::1 bidir
ipv6 pim spt-threshold infinity
!
interface Loopback0
ipv6 address 2001:DB9::1/128
ipv6 pim hello-interval 500
ipv6 pim
!
interface GigabitEthernet0/0/0
ipv6 pim
```

# Configure DTLS relay for EST

Cisco Resilient Mesh uses EST over CoAP/DTLS/UDP for certificate enrollment. During the initial bootstrapping process, nodes that have already joined the network act as DTLS relays for nodes being bootstrapped.

**Procedure**

**Step 1** Use the **interface wpan** *0/1/0* command to enter interface configuration mode for the WPAN interface.

**Example:**

```
Router(config)# interface wpan 0/1/0
```

**Step 2** Use the **dtls-relay** *ipv6-address* [**port** *port-number*] [**max-sessions** *number*] [**lifetime** *seconds*] command to configure the DTLS relay.

**Example:**

```
Router(config-if)# dtls-relay 2060:FACD::6 port 61629 max-sessions 10 lifetime 300
```

**Step 3** Use the **show wpan** *0/1/0* **config** command to verify the DTLS relay configuration.

**Example:**

```
Router# show wpan 0/1/0 config
```

# TLS Support Matrix

Refer to the TLS support matrix to identify the supported TLS versions in Router, WPAN, and Resilient Mesh Endpoints across IOS XE, Classic IOS, and CR-Mesh in Wi-SUN and CG-Mesh deployments.

***Table 15: TLS Support***

| Platform | Software version | Stack mode | TLS versions | Notes |
|---|---|---|---|---|
| IR8140 | Cisco IOS XE | Not applicable | TLS 1.2, TLS 1.3 | Traffic to and from the router; endpoint traffic is passthrough. |
| Cisco 1000 Series Connected Grid Router (CGR) | Cisco IOS | Not applicable | TLS 1.2 | Traffic to and from the router; endpoint traffic is passthrough. |
| WPAN | Not applicable | Wi-SUN | Not applicable | Only transports endpoint traffic. |
| WPAN | Not applicable | CG-Mesh | Not applicable | Only transports endpoint traffic. |
| Resilient Mesh Endpoint (RME) | 6.2.x | Wi-SUN | TLS 1.2 | EAP-TLS authentication. |
| Resilient Mesh Endpoint (RME) | 6.2.x | CG-Mesh | TLS 1.0, TLS 1.2 | EAP-TLS authentication. |
| Resilient Mesh Endpoint (RME) | 5.6.x | CG-Mesh | TLS 1.0 | EAP-TLS authentication. |

# Mesh stack modes

Mesh stack modes let you choose between a Cisco proprietary mesh implementation (CG-Mesh mode) and an implementation based on Wi-SUN open-standards (Wi-SUN mode) for device communication.

- Push the new stack mode and scheduled switch time configurations to all the meters (RME) using Cisco IoT FND, leveraging CSMP TLVs 340 StackModeSettings, 343 StackModeTime, and 344 StackModeResponse.

- Ensure all meters are connected to the Mesh and Cisco IoT FND, so they receive these configurations. Verify that every meter has received the new stack mode and switch time before switching the border router/WPAN to the new stack mode.
- If a meter has not received the stack mode switch time, it will automatically switch to the configured new stack mode after being disconnected from PAN for a maximum offline period of 23 hours.
- Use TLV 345 StackModeStatus to monitor the overall status, timers, and progress of the stack mode switch.

# Configure CG-Mesh stack mode

CG-Mesh mode refers to CR-Mesh operation using Cisco proprietary mesh networking implementation instead of Wi-SUN open-standards based implementation.



**Note**

- Cisco Resilient Mesh Release 6.2 supports both CG-Mesh and Wi-SUN stack modes. CR-Mesh Release 6.3 and above supports only Wi-SUN mode.
- Changing stack mode requires a WPAN module reload.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **interface wpan** *0/1/0* command to specify the WPAN interface and enter interface configuration mode.

**Example:**

```
Router(config)# interface wpan 0/1/0
```

**Step 3** Use the **no wisun-mode** command to enable CG-Mesh mode.

**Example:**

```
Router(config-if)# no wisun-mode
```

**Step 4** Use the **ieee154 beacon-ver-incr-time** *60* command to set the beacon version increase interval.

**Example:**

```
Router(config-if)# ieee154 beacon-ver-incr-time 60
```

**Step 5** Use the **hw-module subslot** *0/1* **reload** command to reload the WPAN interface.

**Example:**

```
Router# hw-module subslot 0/1 reload
```

**Step 6** Use the **ieee154 phy-mode** *2* command to set the PHY mode to a supported value.

**Example:**

```
Router(config-if)# ieee154 phy-mode 2
```

**Step 7** Use the **ieee154 wisun-dwell ucast-dwell-int** *value* **bcast-dwell-int** *value* **bcast-int** *value* command to change the unicast dwell, broadcast dwell, and broadcast interval.

**Example:**

```
Router(config-if)# ieee154 wisun-dwell ucast-dwell-int 125 bcast-dwell-int 125 bcast-int
500
```

**Note** If not configured, all parameters use default values.

You have successfully configured the CR-Mesh mode.

# Configure Wi-SUN stack mode

Wireless Smart Utility Network (Wi-SUN) mode is supported from Cisco Resilient Mesh Release 6.1 and later releases.

**Note**

- Cisco Resilient Mesh Release 6.2 supports both CG-Mesh and Wi-SUN modes. CR-Mesh Release 6.3 and above supports only Wi-SUN mode.
- Changing Wi-SUN mode requires a module reload.
- In Wi-SUN mode, storing mode is not supported.
- In Wi-SUN mode, the mesh key should be reconfigured after changing PANID.

When the IR8100 is in Wi-SUN mode, if there are nodes in the WPAN route table and route poisoning is not enabled, changing the PANID will enable temporary RPL poisoning. It will be disabled automatically. The new PANID will take effect after 3 DIO messages are sent. Validate the connectivity to the IR8100 router.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **interface wpan** *0/1/0* command to specify the WPAN interface and enter interface configuration mode.

**Example:**

```
Router(config)# interface wpan 0/1/0
```

**Step 3** Use the **wisun-mode** command to enable Wi-SUN mode.

**Example:**

```
Router(config-if)# wisun-mode
```

**Step 4** Use the **ieee154 beacon-ver-incr-time** *0* command to set the beacon version increase interval.

**Example:**

```
Router(config-if)# ieee154 beacon-ver-incr-time 0
```

**Step 5** Use the **hw-module subslot** *0/1* **reload** command to reload the WPAN interface.

**Example:**

```
Router# hw-module subslot 0/1 reload
```

**Step 6** Use the **ieee154 phy-mode** *66* command to set the PHY mode to a Wi-SUN supported value.

**Example:**

```
Router(config-if)# ieee154 phy-mode 66
```

**Step 7** (Optional) Use the **ieee154 wisun-dwell ucast-dwell-int** *value* **bcast-dwell-int** *value* **bcast-int** *value* command to change the unicast dwell, broadcast dwell, and broadcast interval.

If not configured, all parameters use default values.

**Example:**

```
Router(config-if)# ieee154 wisun-dwell ucast-dwell-int 125 bcast-dwell-int 125 bcast-int
500
```

# Modulation and data rate

Modulation and data rate (MDR) is a FAN network feature that

- enables devices to adapt data rates or RF modulation based on environmental conditions and neighboring device capabilities
- supports multiple PHY mode configurations in Border Router (BR) and endpoints to handle varying wireless link conditions, and
- advertises configured PHY modes through POM IE (PHY Operating Mode Information Element) as specified in FAN 1.1v5 spec 6.3.4.7.1.

### MDR configuration and operation details

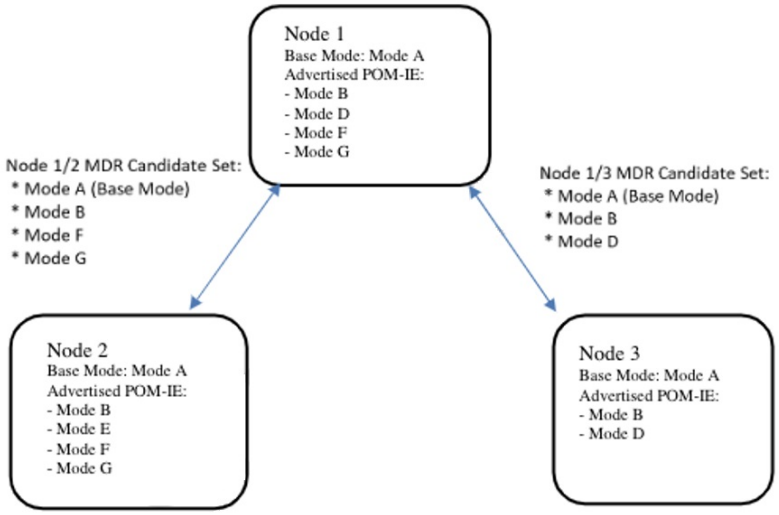
FAN networks typically consist of devices with different physical layer capabilities. The wireless links between different devices in the network may vary greatly due to distance, transmission power, noise, or other interference. Because of these differences, devices should be able to adapt the data rate or RF modulation based on the environment conditions and the neighboring devices communicated with. Multiple PHY mode configuration in Border Router (BR) and End points will help to achieve the above use case. MDR feature is an already supported feature (spec 1.1v2) with PCAP IE as a header for advertising the configured PHY mode. In FAN 1.1v5, this PCAP IE been advertised as POM IE (Phy Operating Mode Information Element). Refer to FAN 1.1v5 spec 6.3.4.7.1 PHY Operating Mode Discovery.

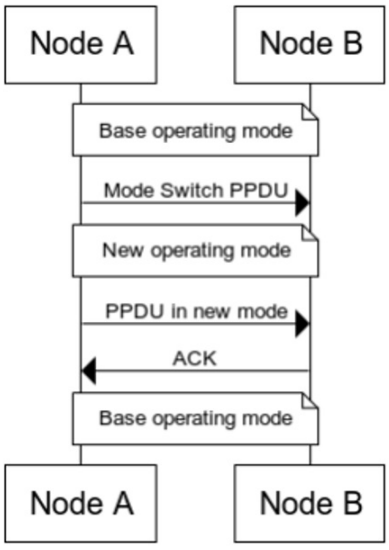
Supported platforms and software releases:

- Border Router: IR8140H, Cisco IOS XE Dulin 17.11.1
- Endpoint: IR510, IR530, WPAN (OFDM and FSK modules), Cisco Resilient Mesh Release 6.6

PHY operating mode selection and switching process:

Based on the set of PHY operating modes advertised by both of a mesh node and a neighbour (indicated by their respective POM-IEs), the intersection of those PHY sets (including the base mode) are candidates for operating mode switching between the two nodes.




Prerequisites for MDR implementation:

All nodes in a PAN must be administratively configured to use the same base PHY operating mode. Neighbor nodes are able to mutually discover each other's PHY operating modes and make application layer decisions to temporarily "switch" to one of the non-base PHY operating modes.

The following combinations alone supported:

- FSK + FSK
- FSK + OFDM option1
- FSK + OFDM option2
- FSK + OFDM option3
- FSK + OFDM option4
- OFDM option1
- OFDM option2
- OFDM option3
- OFDM option4

Combination of different OFDM options are not supported for configuration.

MDR feature limitations:

- Up to 4 phy mode configurations are supported on the Border Router.
- Up to 15 PHY operating modes in a POM IE can be processed, as specified in the Wi-SUN Spec.
- CR-Mesh 6.6 MDR feature cannot work with CR-Mesh 6.5 Release.
- CR-Mesh 6.6 supports Wi-SUN mode only.

Configuration requirements:

When configuring multiple PHY modes, the first mode MUST be the base mode. On the mesh endpoint, it should be the same base mode.

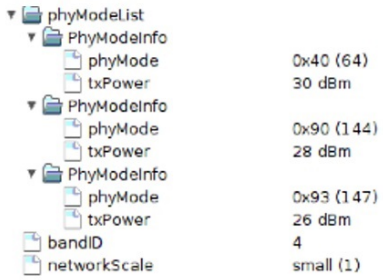
On IR8140H, use the **ieee154 phy-mode** command to configure PHY mode:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#ieee154 phy-mode ?
Supported Phy-Modes:
64:Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz
66:Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
134:Rate=2400 kb/s; Modulation=OFDM; Option=1; MCS=6; Channel Spacing=1200 kHz
144:Rate=50 kb/s; Modulation=OFDM; Option=2; MCS=0; Channel Spacing=800 kHz
147:Rate=400 kb/s; Modulation=OFDM; Option=2; MCS=3; Channel Spacing=800 kHz
149:Rate=800 kb/s; Modulation=OFDM; Option=2; MCS=5; Channel Spacing=800 kHz
150:Rate=1200 kb/s; Modulation=OFDM; Option=2; MCS=6; Channel Spacing=800 kHz
161:Rate=50 kb/s; Modulation=OFDM; Option=3; MCS=1; Channel Spacing=400 kHz
163:Rate=200 kb/s; Modulation=OFDM; Option=3; MCS=3; Channel Spacing=400 kHz
165:Rate=400 kb/s; Modulation=OFDM; Option=3; MCS=5; Channel Spacing=400 kHz
166:Rate=600 kb/s; Modulation=OFDM; Option=3; MCS=6; Channel Spacing=400 kHz
182:Rate=300 kb/s; Modulation=OFDM; Option=4; MCS=6; Channel Spacing=200 kHz

  <1-255>  Enter a value from the list given by: <config-if>ieee154 phy-mode ?

FDO2553J6BF(config-if)#ieee154 phy-mode
FDO2553J6BF(config-if)#ieee154 phy-mode 64 144 147 150
```

PHY mode configured on Endpoint(IR510) – tlv 35 output




### MDR configuration verification

The following command shows the operating on base PHY mode.

```
FDO2553J6BF#show wpan 0/1/0 link-neighbors table
------------------------ WPAN LINK NEIGHBOR TABLE [1] ------------------------------------------
EUI64                   RSSIF   RSSIR   LQIF    LQIR    FIRST_HEARD   LAST_HEARD    MODF       MODR
00173B0500540024        -76     -97     255     95      18:38:04      00:04:57      64         64
6C8BD310003DA362        -43     -67     255     65      18:37:34      00:05:07      64         64
6C8BD310003DA3C4        -44     -67     255     65      18:37:31      00:04:33      64         64
Number of Entries in WPAN LINK NEIGHBOR TABLE: 3
```

The following example shows that the node operating PHY mode is switched from 64 to 147, which is the common highest operating mode between BR and IR510.

```
FDO2553J6BF#show wpan 0/1/0 link-neighbors table
------------------------ WPAN LINK NEIGHBOR TABLE [1] ------------------------------------------
EUI64                   RSSIF   RSSIR   LQIF    LQIR    FIRST_HEARD   LAST_HEARD    MODF       MODR
00173B0500540024        -76     -97     255     95      18:38:04      00:04:57      64         64
6C8BD310003DA362        -45     -69     255     65      18:37:34      00:06:07      147        147
6C8BD310003DA3C4        -44     -67     255     65      18:37:31      00:05:35      64         64
Number of Entries in WPAN LINK NEIGHBOR TABLE: 3
```

# Limited Function Nodes

A Limited Function Node (LFN) is a battery-powered end device that

- operates as RPL leaf nodes in the mesh network, relieved of RPL routing functionality
- provides battery lifetime expected in the range of 15 to 20 years
- cannot be the parent of other nodes in the mesh network, and
- has its own unicast interval, broadcast schedule, and mesh keys in a FAN.

### LFN implementation details

Wi-SUN FAN 1.1v5 details the implementation of LFN node in a FAN Mesh network. CR-Mesh 6.6 release enhances LFN support in IR8140 (CABO) WPAN Border router and IR510. IOS XE 17.11 release implements the authentication of LFN node in a FAN.

Supported platforms:

- IR8140H, Cisco IOS XE Dulin 17.11.1

- WPAN-OFDM module, Cisco Resilient Mesh Release 6.6

LFN configuration commands:

Cisco IOS XE Dulin 17.11.1 support both FAN 1.0 and FAN 1.1 specifications. In order to have LFN in the Border Router, enable LFN for onboarding LFN mesh nodes in your PAN by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#lfn
```

LFN follows different PAN version in the FAN network and it has its own unicast interval and broadcast schedule. From Border Router, you can configure the broadcast interval for LFN by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#ieee154 lfn-bcast interval 300000 sync-period 1
```

Configure LFN mesh key in Border Router:

```
FDO2553J6BF#mesh-security set mesh-lfn-key interface wpaN 0/1/0 key 12312312
```

Configure LFN mesh key lifetime in Border Router under global CLI:

```
FDO2553J6BF#mesh-security mesh-lfn-key lifetime 7776000 ptk-lifetime 31104000 pmk-lifetime
 46656000
```

Configure LFN mesh rollover-ratio and revocation-lifetime-reduction:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#mesh-security mesh-lfn-key revocation-lifetime-reduction 30
FDO2553J6BF(config-if)#mesh-security mesh-lfn-key rollover-ratio 180
```

Configure Mesh-key-exchange timeout:

By default, retry timer of LFN node is 10s during key exchange. Use the following commands to increase the key exchange timeout retry.

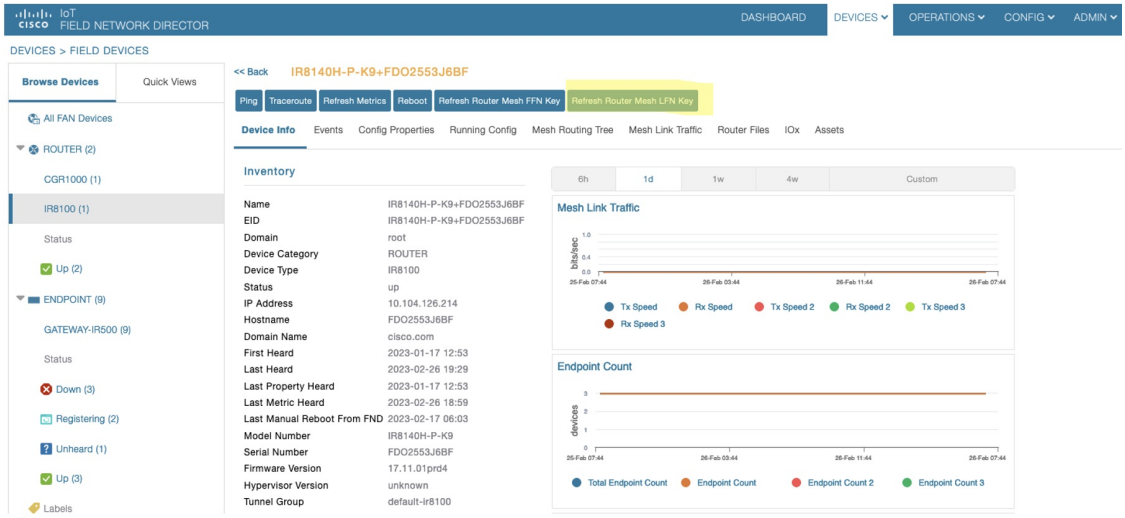
```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#mesh-security key-exchange-message-timeout 30
```

Configure Routing Lifetime for LFN:

LFN nodes are battery powered node. By default, the recommended Registration-lifetime is 24hrs. In Border Router, LFN needs to be maintained in routing table for 24hrs by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#rpl dag-lifetime 60
FDO2553J6BF(config-if)#rpl dag-lifetime-unit 1440
```

Configuring mesh refresh key for LFN from FND:




Verification commands:

To check the LFN version in Border Router:

```
FDO2553J6BF#show wpan 0/1/0 config | i LFN
LFN version: 8929 (2232)
FDO2553J6BF#
```

To check LFN broadcast interval:

```
FDO2553J6BF#show wpan 0/1/0 hardware config | i lfn
lfn_bcast:      interval 300000 sync-period 1
FDO2553J6BF#
```

Border router supports up to 3 keys for LFN. To check LFN Mesh-security Key:

```
FDO2553J6BF#show mesh-security keys lfn
```

```
FDO2553J6BF#show mesh-security keys lfn
Mesh Interface: WPAN0/1/0

LFN Pairwise Master Key Lifetime  : 540 Days 0 Hours 0 Minutes 0 Seconds
LFN Pairwise Temporal Key Lifetime: 360 Days 0 Hours 0 Minutes 0 Seconds
LFN Mesh Key Lifetime    : 90 Days 0 Hours 0 Minutes 0 Seconds

Rollover ratio: 180
Revocation reduction: 30

LFN Key ID     : 0 *
Key expiry     : Wed May 24 13:29:48 2023
Time remaining : 86 Days 12 Hours 36 Minutes 29 Seconds

LFN Key ID     : 1
Key expiry     : Tue Aug 22 13:29:48 2023
Time remaining : 176 Days 12 Hours 36 Minutes 29 Seconds

LFN Key ID     : 2
Key expiry     : Mon Nov 20 13:29:48 2023
Time remaining : 266 Days 12 Hours 36 Minutes 29 Seconds
```

Limitations:

- LFNs are battery powered nodes and work in their own unicast schedule. It is recommended to use long timeout values (180s) when trying to onboard LFN from Border Router.
- IR8140H does not support direct parenting of LFN.

# Direct parenting of LFN support in Wi-SUN mesh deployment

Direct parenting of LFN support in Wi-SUN mesh deployment is a network capability that

- enables IR8140 routers to directly parent Limited Function Nodes (LFNs) in Wi-SUN mesh deployments
- supports battery-powered low-energy endpoints typically used for utility metering of electricity, gas, and water
- allows LFN endpoints to connect to IR8140 as a child but prevents them from parenting other devices in a mesh network.

### Implementation and verification details

From Cisco IOS-XE Release 17.14.1, the IR8140 routers support direct parenting of Limited Function Nodes (LFNs) in Wi-SUN Mesh deployments. Several such LFN endpoints connect to a border router forming a sensor network to implement an Advanced Metering Infrastructure (AMI) deployment.

Previous releases supported IR8140 indirectly parenting LFNs through a partner Full Function Node (FFN) device. For more information, see Limited Function Node.

Use this command given as example to determine if the router has enabled LFN support:

```
IR8140#show wpan 0/2/0 hardware configuration
lfn support: Enabled
```

Use this command given as example to verify the node connected to the router is an LFN or FFN:

```
IR8140#show wpan 0/2/0 link-neighbors ns
------------------------ WPAN LINK NEIGHBOR TABLE WITH NS [2] -------------------------
EUI64            IPV6 address                                Lifetime   Last NS   Node Type
00173B05004D0030 2001:1111:1111:1111:55DC:BEF3:4D9C:FD87   240        15:29:08   LFN
Number of Entries in WPAN LINK NEIGHBOR TABLE: 1
Current time : 15:30:29
```

# Verify WPAN

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **show wpan** *interface-id* command to view all available WPAN show commands.

**Example:**

```
Router# show wpan 0/1/0 ?
```

**Note** You can use these commands to display specific WPAN configuration and status information:

| Command | Description |
|---|---|
| **show wpan config** | Displays the WPAN basic configuration. |
| **show wpan hardware** | Displays WPAN hardware information. Use **show wpan 0/1/0 hardware ?** for options. |
| **show wpan packet-count** | Displays incoming and outgoing packet counts for WPAN traffic. |
| **show wpan link-neighbors** | Displays information about WPAN link neighbors (1-hop range). Note: Minimum RSSI to join is -95 dBm. |
| **show wpan outage-table** | Displays recent power-outage notification (PON) events in the PAN during the past hour. |
| **show wpan restoration-table** | Displays recent power restoration notification (PRN) events in the PAN during the past hour. |
| **show wpan rpl** | Displays WPAN RPL information. |
| **debug wpan all** | Displays all WPAN debugging messages, including errors, fan-mpl, info, packets, and rpl. |

# IR8100 basic WPAN configurations

An IR8100 basic WPAN configuration is a network setup that

- includes Wi-SUN mode operation on the WPAN interface
- configures IEEE 802.15.4 physical layer settings and beacon parameters, and
- enables IPv6 addressing with DHCP server functionality for connected devices.

### WPAN configuration details

The WPAN interface configuration includes several key components:

- **wisun-mode**: Enables Wi-SUN (Wireless Smart Utility Network) operation mode
- **ieee154 phy-mode 66**: Sets the IEEE 802.15.4 physical layer mode
- **ieee154 beacon-async**: Configures asynchronous beacon intervals and suppression
- **ieee154 panid**: Defines the Personal Area Network identifier
- **ieee154 ssid**: Sets the network service set identifier
- **rpl dag-lifetime**: Configures RPL (Routing Protocol for Low-Power and Lossy Networks) parameters

**Note** The **dwell** attribute indicates the maximum transmission time on a channel to comply with government regulations, most of which limit transmissions on a channel to *X* ms within *Y* ms (minimum and maximum duration). The **dwell** command allows you to set both *X* and *Y* . In the U.S., they are typically 400 ms to 20000 ms.

### Basic WPAN interface configuration

The example shows a typical WPAN interface configuration on the IR8100:

```
interface WPAN0/1/0
 wisun-mode
 ieee154 phy-mode 66
 ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
 ieee154 panid 12571
 ieee154 ssid sit-cabo
 ieee154 beacon-ver-incr-time 0
 rpl dag-lifetime 60
 rpl dio-min 14
 rpl version-incr-time 10
 ipv6 address AAAA:BBBB:CCCC:3::1/64
 ipv6 dhcp server MeterNetwork rapid-commit
 authentication host-mode multi-auth
 authentication port-control auto
 dot1x pae authenticator
```

# Example of IR8100 configuration settings for CR-Mesh

The configuration settings for an IR8100 router in a Cisco Resilient Mesh network is given in the example.

```
IR8100#sh run
Building configuration...

Current configuration : 9107 bytes
!
! Last configuration change at 16:53:48 CST Tue Feb 16 2021 by cisc0
!
version 17.5
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec
service call-home
service unsupported-transceiver
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform shell
!
hostname IR8100
!
boot-start-marker
boot system
flash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210207_015223_V17_5_0_161.SSA.bin
boot-end-marker
!
!
logging buffered 1000000
no logging console
enable password cisc0
!
```

```
aaa new-model
!
!
aaa group server radius CGCDN
server name wisun_radius
!
aaa authentication login default local
aaa authentication dot1x default group CGCDN
aaa authorization exec default local
!
aaa common-criteria policy iiot_policy
min-length 10
max-length 127
numeric-count 1
upper-case 1
lower-case 1
char-changes 4
!
!
aaa session-id common
clock timezone CST 8 0
!
!
login on-success log
no ipv6 address-validate
ipv6 unicast-routing
ipv6 dhcp pool dhcp-node
address prefix 2001:CABB::/64 lifetime 60000 36000
vendor-specific 26484
suboption 1 address 2060:FACD::50
suboption 2 address 2060:FACD::50
!
ipv6 multicast-routing
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint TP-self-signed-3764981121
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3764981121
revocation-check none
rsakeypair TP-self-signed-3764981121
!
!
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 TP-self-signed-3764981121
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33373634 39383131 3231301E 170D3230 31313130 30373239
31385A17 0D333031 31313030 37323931 385A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37363439
38313132 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100E821 301D5675 0B3BA0B8 81273D9F B82581E9 9BACAE41 D501A5E9
A8E98EFB 2C25B7C9 A0E0CF17 C39FEBBA E673C855 BDA9379C BDDC68DC 377C2589
21CD8189 6AC98A97 9B5FA5D5 17E51A1F 3DB8BC88 1A844B1E EE69DA60 8D84620A
8A023D87 D93F3ADF 75D99D81 E06BCEF6 AC7C3A2E D70C79F1 C7E8E893 F08BE954
E0184F0D 0E0112BD 497C87E8 5E4788C4 ACF56F92 9134B85B 7D08F6BA 703CF11B
BC8E1377 DC0450E0 A9939952 90F1D84F F235BB5B D54517E9 B636D334 5569278A
3A629DC7 03CC08FF F067EE3F 0EADFAC0 A03C650C A2253E4C 13DD8910 E9726929
9ACD8403 CD16D710 6D5F1FA5 F7F0E310 9060340C 3309446B 99DC10E2 25908D03
D3FBA3E3 54D70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 14C73ACD 622756FB EB532701 66D605BC 49F9FFF2
BE301D06 03551D0E 04160414 C73ACD62 2756FBEB 53270166 D605BC49 F9FFF2BE
300D0609 2A864886 F70D0101 05050003 82010100 DC4AC08A D11E0E05 239FEBCB
694CC50F E0712807 A52F5714 C1501C4A A8283929 23F00BD1 B6F5310E 917C7501
B585E8AE 4CC88BE4 ED5555BF F46F2917 621577D6 6E14E796 B9A24FC7 3191F259
D61C6718 05E2FCB6 443E5D34 CBB90C02 3066F77C 3E3361E0 F975FB8E C026F652
DF2F3B2F FBBF0ABF 6600FD3D 9DB94163 330239C0 3F948CB1 30CEA1EE 3730FDA1
83A37AD9 940D8240 3B5A6D11 2601E91B 401CAB81 7FCC7C6E F3C48F19 B225FBCE
02523D36 8EAA3D42 3C232231 138F8EB0 BD3FF413 5FB879BE 5511A0D2 5953DB50
06E5CC26 082013B8 39D83819 EAA03533 B242A46C 679BE60F 0D9ED9BD 20D03F09
71159FAC 4DFD2DA8 71C5A1DD 94397BA5 6D2CEB0B
quit
!
!
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2438J7BK
memory free low-watermark processor 47507
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
dot1x system-auth-control
!
username cisc0 password 0 cisc0
!
redundancy
mode none
!
!
interface Loopback1
```

```
no ip address
ipv6 address 4008::8/128
!
interface GigabitEthernet0/0/0
ip address 10.79.56.221 255.255.255.0
negotiation auto
ipv6 address 2060:FACD::221/64
ipv6 enable
!
interface GigabitEthernet0/0/1
ip address 192.168.254.101 255.255.255.0
load-interval 30
negotiation auto
ipv6 address 2111:ABCD::111/64
ipv6 enable
ipv6 nd ra suppress
ipv6 ospf 1 area 0
!
interface WPAN0/1/0
no ip address
wisun-mode
ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
ieee154 dwell window 12400 max-dwell 400
ieee154 notch 10-20
ieee154 panid 15294
ieee154 ssid regression
ieee154 beacon-ver-incr-time 0
rpl dag-lifetime 60
rpl dio-dbl 1
rpl dio-min 14
rpl version-incr-time 10
ipv6 address 2001:CABB::1/64
ipv6 enable
ipv6 mld join-group FF38:40:2001:CABB::1
ipv6 dhcp server dhcp-node rapid-commit
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
!
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip tftp blocksize 8192
ip route 10.0.0.0 255.0.0.0 10.79.56.254
ip route 10.79.0.0 255.255.0.0 10.79.56.254
!
!
ipv6 route 2001:DB8:6:D6FF::/64 2111:ABCD::200
ipv6 route 2001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 2015:ABCD::/64 2111:ABCD::200
ipv6 route 3001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 3002:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 3002:ABCD::/64 2111:ABCD::200
ipv6 route 9001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 9002:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 router ospf 1
redistribute rpl
!

tftp-server bootflash:cg-mesh-bridge-6.4weekly-6404-ir510-8546385.bin
!
!
```

```
radius server wisun_radius
address ipv4 10.79.42.79 auth-port 1812 acct-port 1813
key Wi-SUN_radius
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
transport preferred none
stopbits 1
speed 115200
line vty 0 4
exec-timeout 0 0
password cisc0
transport input telnet
line vty 5 15
exec-timeout 0 0
password cisc0
transport input telnet
!
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
ntp server 171.68.38.66
ntp server 10.64.58.51
!
end
```

# ASR configuration example for CR-Mesh

The following example shows the configuration for an ASR in a Cisco Resilient Mesh network.

```
SOL-ASR-7# show run brief
Building configuration...
Current configuration : 5512 bytes
!
! Last configuration change at 10:38:26 PST Fri May 16 2014 by admin
! NVRAM config last updated at 13:44:36 PST Thu May 15 2014 by admin
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime localtime
no platform punt-keepalive disable-kernel-core
!
hostname SOL-ASR-7
!
boot-start-marker
boot system flash:asr1000rp1-adventerprisek9.03.11.00.S.154-1.S-std.bin
boot-end-marker
!
aqm-register-fnf
!
vrf definition Mgmt-intf
 !
 address-family ipv4
```

```
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no logging console
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
!
!
!
!
!
!
!
no ip domain lookup
ip domain name ipv6lab.com
!
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
crypto pki trustpoint LDevID
 enrollment retry count 10
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number
 ip-address none
 password
 fingerprint F23314787BD98B99AF1FE0B2D338961D125EAE51
 revocation-check none
 rsakeypair LDevID
!
```

```
crypto pki profile enrollment LDevID
 enrollment url  http://192.168.100.120/certsrv/mscep/mscep.dll
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = ipv6lab-sol-radius1-ca
!
crypto pki certificate chain LDevID
 certificate 4B88014800010000000FC
 certificate ca 2539E6B5CFF2FB894AC90A73EA69A645
spanning-tree extend system-id
!
username admin privilege 15 password 0 cisco
!
redundancy
 mode none
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
crypto ikev2 redirect gateway init
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-128
 integrity sha1
 group 5
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 1
!
!
crypto ikev2 cluster
 port 2000
 standby-group group1
 slave priority 90
 slave max-session 10
 no shutdown
!
!
cdp run
!
ip tftp source-interface GigabitEthernet0/0/3
ip ssh version 2
!
!
!
!
!
!
!
!
crypto ipsec transform-set AES_128_SHA1 esp-aes esp-sha-hmac
```

```
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set AES_128_SHA1
 set ikev2-profile FlexVPN_IKEv2_Profile
 responder-only
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 20.0.0.3 255.255.0.0
 ipv6 address 2003:20::1/128
 ipv6 address 2333::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0/0
 ip address 173.36.248.224 255.255.255.192
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 ip address 10.0.2.70 255.255.255.0
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2001:A02::A00:246/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
 cdp enable
!
interface GigabitEthernet0/0/2
 ip address 11.0.0.70 255.255.255.0
 standby 1 ip 11.0.0.100
 standby 1 priority 110
 standby 1 name group1
 negotiation auto
 ipv6 enable
 cdp enable
!
interface GigabitEthernet0/0/3
 ip address 11.0.1.70 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/1/0
 description WIMAX-BASESTATION
 ip address 192.10.0.88 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/1/1
 no ip address
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2010:DEAD:BEEF:CAFE::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
!
```

```
interface GigabitEthernet0/1/2
 no ip address
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2011:DEAD:BEEF:CAFE::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
!
interface GigabitEthernet0/1/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface Virtual-Template1 type tunnel
 description ip pim sparse-mode
 ip unnumbered Loopback0
 ipv6 address autoconfig
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
router ospf 1
 redistribute static subnets
 network 10.0.2.0 0.0.0.255 area 1
 network 11.0.0.0 0.0.0.255 area 1
 network 11.0.1.0 0.0.0.255 area 1
 network 173.36.0.0 0.0.255.255 area 1
 network 192.10.0.0 0.0.0.255 area 1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 10.0.0.0 255.255.255.0 173.36.248.193
!
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit any
!
ipv6 route 2005:DEAD:BEEF:CAFE::/64 2001:420:7BF:7E8::1
ipv6 route 2006:DEAD:BEEF:CAFE::/64 2001:420:7BF:7E8::B
ipv6 local pool IPV6_POOL 2001:10::/64 64
ipv6 pim rp-address 2333::1
ipv6 router ospf 1
 redistribute static
!
!
!
!
!
!
```

```
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 permit ipv6 any any
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 transport input all
 transport output all
!
ntp server 192.168.100.250
netconf max-sessions 16
netconf ssh
!
end
SOL-ASR-7#
```

# Check and upgrade the WPAN firmware version

For the IR8100, only the IRMH WPAN is supported, and the minimum required version is 6.2.19.



**Note** WPAN firmware is not integrated into the IR8100 system firmware and must be upgraded separately.

### Procedure

**Step 1** Use the **show wpan** *0/1/0* **hardware hwversion** command to check the version of the WPAN hardware in slot 1.

**Example:**

```
Router# show wpan 0/1/0 hardware hwversion
hardware version: CGM-WPAN, 1.0, IRMH-WPAN/1.0/2.0
```

**Step 2** Use the **show wpan** *0/1/0* **hardware version** command to check the installed CR-Mesh firmware version of the WPAN.

**Example:**

```
Router# show wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```

You can also display the WPAN firmware version using the **show wpan** *0/1/0* **config** command:

```
Router# show wpan 0/1/0 config
module type:    RF-WPAN (IEEE 802.15.4e/g RF 900MHz)
.
.
.
firmware version:      6.2RC(6.2.20)
```

# Upgrade WPAN firmware

**Before you begin**

The appropriate WPAN firmware image must be copied and available on the IR8100 flash in the root directory.

Follow these steps to upgrade the WPAN firmware:

**Procedure**

**Step 1** Use the **install-firmware** *image* command to install the firmware.

**Example:**

```
Router(config-if)# install-firmware image
Firmware upgrade starting. This may take several minutes. Please do not interrupt.
.....................
Installed the WPAN 6.0 firmware successfully (94 sec).
Please reload the WPAN module in slot 1!!
```

**Step 2** Use the **hw-module subslot** *0/1* **shutdown unpowered** command to power down the WPAN module.

**Example:**

```
Router# configure terminal
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

**Step 3** Wait for power-down messages, wait 60–90 seconds, and then use the **no hw-module subslot** *0/1* **shutdown unpowered** command to power up the module.

**Example:**

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

**Step 4** Wait for power-up messages and wait at least 500 seconds before proceeding. Verify the status and hardware version using the **show ip interface brief** and **show wpan** *0/1/0* **hardware version** commands.

**Example:**

```
Router# show ip interface brief | inc Wpan
Wpan0/10                   unassigned      YES unset  up                    up
Router# show wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```

# Upgrade WPAN firmware (CG-Mesh to WiSUN)

**Before you begin**

The appropriate WPAN firmware image must be copied and available in the root directory of the IR8100 flash.

**Procedure**

**Step 1** Use the **install-firmware** *image* command to install the firmware.

**Example:**

```
Router(config-if)# install-firmware image
Firmware upgrade starting. This may take several minutes. Please do not interrupt.
.....................
Installed the WPAN 6.0 firmware successfully (94 sec).
Please reload the WPAN module in slot 1!!
```

**Step 2** Use the **hw-module subslot** *0/1* **shutdown unpowered** command to power down the WPAN module.

**Example:**

```
Router# configure terminal
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

**Step 3** Wait for power-down messages, wait 60–90 seconds, and then use the **no hw-module subslot** *0/1* **shutdown unpowered** command to power up the module.

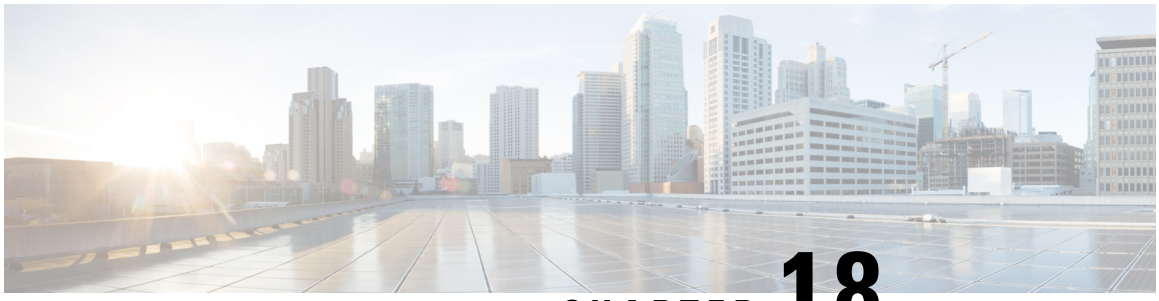
**Example:**

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

**Step 4** Wait for power-up messages and wait at least 500 seconds before proceeding. Verify the status and hardware version using the **show ip interface brief** and **show wpan** *0/1/0* **hardware version** commands.

**Example:**

```
Router# show ip interface brief | inc Wpan
Wpan0/10                   unassigned      YES unset  up                    up
Router# show wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```



CHAPTER 18

# DHCP Option 82

*Table 16: Feature History Table*

| Feature name | Release information | Feature description |
|---|---|---|
| DHCP Option 82 | Release 26.2.1 | Starting with Cisco IOS XE Release 26.2.1, DHCP servers on routers support DHCP Option 82 relay information. The DHCP server can use the Circuit ID and Remote ID inserted by a DHCP relay agent to select an address pool for a client. This support enables predictable, location-based IP address assignment without requiring administrators to track client MAC addresses. |


- DHCP Option 82, on page 147
- Prerequisites, on page 148
- Key considerations, on page 149
- Limitations, on page 149
- DHCP Option 82 packet flow, on page 149
- Hexadecimal pattern and suboption decoding, on page 150
- Configure DHCP Option 82 on server, on page 151
- Configure DHCP address pool, on page 153
- Configure DHCP relay agent, on page 154
- Configure relay chaining on relay agents, on page 156
- Verify DHCP Option 82, on page 157
- Debug DHCP Option 82 logs, on page 157


# DHCP Option 82

The Dynamic Host Configuration Protocol (DHCP) Option 82 feature allows the server to allocate dynamic IP addresses based on the relay information sent by the relay agent. It enables predictive IP address assignment by the server based on network switch ports.

DHCP Option 82 enables DHCP relay agents to insert additional information such as Circuit ID, Remote ID and other configuration information into DHCP request messages before forwarding them from the client to the server.

Starting with Cisco IOS XE Release 26.2.1, DHCP servers support DHCP Option 82 on routers. This platform-independent feature includes the following suboptions:

- Circuit ID suboption: Identifies the relay agent's source interface or port where the client is connected.
- Remote ID suboption: Identifies the relay agent.

The DHCP server allows for address reservation based on Option 82 values, enabling consistent IP assignments per interface or location.

### Benefits of DHCP Option 82

The use of DHCP Option 82 provides several operational and security advantages for network management such as:

- Predictable IP assignment: Enables static or predictable IP assignment for DHCP clients based on switch ports instead of MAC addresses.
- Enhanced security: Improves IP address management and security.
- Operational efficiency: Eliminates manual intervention or the need to track device MAC addresses.
- Granular control: Allows ISPs and network administrators to map specific user accounts to physical locations, enabling consistent, location-based IP assignments.

# Prerequisites

Before configuring DHCP Option 82, you must ensure these requirements are met:

- A relay agent must be configured with global and VLAN-based DHCP snooping enabled.
- A DHCP server is available.
- A DHCP client is connected.
- A relay chaining topology is present wherever applicable.
- The client must be connected to the relay agent through an SVI interface for enabling VLAN-based snooping.
- Class based support must be enabled on the DHCP server.

**Note** You must know the hexadecimal value of each byte location in DHCP Option 82 to configure the relay-information hexadecimal command.For more information, see Circuit ID and Remote ID decode values

# Key considerations

Key considerations for using DHCP Option 82 are:

- DHCP Option 82 support must be enabled on both the relay agent and DHCP server.
- You need to consider whether to use the DHCP Option 82 feature or not for predictable usage of IP assignment for DHCP clients.
- You need to consider whether to enable DHCP Option 82 globally for all interfaces or selectively on specific VLANs or interfaces only.
- You need to consider which information you want to match in the DHCP message received by the server. This can be Circuit ID, Remote ID or both.

# Limitations

Limitations while using DHCP Option 82 are:

- Support must be enabled on both the relay agent and the DHCP server for it to work properly.
- If the DHCP server ignores DHCP Option 82, port-based deterministic assignment will not occur.
- It is not suitable for environments where MAC based IP address assignment is required.

# DHCP Option 82 packet flow

### Summary

DHCP Option 82 enables network administrators to track the location information of DHCP clients by inserting additional metadata as DHCP packets traverse relay agents. This process ensures accurate IP assignment and aids in network management.

### Workflow

The DHCP packet flow through a network when DHCP Option 82 is enabled is as given:

1. The DHCP client broadcasts a DHCP request on the local network.
2. The first DHCP relay agent intercepts the broadcast and inserts the DHCP Option 82 field, which includes suboptions such as Circuit ID and Remote ID.
3. If a second relay agent resides closer to the DHCP server, the second relay agent encapsulates the DHCP Option 82 field coming from the first relay agent and forwards it to the DHCP server. This process preserves the information from both relay agents.
4. The relay agent sets the gateway IP address (giaddr) field in the DHCP packet to its own IP address. The giaddr field enables the DHCP server to identify the subnet from which the request originated.
5. The relay agent unicasts the DHCP packet to the DHCP server.

6. The DHCP server uses the DHCP Option 82 information to determine the appropriate IP address pool and configuration parameters for the client.
7. The DHCP server sends the reply to the relay agent using the giaddr address.
8. The relay agent removes the DHCP Option 82 information from the reply before forwarding the DHCP reply to the client.

# Hexadecimal pattern and suboption decoding

The DHCP Option 82 hexadecimal pattern can be decoded for Circuit ID and Remote ID separately as shown in the examples.

### Hexadecimal pattern sample

The Option 82 hexadecimal pattern `010600040005010a020701057065747261` consists of two primary suboptions:

- `01 06 00040005010a`: Circuit ID (Suboption 1).
- `02 07 01057065747261`: Remote ID (Suboption 2).

| Field | Meaning |
|---|---|
| 01 | Circuit-ID suboption. |
| 06 | Circuit-ID length. |
| 00040005010a | Circuit-ID value. |
| 02 | Remote-ID suboption. |
| 07 | Remote-ID length. |
| 01057065747261 | Remote-ID value. |

### Circuit ID Decode

The Circuit ID `00040005010a` identifies client's point of attachment specifying the port and VLAN of the connected client. By default, it follows the **vlan-mod-port** format.

```
Router# show cdp neighbors
         Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
         device1         Gig 1/10            175           R S I  ESR-6300- Gig 0/1/0

Router# show vlan brief
         VLAN          Name                                Status    Ports
         5    TURBINE_INTERNAL                 active    Gi1/10
```

**Note** Decoding the Circuit ID `00040005010a`:

- `00`: Default format (vlan-mod-port).
- `04`: Length (4 bytes).
- `0005`: VLAN ID (Hex 0005 = Decimal 5).
- `010a`: Module 1, Port 10 (Hex 0a = Decimal 10).

### Remote ID Decode

The Remote ID `01057065747261` identifies the originating device (MAC address or Hostname). It can be configured to use the device hostname.

```
Router(config)# ip dhcp snooping information option format remote-id hostname
```

**Note** Decoding the Remote ID `01057065747261`:

- `01`: Hostname format.
- `05`: Length (5 bytes).
- `7065747261`: Hexadecimal ASCII for router.

# Configure DHCP Option 82 on server

To configure DHCP Option 82 on Cisco IR router server, you need to follow these tasks:

- Enable DHCP Option 82 for DHCP address allocation on the server.
- Define the DHCP class and relay agent information patterns.
- Define the DHCP address pool on the server.
- Enable relay chaining on DHCP relay agents.
- Verify DHCP Option 82
- Debug DHCP Option 82 logs.

Follow these steps to configure DHCP Option 82 on the server.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ip dhcp class** *class_name* command to enable DHCP address allocation using DHCP class.

**Example:**

```
Router(config)# ip dhcp class class_name
```

**Note**
- You can use Step 2 to enable DHCP Option 82 for DHCP address allocation on the server.
- You can disable this functionality, without deleting the DHCP class configuration.

**Step 3** Use the **relay agent information** command to enter relay agent information option configuration mode and define the DHCP class and relay agent information patterns.

**Example:**

```
Router(dhcp-class)# relay agent information
```

**Note** The `relay agent information` command validates only the presence of Option 82 in the DHCP packet. It does not evaluate the Circuit ID or Remote ID. As a result, any DHCP packet containing Option 82, regardless of its source port or relay agent will match this DHCP class and be assigned an IP address.

**Step 4** (Optional) Use the **relay-information hex** *pattern* [*] [**mask** *mask*] command to optionally specify a hexadecimal value for the full relay information option.

**Example:**

```
Router(dhcp-class-relayinfo)# relay-information hex 010600040005010a020701057065747261
```

**Example:**

```
Router(dhcp-class-relayinfo)# relay-information hex 01030a0b0c02050000000123 mask
00000000000000000ffffffffffffffff
```

**Example:**

```
Router(dhcp-class-relayinfo)# relay-information hex 010600040005010a*
```

**Note**

- The Option 82 hexadecimal pattern includes two sub options: one for Circuit ID and the other for Remote ID.
- Each suboption can be decoded to represent the suboption type, length, VLAN, module port, client interface and MAC address.
- You can match the hexadecimal pattern either fully or partially for specific scenarios of IP assignment.
- You can use the mask option to mask either the Circuit ID or Remote ID partially.
- You can use * as a wildcard pattern at the end of the hexadecimal pattern to match only the beginning of the relay information value.
- If you omit this step, no pattern is configured and it is considered a match to any relay agent information option value, but the relay information option must be present in the DHCP packet.
- Repeat Step 4 for each DHCP class you need to configure.

### What to do next

For more information, see Configuring DHCP Address Allocation Using Option 82.

# Configure DHCP address pool

Follow these steps to configure and define DHCP address pool for DHCP address allocation.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ip dhcp pool** *name* command to configure a DHCP address pool on a DHCP server and enter DHCP pool configuration mode.

**Example:**

```
Router(config)# ip dhcp pool ABC
```

**Step 3** Use the **network** *network-number* [*mask* |*prefix-length*] command to configure the subnet number and mask for a DHCP address pool on the DHCP server.

**Example:**

```
Router(dhcp-pool)# network 10.0.20.0 255.255.0.0
```

**Step 4** Use the **class** *name* command to associate a class with a pool and enters DHCP pool class configuration mode.

**Example:**

```
Router(dhcp-pool)# class CLASS1
```

**Note** This command will also create a DHCP class if the DHCP class is not yet defined.

**Step 5** Use the **address range** *start-ip end-ip* command optionally to set an address range for a DHCP class in a DHCP server address pool.

**Example:**

```
Router(dhcp-pool-class)# address range 10.0.20.1 10.0.20.100
```

**Note**
- Repeat Step 5 for each DHCP class you need to associate to the DHCP pool.
- If this command is not configured for a class, the default value is the entire subnet of the pool.

# Configure DHCP relay agent

Use this task to configure the client-facing interface as a relay agent port on the router.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ip dhcp snooping** command to enable the DHCP snooping feature globally

**Example:**

```
Router(config)# ip dhcp snooping
```

**Step 3** Use the **ip dhcp snooping vlan** *vlan-id* command to enable DHCP snooping for VLAN.

**Example:**

```
Router(config)# ip dhcp snooping vlan 5
```

**Step 4** Use these steps to configure SVI:

a) Use the **interface** *vlan-id* command to select the SVI corresponding to the client VLAN.

**Example:**

```
Router(config)# interface Vlan5
```

b) Use the **ip address** *ip-address subnet-mask* command to assign an IP address and subnet mask to the SVI.

**Example:**

```
Router(config-if)# ip address 10.166.1.1 255.255.0.0
```

c) Use the **ip helper-address** *ip-address* command to specify the IP address of the DHCP server.

**Example:**

```
Router(config-if)# ip helper-address 110.1.1.1
```

**Step 5** Use the **interface** command to select the specific interface connected to the client.

**Example:**

```
Router(config)# interface GigabitEthernet1/10
```

**Step 6** Use the **description** *client* command to provide a label for the client connection.

**Example:**

```
Router(config-if)# description CLIENT-1
```

**Step 7** Use the **switchport mode access** command to set the interface to access mode.

**Example:**

```
Router(config-if)# switchport mode access
```

**Step 8** Use the **switchport access vlan** command to assign the interface to the client VLAN.

**Example:**

```
Router(config-if)# switchport access vlan 5
```

**Step 9** (Optional) Use these commands to define custom Circuit ID and Remote ID values, overriding the defaults:

a) (Optional) Use the **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *circuit-id-string* command to override the default Circuit ID (**vlan mod port**) with a user-defined string.

**Example:**

```
Router(config-if)# ip dhcp snooping vlan 5 information option format-type circuit-id
string abc
```

b) (Optional) Use the **ip dhcp snooping information option format remote-id string** *remote-id-string* command to override the default Remote ID (MAC address) with a user-defined string.

**Example:**

```
Router(config)# ip dhcp snooping information option format remote-id string abc
```

c) Use the **exit** command to return to global configuration mode.

**Example:**

```
Router(config-if)# exit
```

### What to do next

For more information, see Configuring the Cisco IOS XE DHCP Relay Agent.

# Configure relay chaining on relay agents

Use this task to configure relay chaining when multiple relay agents are used in the network. Enabling encapsulation on the secondary relay agent ensures that the original DHCP Option 82 data is preserved as the request is forwarded to the DHCP server.

**Before you begin**

**Note**

- Ensure DHCP snooping is enabled on both relay agents for their respective client VLANs.
- Relay chaining requires that DHCP snooping be enabled on both relay agents for their respective client VLANs. Ensure that interfaces are correctly configured between the relay agents to allow the passage of DHCP traffic.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ip dhcp relay information option vpn** command to enable the inclusion of VPN information in the relay agent inforamtion.

**Example:**

```
Router(config)# ip dhcp relay information option vpn
```

**Step 3** Use the **ip dhcp relay information policy encapsulate** command to enable the encapsulation policy on the secondary relay agent.

**Example:**

```
Router(config)# ip dhcp relay information policy encapsulate
```

**Note** In a double relay agent scenario, this configuration must be applied on the relay agent closest to the server.

**Step 4** Use the **exit** command to return to privileged EXEC mode.

**Example:**

```
Router(config)# exit
```

An example of an encapsulated hexadecimal pattern format received by server in relay chaining is as given:

```
091f000000091a0a18bea80a0152120106000401f40105020800066 8d972ad3540020c020a00003c3c3c010e000000
```

# Verify DHCP Option 82

Use these steps to verify DHCP Option 82 configuration.

**Procedure**

**Step 1** Use these commands on the DHCP server side:

a) Use the **more system:running-config** command to display the running configuration.

**Example:**

```
Router# show running-config
```

**Note** This command will display the configured DHCP classes and DHCP pools.

b) Use the **show ip dhcp binding** command to display the client's MAC IP address.

**Example:**

```
Router# show ip dhcp binding
```

**Step 2** Use these commands on the DHCP relay agent side:

a) Use the **show ip dhcp snooping binding** command to verify the relay agent's snooping bindings.

**Example:**

```
Router# show ip dhcp snooping binding
```

b) Use the **show ip dhcp snooping** command to validate the Circuit ID and Remote ID.

**Example:**

```
Router# show ip dhcp snooping
```

# Debug DHCP Option 82 logs

Use this task to troubleshoot DHCP Option 82 configurations and derive the required hexadecimal patterns for class matching by enabling debug logs on both the DHCP server and the relay agent.

**Procedure**

**Step 1** Use the **debug ip dhcp server** command on the DHCP server to monitor server-side events, classes, and packets.

**Example:**

```
Router# debug ip dhcp server event
         Router# debug ip dhcp server class
         Router# debug ip dhcp server packet
```

**Step 2** Use the **debug ip dhcp snooping** command on the relay agent to monitor snooping events, agent processing, and packets.

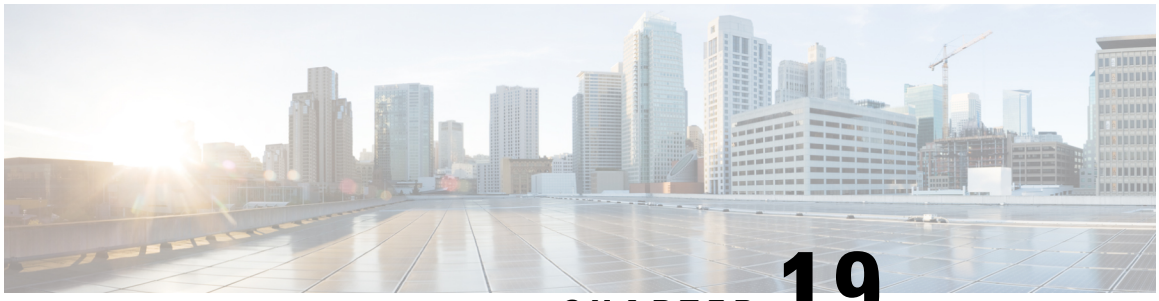
**Example:**

```
Router# debug ip dhcp snooping agent
         Router# debug ip dhcp snooping event
         Router# debug ip dhcp snooping packet
```

**Note** You can analyze the generated logs to identify the `relay-information` hexadecimal pattern being received by the server.

**Example:**

```
*May 13 2026 08:25:19.629: DHCPD: Searching for a match to 'relay-information
010600040005010a020701057065747261' in class class_turbine
          *May 13 2026 08:25:19.629: DHCPD: input pattern 'relay-information
010600040005010a020701057065747261' matches class CLASS1
```



CHAPTER 19

# IKEv2 and IPsec PFS Post Quantum Cryptography

*Table 17: Feature History Table*

| Feature name | Release information | Feature description |
|---|---|---|
| IKEv2 and IPsec PFS Post Quantum Cryptography | Release 26.2.1 | Cisco IoT routers can combine a traditional Diffie-Hellman key exchange with the NIST-standardized Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) to establish keys for IKEv2/IPsec sessions. This hybrid approach helps protect recorded VPN traffic against future harvest-now, decrypt-later attacks. |


- IKEv2 and IPsec PFS Post Quantum Cryptography, on page 159
- Benefits of PQC, on page 160
- Prerequisites, on page 160
- Limitations, on page 160
- ML-KEM algorithm and parameter sets, on page 161
- PFS negotiation behavior, on page 162
- Configure an IKEv2 proposal for PQC, on page 162
- Configure Perfect Forward Secrecy with PQC, on page 164
- Verify the PQC hybrid key exchange, on page 165
- Troubleshooting PQC hybrid key exchange, on page 166


# IKEv2 and IPsec PFS Post Quantum Cryptography

Quantum-Safe Encryption refers to cryptographic techniques designed to protect network communications against attacks by computers and future cryptographically relevant quantum computers.

Post-Quantum Cryptography (PQC) is part of this broader security approach. PQC includes quantum-resistant algorithms for functions such as key establishment and digital signatures. These algorithms help mitigate harvest-now, decrypt-later attacks, in which an attacker records encrypted traffic and attempts to decrypt it later using a sufficiently capable quantum computer.

PQC does not replace existing public-key algorithms. Instead, it works alongside them to create a quantum-safe hybrid key exchange.

The Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) is a National Institute of Standards and Technology (NIST)-standardized post-quantum key-encapsulation mechanism. ML-KEM enables two peers to establish a shared secret that can be used to derive cryptographic session keys.

On supported Cisco routers, ML-KEM is combined with a traditional key-exchange algorithm to provide a hybrid key establishment for IKEv2/IPsec Perfect Forward Secrecy (PFS). The hybrid approach protects the negotiated session as long as at least one of the constituent key-establishment mechanisms remains secure.

For more information on PQC on Cisco routers with IKEv2 sessions, see Security and VPN Configuration Guide.

For more information on Quantum-Safe Encryption and the related protocols, see: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html.



**Note** Postquantum preshared keys (PPKs), including dynamic PPKs obtained through the Secure Key Integration Protocol (SKIP), can be used with ML-KEM-based hybrid key establishment.

# Benefits of PQC

You can use the PQC feature to strengthen the security of your IPsec and IKEv2 connections with quantum-safe, future-proof protection for traffic between Cisco IoT routers.

The PQC hybrid key exchange provides these benefits:

- Future-proof security: Protects traffic against future quantum-computer-based attacks.
- Defense in depth: Combines a classical DH algorithm with ML-KEM, so the session stays secure even if one algorithm is broken.
- Smooth migration: Supports phased migration in existing networks through the optional fallback keyword.

# Prerequisites

Before you configure the PQC hybrid key exchange, ensure that the following requirements are met:

- Both peers support PQC, or the optional keyword is used to allow fallback during migration.
- IKEv2/IPsec is configured and operational between the peers.

# Limitations

The limitations with respect to using PQC are:

- IKEv2 always uses hybrid key exchange: a combination of Diffie-Hellman (DH) and ML-KEM algorithms. Pure-PQC key exchange is not supported for IKEv2.

- The encapsulation keys and ciphertexts used by ML-KEM-768 and ML-KEM-1024 may cause IKEv2 messages to exceed typical path maximum transmission units (MTUs), resulting in IP fragmentation and potential packet drops. To avoid IP fragmentation, enable IKEv2 fragmentation and set the IKEv2 fragmentation MTU to 1400 bytes.
- This feature provides post-quantum key establishment only. It does not provide post-quantum peer authentication. IKEv2 peers continue to use the configured authentication method, such as a preshared key or certificate-based authentication.
- ML-KEM establishes shared keying material; it does not encrypt user traffic. The encryption algorithm configured in the IPsec transform set, such as AES-CBC or AES-GCM, continues to encrypt the user traffic.

**Note** License, platform, and software support: This feature does not require an additional feature license. ML-KEM-based quantum-safe key establishment is supported on all Cisco IoT routers with Cisco IOS XE Release 26.2.1.

### Supported routers

The supported routers are:

- Cisco Catalyst IR1101 Rugged Series Router,
- Cisco Catalyst IR1800 Rugged Series Router,
- Cisco Catalyst IR8340 Rugged Series Router,
- Cisco Catalyst IR8140 Heavy Duty Router, and
- Cisco ESR6300 Embedded Series Router.

## Phased migration in Hub-and-Spoke deployments

If an older responder (hub) receives a PQC proposal from upgraded spokes (initiators), the negotiation fails.

To avoid this, it is recommended that you always upgrade the hub first and configure **optional** in the hub's IKEv2 proposal.

When any issue occurs, the responder logs the following errors:

IKEv2-INTERNAL: Transform type 6 invalid.

IKEv2-ERROR: Failed to parse the packet: The peer's proposal is invalid.

# ML-KEM algorithm and parameter sets

Cisco IoT routers support the three National Institute of Standards and Technology (NIST)-standardized ML-KEM parameter sets: ML-KEM-512, ML-KEM-768, and ML-KEM-1024. During the key exchange, the peers exchange an encapsulation key (public key) and a ciphertext.

*Table 18: ML-KEM parameter sets (sizes in bytes)*

| Parameter | ML-KEM-512 | ML-KEM-768 | ML-KEM-1024 |
|---|---|---|---|
| Encapsulation key size (public key) | 800 | 1184 | 1568 |
| Decapsulation key size (private key) | 1632 | 2400 | 3168 |
| Shared secret key size | 32 | 32 | 32 |
| Ciphertext size | 768 | 1088 | 1568 |

# PFS negotiation behavior

*Table 19: PFS negotiation behavior for Cisco IOS XE to Cisco IOS XE devices*

| Initiator/ Responder | no set pfs | set pfs | set pfs <group> | set pfs <group> pqc <mlkem> |
|---|---|---|---|---|
| **set pfs** | UP (ML-KEM inherit) | UP (ML-KEM inherit) | UP (DH+ML-KEM inherit) | UP (DH+ML-KEM inherit) |
| **set pfs** <*group*> | UP (DH) | DOWN | UP (DH) | DOWN |
| **set pfs** <*group*> **pqc** <*mlkem*> | UP (DH+ML-KEM) | UP (DH+ML-KEM inherit) | UP (DH+ML-KEM) | UP (DH+ML-KEM) |

**Note** During initial session establishment, `CHILD_SA` output might display `PFS: N`. After the `CHILD_SA` rekeys, verify the negotiated ML-KEM and DH PFS settings.

# Configure an IKEv2 proposal for PQC

Follow these steps to enable ML-KEM algorithm in an IKEv2 proposal.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **crypto ikev2 fragmentation mtu** *mtu-size* command to enable IKEv2 fragmentation and set the IKEv2 fragmentation MTU to 1400 bytes.

**Example:**

```
Router(config)# crypto ikev2 fragmentation mtu 1400
```

**Step 3** Use the **crypto ikev2 proposal** *name* command to create or edit an IKEv2 proposal.

**Example:**

```
Router(config)# crypto ikev2 proposal prop1
```

**Step 4** Use the **encryption** *aes-cbc-key* command to configure AES key in CBC mode.

**Example:**

```
Router(config-ikev2-proposal)# encryption aes-cbc-256
```

a) Use the **integrity** *integrity-algorithm* command to configure the IKEv2 integrity algorithm.

**Example:**

```
Router(config-ikev2-proposal)# integrity sha512
```

b) Use the **group** *group-number* command to configure Diffie-Hellman group for classical key exchange used with ML-KEM.

**Example:**

```
Router(config-ikev2-proposal)# group 19
```

**Step 5** Use the **pqc mlkem1024 mlkem768 mlkem512 optional** command to enable one or more ML-KEM algorithm parameter sets.

**Example:**

```
Router(config-ikev2-proposal)# pqc mlkem1024 mlkem768 mlkem512 optional
```

**Note** The proposal enables **pqc mlkem768 optional** by default. The **optional** keyword allows the SA to fall back to a classical (non-PQC) negotiation if the peer does not support PQC, which supports coexistence during phased migration.

**Step 6** Use these commands to create the IKEv2 policy and attach the proposal:

a) Use the **crypto ikev2 policy** *policy* command to create the IKEv2 policy.

**Example:**

```
Router(config)# crypto ikev2 policy pol1
```

b) Use the **match fvrf any** command to apply the IKEv2 policy to negotiations through any front-door VRF (FVRF).

**Example:**

```
Router(config-ikev2-policy)# match fvrf any
```

c) Use the **proposal** *proposal-name* command to add the PQC-enabled proposal to the IKEv2 policy.

**Example:**

```
Router(config-ikev2-policy)# proposal prop1
```

The **proposal** *proposal* command makes the PQC-enabled proposal available during IKEv2 negotiation for sessions that match this policy.

**Step 7** Use these commands to associate the existing IKEv2 profile with the IPsec profile:

a) Use the **crypto ipsec profile** *profile-name* command to create an IPsec profile.

**Example:**

```
Router(config)# crypto ipsec profile gen
```

b) Use the **set ikev2-profile** *ikev2-profile-name* command to associate an existing IKEv2 profile with the IPsec profile.

**Example:**

```
Router(ipsec-profile)# set ikev2-profile prof1
```

**Note** The profile and IPsec transform set can already exist, if not you can create it using the create IPsec profile option given in step 7.

**Step 8** Use these commands to apply the IPsec profile to the tunnel:

a) Use the **interface tunnel** *tunnel-interface-number* command to create a tunnel interface.

**Example:**

```
Router(config)# interface tunnel 1
```

b) Use the **tunnel protection ipsec profile** *ipsec-profile-name* command to protect the tunnel with IPsec profile.

**Example:**

```
Router(config-if)# tunnel protection ipsec profile gen
```

**Step 9** Use the **end** command to return to privileged EXEC mode.

**Example:**

```
Router(config-if)# end
```

# Configure Perfect Forward Secrecy with PQC

Perfect Forward Secrecy (PFS) adds extra randomness to derive session keys during each key exchange. With PQC, the key exchange can use DH, ML-KEM, or DH + ML-KEM. PFS is optional and can be disabled.

Follow these steps to configure PFS with PQC.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **crypto ipsec profile** *name* command to enter the IPsec profile.

**Example:**

```
Router(config)# crypto ipsec profile P1
```

**Step 3** Use the **set pfs** *group* **pqc** *mlkem-algorithm* command to enable PFS, specify a DH group, and an ML-KEM algorithm, or both.

**Example:**

```
Router(ipsec-profile)# set pfs group19 pqc mlkem1024
```

**Note** When **set pfs** is used:

- Without PQC: Starting from Cisco IOS XE Release 26.2.1 onwards, the DH group is inherited from the IKEv2 SA.
- With PQC: The DH group is inherited from the IKEv2 SA. Exchanges are optimized for Cisco IOS XE to Cisco IOS XE deployments using an ML-KEM-only IPsec Child Security Association exchange.

# Verify the PQC hybrid key exchange

Follow these steps to verify that the PQC hybrid key exchange is active.

**Procedure**

**Step 1** Use the **show crypto ikev2 sa detail** command to verify the IKEv2 SA and the PQC key exchange algorithm.

**Example:**

```
Router# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local              Remote             fvrf/ivrf   Status
1         10.0.149.203/500   10.0.149.217/500   none/none   READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth
verify: PSK
PQC Key Exchange: ML-KEM-1024
...
Quantum-safe Encryption using PQC: ML-KEM-1024
PEER TYPE: IOS-XE
```

**Step 2** Use the **show crypto ipsec sa** command to verify the IPsec SA. The PQC key exchange appears after the first IPsec SA rekey.

**Example:**

```
Router# show crypto ipsec sa
...
PFS (Y/N): Y, DH group: group19, PQC Key Exchange: ML-KEM-1024
```

**Note** The PQC key exchange value in the IPsec SA output appears only after an IPsec SA rekey.

When the show commands display the configured ML-KEM algorithm and the tunnel status is READY, the quantum-safe hybrid key exchange is active.

# Troubleshooting PQC hybrid key exchange

Use these debug commands to troubleshoot PQC hybrid key exchange issues on a Cisco IoT router.

Follow these steps to debug the PQC hybrid key exchange.

### Procedure

**Step 1** Use the **debug crypto ikev2** commands to debug IKEv2 negotiation, errors, packets, and internal events.

**Example:**

```
Router# debug crypto ikev2
Router# debug crypto ikev2 error
Router# debug crypto ikev2 packet
Router# debug crypto ikev2 internal
```

**Step 2** Use the **debug crypto kmi** command to debug Key Management Infrastructure (KMI) events.

**Example:**

```
Router# debug crypto kmi
```

**Step 3** Use the **debug crypto socket** command to debug crypto socket events.

**Example:**

```
Router# debug crypto socket
```

**Step 4** Use the **debug crypto ipsec** commands to debug IPsec negotiation, errors, messages, and state changes.

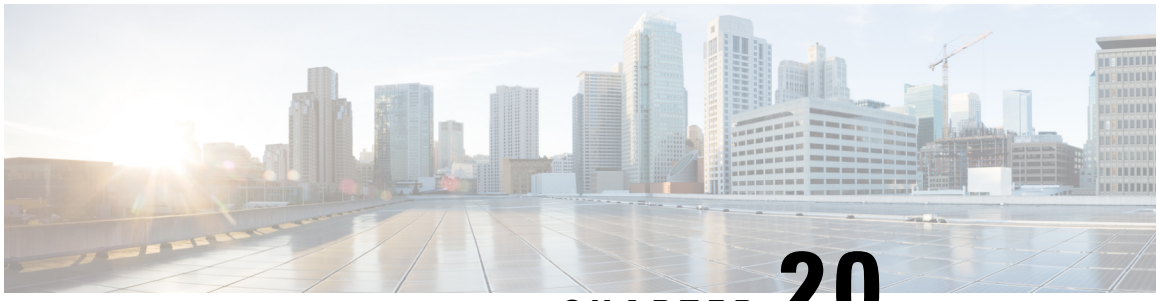
**Example:**

```
Router# debug crypto ipsec
Router# debug crypto ipsec error
Router# debug crypto ipsec message
Router# debug crypto ipsec state
```

**Step 5** Use the **debug tunnel protection** command to debug tunnel protection events.

**Example:**

```
Router# debug tunnel protection
```



CHAPTER 20

# Post Quantum Cryptography for SSHv2 sessions

*Table 20: Feature History Table*

| Feature name | Release information | Feature description |
|---|---|---|
| Post Quantum Cryptography for SSHv2 sessions | Release 26.2.1 | Cisco IoT routers can combine the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) with classical elliptic-curve key-exchange algorithms to establish keys for SSHv2 sessions. |


- Implementation of Post Quantum Cryptography, on page 167
- Overview, on page 168
- Factors to consider for deploying PQC, on page 168
- Protocol requirements, on page 168
- Restrictions for PQC, on page 168
- PQC negotiation scenarios , on page 169
- Configure PQC for SSHv2 sessions, on page 169
- Verify PQC for SSHv2 sessions, on page 170
- Key elements of PQC, on page 170
- Supported platforms, on page 172


# Implementation of Post Quantum Cryptography

Cisco utilizes a hybrid approach to implement Post Quantum Cryptography (PQC). The hybrid approach to PQC combines a quantum-resistant algorithm, such as the module-lattice based ML-KEM (e.g., mlkem768), with a classical elliptic curve key exchange algorithm like NIST P-256 or X25519, along with a hash function such as SHA-256.

This combination provides enhanced security by protecting against both classical and quantum attacks while maintaining compatibility and performance with existing cryptographic protocols.

Cisco implements this hybrid approach in protocols like SSH allowing configurations that enforce the use of ML-KEM algorithms for quantum resistance without falling back to classical-only key exchanges.

# Overview

PQC refers to cryptographic algorithms designed to be secure against attacks from quantum computers which can break many classical encryption methods. Current widely used encryption methods—such as Diffie-Hellman (DH), and Elliptic Curve Diffie-Hellman (ECDH) — are vulnerable to being broken as quantum computing technology advances.

Implementing quantum-safe encryption now is critical for the long-term confidentiality and integrity of sensitive communications, particularly for government, military, and financial sectors.

# Factors to consider for deploying PQC

Review these factors before deploying PQC.

**Backward compatibility with classical algorithms**
If a device is only configured for PQC and the SSH client does not support PQC, the SSH session will fail and no connection will be established.
**Impact on computational time**
The key size in PQC implementations may have an impact on the computational time due to the mathematical complexity and processing requirements of quantum-resistant algorithms. Larger key sizes generally increase the computational workload. PQC implementations must consider hardware acceleration and software optimizations to mitigate the increased computational time due to larger key sizes.

# Protocol requirements

## Protocol requirements

**SSHv2 :**

To establish secure, encrypted, and remote command-line access to servers and network devices over unsecured network use SSH version 2.0. PQC cannot be implemented on SSHv1 due to severe security vulnerabilities and it does not support the modern, complex key exchange mechanisms required to resist quantum computer attacks.

**Key Pairs :**

Ensure that RSA key pair or EC key pair for the SSH server is generated using crypto key generate command.

# Restrictions for PQC

Implementing PQC is not supported on devices that operate in Federal Information Processing Standards (FIPS) mode.

# PQC negotiation scenarios

During the SSH protocol connection setup, the client and server negotiate which cryptographic algorithms to use for securing the session. This negotiation process is a basic example of how algorithm negotiation works in SSH and is applicable to any similar negotiation process.

The algorithms are considered in the order they are configured on the device, meaning the priority or preference of algorithms is determined by the sequence in which they are listed in the configuration. The negotiation proceeds by trying the algorithms in that configured order until a mutually supported algorithm is found and agreed upon for use in the session. The server must support at least one algorithm from the client's list for successful negotiation.

***Table 21: sfds***

| Client configuration | Server configuration | Negotiated algorithm |
|---|---|---|
| Classical, Hybrid | Classical, Hybrid | Classical |
| Hybrid, Classical | Hybrid, Classical | Hybrid |
| Classical, Hybrid | Hybrid | Hybrid |
| Hybrid, Classical | Classical | Classical |
| Classical | Classical, Hybrid | Classical |
| Hybrid | Classical, Hybrid | Hybrid |
| Classical | Hybrid | None |
| Hybrid | Classical | None |
| Mixed (No overlap) | Mixed (No overlap) | None |

# Configure PQC for SSHv2 sessions

Use these commands to set up devices as an SSH server and an SSH client. This allows the device to accept connection requests from remote SSH clients, enabling secure remote management of the device through SSH connections.

**Note** The PQC algorithms are not enabled by default and must be explicitly enabled.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **ip ssh server algorithm kex** *algorithm* command to configure the PQC based key-exchange algorithms that the SSH server supports.

**Example:**

```
Router(config)# ip ssh server algorithm kex mlkem768nistp256-sha256
```

**Step 3** Use the **ip ssh client algorithm kex** *algorithm* command to configure the PQC based key-exchange algorithms that SSH client supports.

**Example:**

```
Router(config)# ip ssh client algorithm kex mlkem768x25519-sha256
```

This command is used to define the order and selection of key exchange (KEX) algorithms that the SSH client will use during the SSH handshake process.

# Verify PQC for SSHv2 sessions

Use this section to understand how to verify PQC implementation for SSHv2.

| Command | Purpose | What to look for in output |
|---|---|---|
| **show ip ssh** | Displays the status of the SSH server, its configuration details. | In the output of this command, look for these details that indicate PQC implementation is successful:<br>KEX algorithms:<br>**mlkem1024nistp384-sha384,**<br>**mlkem768nistp256-sha256,**<br>**mlkem768x25519-sha256** |

This example shows the response when a PQC algorithm command is entered on a platform that does not support PQC.

```
Router(config)# ip ssh server algorithm kex mlkem1024nistp384-sha384 ecdh-sha2-nistp256
Router(config)#
000205: Jun 18 16:41:43.086: %SSH-3-KEX_PQC_NOT_SUPP: PQ/T hybrid key exchange algorithms
are not supported on this platform.
Router(config)#
```

# Key elements of PQC

PQC is implemented by using the algorithms available as part of Module-lattice based Cryptography. Module-lattice based Cryptography is a type of quantum-resistant public-key cryptography that uses structured, high-dimensional grid points (lattices) to secure data. Cisco implements PQC into protocols like SSH using ML-KEM.

These algorithms are resistant to quantum attacks and are used for secure key establishment, encryption, and digital authentication or signatures.

This table lists the areas in which each algorithm can be used:

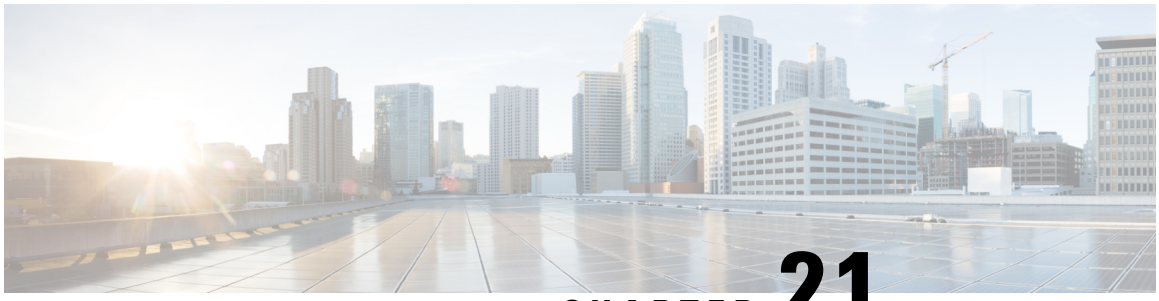
| ML-KEM algorithm | What this algorithm means | Security Level |
|---|---|---|
| mlkem768x25519-sha256 | ML-KEM 768 is a PQC algorithm based on module-lattice cryptography, providing resistance against quantum attacks.<br>X25519 is a widely used classical elliptic curve Diffie-Hellman key exchange algorithm.<br>SHA-256 is the hash function used for cryptographic hashing in the key exchange process.<br>In summary, mlkem768x25519-sha256 is a hybrid PQC key exchange algorithm combining the ML-KEM 768-bit lattice-based scheme with classical X25519 and SHA-256, used to secure key exchanges against quantum and classical threats in Cisco's PQC-enabled network protocols. | The security level of this implementation is balanced and is best suited for deployments where performance metrics are critical. |
| mlkem768nistp256-sha256 | ML-KEM 768 is a PQC algorithm based on module-lattice cryptography, providing resistance against quantum attacks.<br>NIST P-256 is a widely used classical elliptic curve Diffie-Hellman key exchange algorithm standardized by NIST.<br>SHA-256 is the hash function used for cryptographic hashing in the key exchange process.<br>In summary, mlkem768x25519-sha256 is a hybrid PQC key exchange algorithm combining the ML-KEM 768-bit lattice-based scheme with classical X25519 and SHA-256, used to secure key exchanges against quantum and classical threats in Cisco's PQC-enabled network protocols. | The security level of this implementation is good and is best suited for most deployments. |

| ML-KEM algorithm | What this algorithm means | Security Level |
|---|---|---|
| mlkem1024nistp384-sha384 | ML-KEM 768 is a PQC algorithm based on module-lattice cryptography, providing resistance against quantum attacks.<br>1024 is the highest security parameter set, equivalent to the security level of AES-256.<br>NIST P-384 is the traditional (classical) component. It uses Elliptic Curve Diffie-Hellman (ECDH) with the NIST P-384 curve to maintain security against current non-quantum threats.<br>In summary, mlkem1024nistp384-sha384 represents a hybrid cryptographic proposal combining a quantum-resistant ML-KEM algorithm with classical elliptic curve cryptography (NIST P-384) and SHA-384 hashing. This hybrid approach ensures security against both classical and quantum attacks by negotiating keys using both classical and post-quantum algorithms. | The security level of this implementation is the highest and is best suited for deployments where maximum security is needed. |

# Supported platforms

PQC can be configured only on these platforms in autonomous mode:

- Cisco Catalyst IR1101 Rugged Series Routers,
- Cisco IR1000 Rugged Series Secure Routers
- Cisco Catalyst IR1800 Rugged Series Routers,
- Cisco Catalyst IR8140 Heavy Duty Series Routers,
- Cisco Catalyst IR8340 Rugged Series Routers,
- Cisco Embedded Service 6300 Series Routers.



CHAPTER 21

# System messages

This section provides details on system messages to facilitate effective monitoring and maintenance of the system.


- Information about process management, on page 173
- How to Find Error Message Details, on page 173


# Information about process management

Process management is the infrastructure for starting and monitoring software on a router.

- It is platform independent.
- It provides consistent error messages across platforms running on Cisco IOS XE.

### Remote monitoring and system messages

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. While direct involvement in process management is not required, reviewing system messages regarding process failures and other issues is recommended.

# How to Find Error Message Details

Provides guidance on using the Error Message Decoder tool to resolve system errors by entering specific message strings to retrieve detailed explanations and recommended troubleshooting steps.

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.

*Table 22: Error Message: %PMAN-0-PROCESS_NOTIFICATION*

| 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. |

*Table 23: Error Message: %PMAN-0-PROCFAILCRIT*

| 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 . Search for resolved software issues using the Bug Search Tool at: https://bst.cloudapps.cisco.com/bugsearch . 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. 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. |

*Table 24: Error Message: %PMAN-3-PROCFAILOPT*

| 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. Search for resolved software issues using the Bug Search Tool at: https://bst.cloudapps.cisco.com/bugsearch . 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. 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. |

*Table 25: Error Message: %PMAN-3-PROCFAIL*

| Explanation | Recommended Action |
|---|---|
| The process has failed as the result of an error. | 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 . Search for resolved software issues using the Bug Search Tool at: https://bst.cloudapps.cisco.com/bugsearch . 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. 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. |

*Table 26: Error Message: %PMAN-3-PROCFAIL_IGNORE*

| 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. |

*Table 27: Error Message: %PMAN-3-PROCHOLDDOWN*

| 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 . Search for resolved software issues using the Bug Search Tool at: https://bst.cloudapps.cisco.com/bugsearch . 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. 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. |

*Table 28: Error Message: %PMAN-3-RELOAD_RP_SB_NOT_READY*

| 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. |

*Table 29: Error Message: %PMAN-3-RELOAD_RP*

| 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. |

*Table 30: Error Message: %PMAN-3-RELOAD_SYSTEM*

| 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. |

*Table 31: Error Message: %PMAN-3-PROC_BAD_EXECUTABLE*

| 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. |

*Table 32: Error Message: %PMAN-3-PROC_BAD_COMMAND*

| 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. |

*Table 33: Error Message: %PMAN-3-PROC_EMPTY_EXEC_FILE*

| Explanation | Recommended Action |
|---|---|
| The executable file used for the process is empty. | Ensure that the named executable is non-zero in size. |

*Table 34: Error Message: %PMAN-5-EXITACTION*

| 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. |

*Table 35: Error Message: %PMAN-6-PROCSHUT*

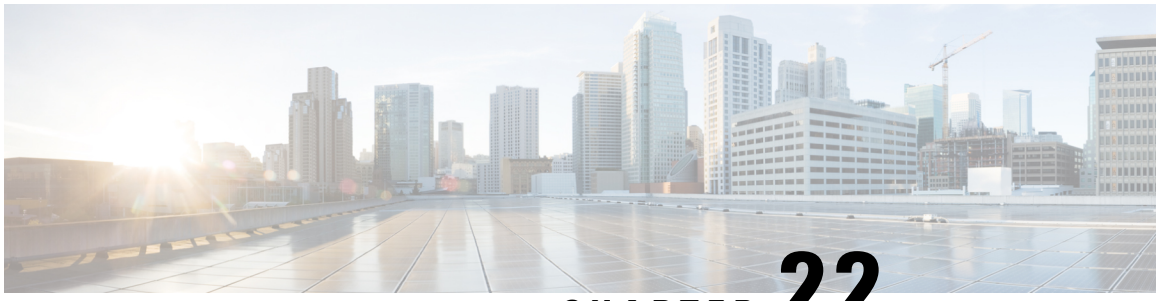
| Explanation | Recommended Action |
|---|---|
| The process has gracefully shut down. | No user action is necessary. This message is provided for informational purposes only. |

*Table 36: Error Message: %PMAN-6-PROCSTART*

| Explanation | Recommended Action |
|---|---|
| The process has launched and is operating properly. | No user action is necessary. This message is provided for informational purposes only. |

*Table 37: Error Message: %PMAN-6-PROCSTATELESS*

| Explanation | Recommended Action |
|---|---|
| The process has requested a stateless restart. | No user action is necessary. This message is provided for informational purposes only. |



CHAPTER 22

# Environmental monitoring

Provides information about environmental monitoring sections and capabilities.


- Environmental monitoring, on page 179


# Environmental monitoring

Provides information about environmental monitoring sections and capabilities.

## Environmental monitoring

Environmental monitoring is a router system that monitors environmental conditions and responds to abnormal events.

- monitors temperature of CPUs and motherboard
- records abnormal events and generates notifications
- monitors Simple Network Management Protocol (SNMP) traps
- generates and collects Onboard Failure Logging (OBFL) data
- sends call home event notifications
- logs system error messages, and
- displays present settings and status.

## Environmental monitoring and reporting functions

Environmental monitoring and reporting functions are system capabilities that allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

### Function types

The environmental monitoring and reporting functions include:


- Environmental monitoring functions, on page 180
- Environmental Reporting Functions, on page 181

# Environmental monitoring functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

### Environmental operating conditions

The router is expected to meet the following environmental operating conditions

- Non-operating Temperature: -40°F to 158°F (-40°C to 70°C)
- Non-operating Humidity: 5 to 95% relative humidity (non-condensing)
- Operating Temperature:

  -40° to 140°F (-40° to 60°C) in a sealed NEMA cabinet with no airflow

  -40° to 158°F (-40° to 70°C) in a vented cabinet with 40 lfm of air

  -40° to 167°F (-40° to 75°C) in a forced air enclosure with 200 lfm of air
- Operating Humidity: 10% to 95% relative humidity (non-condensing)
- Operating Altitude: -500 to 5,000 feet. Derate max operating temperature 1.5°C per 1000 feet.

### Status condition levels

The following table displays the levels of status conditions used by the environmental monitoring system.

***Table 38: 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. |

### Temperature and voltage cxceed max or min thresholds

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

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

Provides a list of commands to monitor and report environmental status for the router.

The following commands are available to retrieve and display environmental status reports:

- **show diag all eeprom**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform** and **show platform diag**
- **show platform software status control-processor**
- **show diag slot R0 eeprom detail**
- **show version** and **show power**
-

```
Router# show diag all eeprom
MIDPLANE EEPROM data:
Product Identifier (PID) : IR8140H-P-K9
Version Identifier (VID) : V00
PCB Serial Number : FDO24370MFT
Top Assy. Revision : 15
Hardware Revision : 0.1
Asset ID : P2
CLEI Code : UNASSIGNED
External PoE Module POE0 EEPROM data is not initialized
Internal PoE is not present
Slot R0 EEPROM data:
Product Identifier (PID) : IR8140H-P-K9
Version Identifier (VID) : V00
PCB Serial Number : FDO24370MFT
Top Assy. Revision : 15
Hardware Revision : 0.1
CLEI Code : UNASSIGNED
Slot F0 EEPROM data:
Product Identifier (PID) : IR8140H-P-K9
Version Identifier (VID) : V00
PCB Serial Number : FDO24370MFT
Top Assy. Revision : 15
Hardware Revision : 0.1
CLEI Code : UNASSIGNED
Slot 0 EEPROM data:
Product Identifier (PID) : IR8140H-P-K9
Version Identifier (VID) : V00
PCB Serial Number : FDO24370MFT
Top Assy. Revision : 15
Hardware Revision : 0.1
CLEI Code : UNASSIGNED
Slot 1 EEPROM data is not initialized
Slot 2 EEPROM data is not initialized
Slot 3 contains a BBU Unit.
```

```
Please use 'show platform hardware battery sprom [details]' to get EEPROM data.
Slot 4 contains a BBU Unit.
Please use 'show platform hardware battery sprom [details]' to get EEPROM data.
Slot 5 contains a BBU Unit.
Please use 'show platform hardware battery sprom [details]' to get EEPROM data.
SPA EEPROM data for subslot 0/0:
Product Identifier (PID) : IR8140H-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) : IRMH-WPAN-NA
Version Identifier (VID) : V00
PCB Serial Number : FDO24350D18
Top Assy. Revision : 07
Hardware Revision : 2.0
CLEI Code : UNASSIGNED
SPA EEPROM data for subslot 0/2:
Product Identifier (PID) : IRMH-LTEAP18-GL
Version Identifier (VID) : V00
PCB Serial Number : FDO24360MVH
Hardware Revision : 1.0
CLEI Code : N/A
SPA EEPROM data for subslot 0/3:
Product Identifier (PID) : IRMH-LTEA-EA
Version Identifier (VID) : V00
PCB Serial Number : FDO24360MU4
Hardware Revision : 1.0
CLEI Code :
SPA EEPROM data for subslot 0/4 is not available
SPA EEPROM data for subslot 0/5 is not available
SPA EEPROM data for subslot 0/6 is not available
SPA EEPROM data for subslot 1/0 is not available
SPA EEPROM data for subslot 1/1 is not available
SPA EEPROM data for subslot 1/2 is not available
SPA EEPROM data for subslot 1/3 is not available
SPA EEPROM data for subslot 1/4 is not available
SPA EEPROM data for subslot 1/5 is not available
SPA EEPROM data for subslot 1/6 is not available
SPA EEPROM data for subslot 2/0 is not available
SPA EEPROM data for subslot 2/1 is not available
SPA EEPROM data for subslot 2/2 is not available
SPA EEPROM data for subslot 2/3 is not available
SPA EEPROM data for subslot 2/4 is not available
SPA EEPROM data for subslot 2/5 is not available
SPA EEPROM data for subslot 2/6 is not available
SPA EEPROM data for subslot 3/0 is not available
SPA EEPROM data for subslot 3/1 is not available
SPA EEPROM data for subslot 3/2 is not available
SPA EEPROM data for subslot 3/3 is not available
SPA EEPROM data for subslot 3/4 is not available
SPA EEPROM data for subslot 3/5 is not available
SPA EEPROM data for subslot 3/6 is not available
SPA EEPROM data for subslot 4/0 is not available
SPA EEPROM data for subslot 4/1 is not available
SPA EEPROM data for subslot 4/2 is not available
SPA EEPROM data for subslot 4/3 is not available
SPA EEPROM data for subslot 4/4 is not available
SPA EEPROM data for subslot 4/5 is not available
SPA EEPROM data for subslot 4/6 is not available
SPA EEPROM data for subslot 5/0 is not available
```

```
SPA EEPROM data for subslot 5/1 is not available
SPA EEPROM data for subslot 5/2 is not available
SPA EEPROM data for subslot 5/3 is not available
SPA EEPROM data for subslot 5/4 is not available
SPA EEPROM data for subslot 5/5 is not available
SPA EEPROM data for subslot 5/6 is not available
Router#
```

```
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 39 Celsius (80 ,85 ,90 ,na )(Celsius)
Router#
```

```
Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: LM75BXXX R0 Normal 48 Celsius
```

```
Router# show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco Catalyst IR8140H Heavy Duty Series Router with PoE"
PID: IR8140H-P-K9 , VID: V00 , SN: FDO2441J91D
NAME: "Power Supply Module 0", DESCR: "60W AC Power Supply module"
PID: IRMH-PWR60W-AC , VID: V01 , SN: LIT22503LDK
NAME: "module 0", DESCR: "Cisco Catalyst IR8140H-P-K9 Fixed and pluggable Interface Module
 controller"
PID: IR8140H-P-K9 , VID: , SN:
NAME: "NIM subslot 0/1", DESCR: "IRMH-WPAN-NA Module"
PID: IRMH-WPAN-NA , VID: V00 , SN: FDO24350D18
NAME: "NIM subslot 0/2", DESCR: "IRMH-LTEAP18-GL Module"
PID: IRMH-LTEAP18-GL , VID: V00 , SN: FDO24360MVH
NAME: "Modem on Cellular0/2/0", DESCR: "Telit LM960"
PID: LM960 , VID: 1.0 , SN: 358347100029266
NAME: "PIM subslot 0/2", DESCR: "P-LTEAP18-GL Module"
PID: P-LTEAP18-GL , VID: V01 , SN: FOC242100XW
NAME: "NIM subslot 0/3", DESCR: "IRMH-LTEA-EA Module"
PID: IRMH-LTEA-EA , VID: V00 , SN: FDO24360MU4
NAME: "Modem on Cellular0/3/0", DESCR: "Sierra Wireless EM7455"
PID: EM7455 , VID: 1.0 , SN: 356129072307959
NAME: "PIM subslot 0/3", DESCR: "P-LTEA-EA Module"
PID: P-LTEA-EA , VID: V02 , SN: FOC24290CZ2
NAME: "NIM subslot 0/0", DESCR: "Front Panel 2 port Gigabitethernet Module"
PID: IR8140H-2x1GE , VID: V01 , SN:
NAME: "subslot 0/0 transceiver 1", DESCR: "GE T"
PID: GLC-TE , VID: V03 , SN: AVC24140C5S
NAME: "module 1", DESCR: "Supervisor Module with 1 Copper + 1 Fiber Port for IR8140"
PID: IRMH-SUP-SP , VID: , SN:
NAME: "module 3", DESCR: "Stackable Battery Backup unit for IR8140"
PID: CGR-BATT-4AH , VID: V03 , SN: NVT24231754
NAME: "module 4", DESCR: "Stackable Battery Backup unit for IR8140"
PID: CGR-BATT-4AH , VID: V03 , SN: NVT24233031
NAME: "module 5", DESCR: "Stackable Battery Backup unit for IR8140"
PID: CGR-BATT-4AH , VID: V03 , SN: NVT24232260
NAME: "module R0", DESCR: "Cisco Catalyst IR8140H-P-K9 Route Processor"
PID: IR8140H-P-K9 , VID: V00 , SN: FDO24370MFT
NAME: "module F0", DESCR: "Cisco Catalyst IR8140H-P-K9 Forwarding Processor"
PID: IR8140H-P-K9 , VID: , SN:
```

```
Router# show platform
Chassis type: IR8140H-P-K9
```

```
Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 IR8140H-P-K9 ok 01:35:07
0/0 IR8140H-2x1GE ok 01:33:56
0/1 IRMH-WPAN-NA ok 01:33:55
0/2 IRMH-LTEAP18-GL ok 01:33:55
0/3 IRMH-LTEA-EA ok 01:33:55
1 IRMH-SUP-SP ok 01:35:07
R0 IR8140H-P-K9 ok, active 01:35:07
F0 IR8140H-P-K9 ok, active 01:35:07
P0 IRMH-PWR60W-AC ok 01:34:29
Router#
```

```
Router# show platform diag
Chassis type: IR8140H-P-K9
Slot: 0, IR8140H-P-K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:42 (01:35:35 ago)
Software declared up time : 00:01:31 (01:34:46 ago)
CPLD version :
Firmware version : 1.4(DEV) [root-vganev 100]
Sub-slot: 0/0, IR8140H-2x1GE
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:01:53 (01:34:23 ago)
Logical insert detect time : 00:01:53 (01:34:23 ago)
Sub-slot: 0/1, IRMH-WPAN-NA
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:01:54 (01:34:23 ago)
Logical insert detect time : 00:01:54 (01:34:23 ago)
Sub-slot: 0/2, IRMH-LTEAP18-GL
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:01:54 (01:34:23 ago)
Logical insert detect time : 00:01:54 (01:34:23 ago)
Sub-slot: 0/3, IRMH-LTEA-EA
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:01:54 (01:34:22 ago)
Logical insert detect time : 00:01:54 (01:34:22 ago)
Slot: 1, IRMH-SUP-SP
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:42 (01:35:35 ago)
Software declared up time : 00:00:00 (never ago)
CPLD version : N/A
Firmware version : N/A
Slot: R0, IR8140H-P-K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:42 (01:35:35 ago)
Software declared up time : 00:00:42 (01:35:35 ago)
CPLD version : 00000000
Firmware version : 1.4(DEV) [root-vganev 100]
Slot: F0, IR8140H-P-K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:42 (01:35:35 ago)
Software declared up time : 00:01:32 (01:34:44 ago)
```

```
Hardware ready signal time : 00:00:00 (never ago)
Packet ready signal time : 00:01:38 (01:34:38 ago)
CPLD version : 00000000
Firmware version : 1.4(DEV) [root-vganev 100]
Slot: P0, IRMH-PWR60W-AC
State : ok
Physical insert detect time : 00:01:20 (01:34:57 ago)
Slot: GE-POE, Unknown
State : NA
Physical insert detect time : 00:00:00 (never ago)
Router#
```

```
Router# show platform software status control-processor
RP0: online, statistics updated 1 seconds ago
Load Average: healthy
1-Min: 1.04, status: healthy, under 5.00
5-Min: 0.94, status: healthy, under 5.00
15-Min: 0.96, status: healthy, under 5.00
Memory (kb): healthy
Total: 8116912
Used: 3315056 (41%), status: healthy
Free: 4801856 (59%)
Committed: 3109960 (38%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.25, System: 2.51, Nice: 0.00, Idle: 92.99
IRQ: 2.71, SIRQ: 0.52, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 4.34, System: 3.43, Nice: 0.00, Idle: 92.21
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 4.02, System: 2.31, Nice: 0.00, Idle: 93.25
IRQ: 0.40, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 23.50, System: 39.40, Nice: 0.00, Idle: 28.69
IRQ: 8.38, SIRQ: 0.00, IOwait: 0.00
Router#
```

```
Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:
EEPROM version : 4
Compatible Type : 0xFF
Hardware Revision : 0.1
PCB Part Number : 73-104919-02
Board Revision : 03
Deviation Number : 0
Fab Version : 02
PCB Serial Number : FDO24370MFT
Top Assy. Part Number : 68-102792-02
Top Assy. Revision : 15
Chassis Serial Number : FDO2441J91D
Product Identifier (PID) : IR8140H-P-K9
Version Identifier (VID) : V00
CLEI Code : UNASSIGNED
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Asset ID : P2
Asset Alias : 20530
Power Consumption : 60000 mWatts (Maximum)
Power Consumption Mode 1 : 499260 mWatts
Power Consumption Mode 2 : 635950 mWatts
Power Consumption Mode 3 : 556720 mWatts
Chassis MAC Address : f86b.d978.8320
MAC Address block size : 16
```

```
Controller Type : 4396
Asset ID :
Router#

Router# show version
Cisco IOS XE Software, Version BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148
Cisco IOS Software [Bengaluru], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M),
Experimental Version 17.5.20210124:064309
[S2C-build-v175_throttle-507-/nobackup/mcpre/BLD-BLD_V175_THROTTLE_LATEST_20210124_063209
226]
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sun 24-Jan-21 06:10 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: 1.4(REL)
CABO_SIT_Cellular uptime is 1 hour, 37 minutes
Uptime for this control processor is 1 hour, 38 minutes
System returned to ROM by reload
System image file is
"bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148.SSA.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 Type Technology-package Technology-package
Current Next Reboot
------------------------------------------------------------------
Smart License Perpetual network-advantage network-advantage
Smart License Subscription None None
The current throughput level is 50000 kbps
Smart Licensing Status: Registration Not Applicable/Not Applicable
cisco IR8140H-P-K9 (1RU) processor with 1948753K/6147K bytes of memory.
Processor board ID FDO2441J91D
Router operating mode: Autonomous
2 Gigabit Ethernet interfaces
4 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8116912K bytes of physical memory.
8032254K bytes of Bootflash at bootflash:.
Configuration register is 0x2102
Router#

Router# show power
Main PSU :
Total Power Consumed: 22.92 Watts
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 : 15.4 Watts
Router#
```

# Additional references

This topic provides references to MIBs associated with the power efficiency management feature.

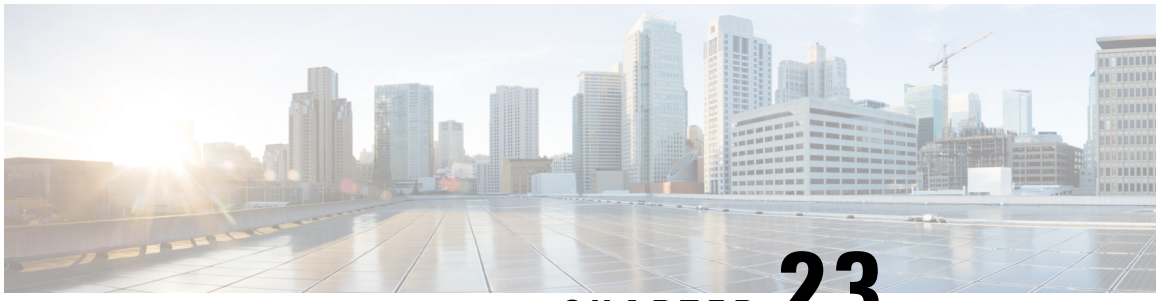
### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-ENTITY-FRU-CONTROL-MIB | 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 . |

## Technical assistance

This reference provides information on accessing the Cisco Support website for technical documentation, troubleshooting tools, and subscription services for product alerts.

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>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.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |



CHAPTER 23

# IOx application hosting

Provides an overview of the IOx application hosting architecture and its integration with network infrastructure.


- Application hosting, on page 189


# Application hosting

Application hosting is a software as a service solution that:

- enables hosted applications to run remotely using commands
- gives administrators a platform for leveraging their own tools and utilities, and
- provides software as a service capabilities for remote application execution.

## Application hosting

Application hosting is a network capability that enables third-party applications to run directly on network infrastructure devices.

### Application hosting

Application hosting is a platform capability that:

- enables administrators to leverage their own tools and utilities on network devices
- provides reusable, portable, and scalable applications for virtual environments, and
- supports third-party off-the-shelf applications built using Linux tool chains.

#### Application hosting capabilities

Applications hosted on network devices serve various purposes:

- Automation
- Configuration management monitoring
- Integration with existing tool chains

Cisco devices support custom applications cross-compiled with the software development kit that Cisco provides.

## IOx framework

IOx is a Cisco-developed end-to-end application framework that:

- provides application hosting capabilities for different application types on Cisco network platforms
- uses a different architecture for the IR8100 compared to other Cisco platforms that use the hypervisor approach, and
- runs as a process on the IR8100 rather than as a virtual machine like on other platforms.

## Cisco application hosting

Cisco application hosting is a virtualization service that:

- launches designated applications in containers
- checks available resources (memory, CPU, and storage), and allocates and manages them
- provides an application hosting infrastructure referred to as Cisco Application Framework (CAF), and
- helps in the setup of platform-specific networking (packet-path) via VirtualPortGroup and management interfaces.

### Application hosting services

Application hosting provides the following services:

- Provides support for console logging
- Provides access to services via REST APIs
- Provides a CLI endpoint

The IR8100 allows you to deploy applications using the application hosting CLI commands. You can also deploy applications using the Local Manager and Fog Director.

The container is referred to as the virtualization environment provided to run the guest application on the host operating system. The Cisco IOS-XE virtualization services provide manageability and networking models for running guest applications. The virtualization infrastructure allows the administrator to define a logical interface that specifies the connectivity between the host and the guest. IOx maps the logical interface into the Virtual Network Interface Card (vNIC) that the guest application uses.

Applications to be deployed in the containers are packaged as TAR files. The configuration that is specific to these applications is also packaged as part of the TAR file.

The management interface on the device connects the application hosting network to the IOS management interface. The Layer 3 interface of the application receives the Layer 2 bridged traffic from the IOS management interface. The management interface connects through the management bridge to the container/application interface. The IP address of the application must be on the same subnet as the management interface IP address.

## IOXMAN

IOXMAN is a process that:

- establishes a tracing infrastructure to provide logging or tracing services for guest applications, except Libvirt, that emulates serial devices
- operates based on the lifecycle of the guest application to enable and disable the tracing service
- sends logging data to IOS syslog, saves tracing data to IOx tracelog, and maintains IOx tracelog for each guest application.

# Application hosting on the IR8100 industrial integrated services router

Application hosting on the IR8100 industrial integrated services router is a network service capability that:

- requires applications to comply with ARM 64-bits architecture due to the non-x86 CPU design
- supports deployment through CLI commands, Local Manager WebUI, and Fog Director management platforms, and
- requires Virtual Port Group interface configuration before installing or activating IOx applications from Local Manager.

### Deployment methods and requirements



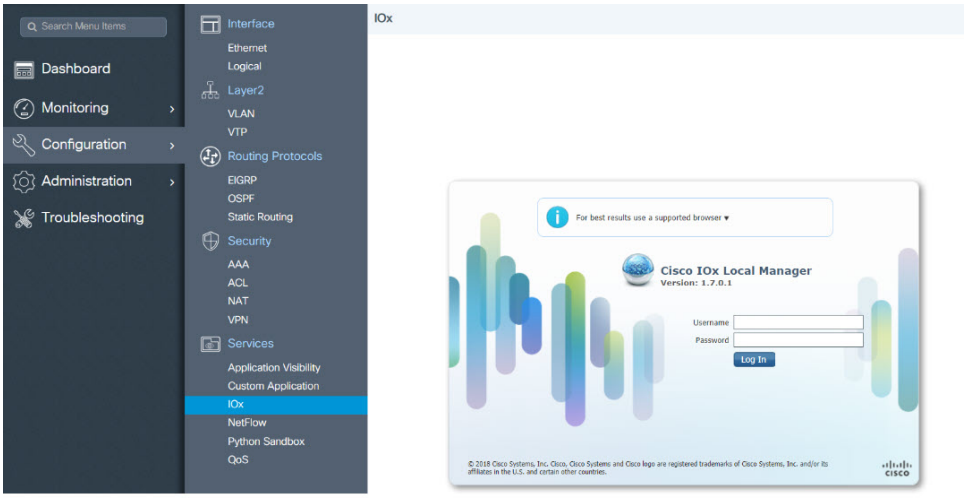
**Note**

- The IR8100 CPU is not based on x86 architecture like other routers. Therefore, this requires the application to comply with the ARM 64-bits architecture.
- Before installing or activating an IOx application from Local Manager, you need to configure the required Virtual Port Group interfaces.

Application hosting can be achieved using the application hosting CLI commands as well as using Local Manager and Fog Director. Application hosting using Local Manager is done through WebUI. To deploy the applications using Local Manager, enable WebUI and then log in to Local Manager.

Application Management is available using FND.

*Figure 3: Local Manager*




1. From WebUI, click on **Configuration > Services > IOx**

2. Log in using the username and password configured.

3. Follow the steps for the application lifecycle in the **Cisco IOx Local Manager Reference Guide** using this link: https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-7/b_iox_lm_ref_guide_1_7/b_iox_lm_ref_guide_1_7_chapter_011.html

The next section explains the deployment of an application using the application hosting CLI commands.

# VirtualPortGroup

A VirtualPortGroup is a software construct on Cisco IOS that:

- maps to a Linux bridge IP address
- represents the switch virtual interface (SVI) of the Linux container, and
- connects the application hosting network to the IOS routing domain.

### VirtualPortGroup configuration and connectivity

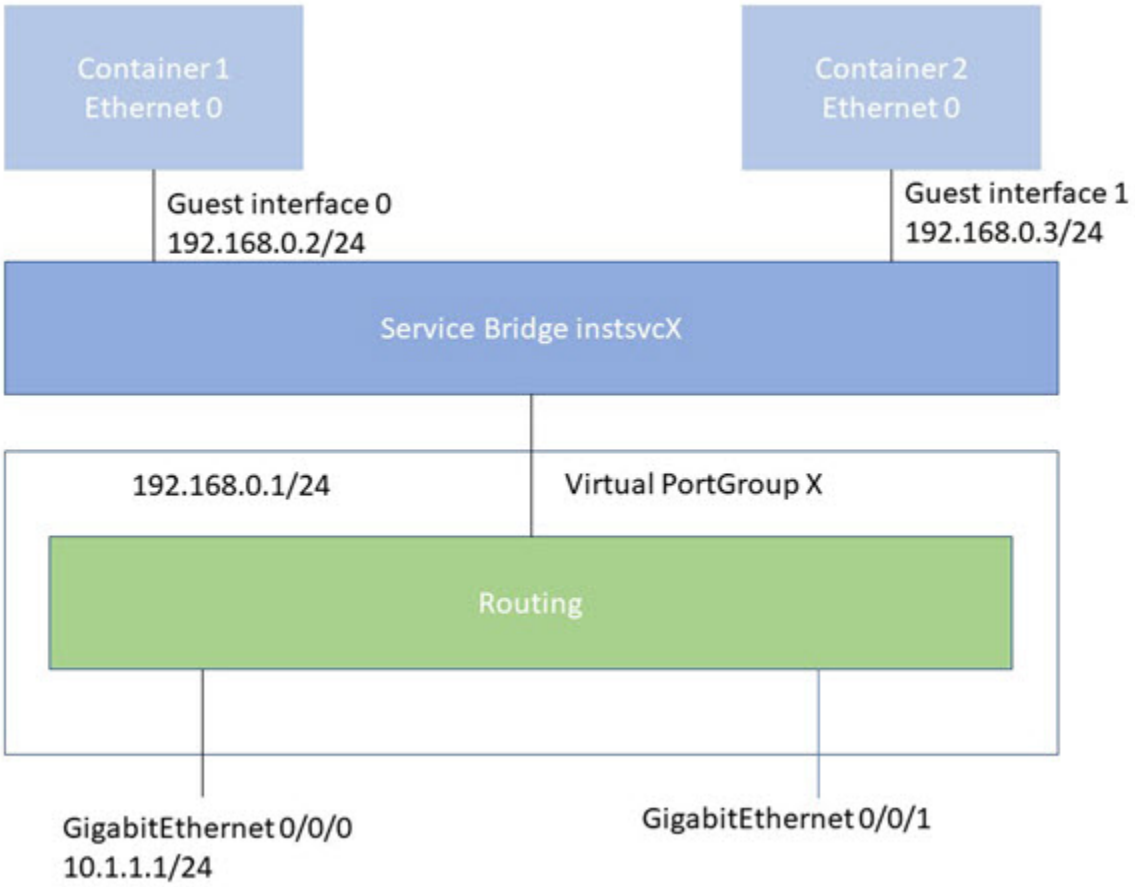
Each bridge can contain multiple interfaces; each mapping to a different container. Each container can also have multiple interfaces.

VirtualPortGroup interfaces are configured by using the interface virtualportgroup command. Once these interfaces are created, IP address and other resources are allocated.

The VirtualPortGroup interface connects the application hosting network to the IOS routing domain. The Layer 3 interface of the application receives routed traffic from IOS. The VirtualPortGroup interface connects through the SVC Bridge to the container/application interface.

The graphic helps to understand the relationship between the VirtualPortGroup and other interfaces, as it is different than the IR8x9 routers.

*Figure 4: Virtual Port Group Mapping*




# vNICs

A vNIC is a virtual network interface card that

- forms part of an application container in a virtual Ethernet pair configuration
- connects to the platform dataplane for sending and receiving packets, and
- operates as a standard Ethernet interface inside the container.

### vNIC architecture and management

For container life cycle management, the Layer 3 routing model supports one container per internal logical interface. This configuration creates a virtual Ethernet pair for each application, where one interface (vNIC) belongs to the application container and the other interface (vpgX) belongs to the host system.

IOx manages the following components for each vNIC:

- Gateway (VirtualPortGroup interface) assignment
- IP address allocation
- Unique MAC address assignment

# Configure application hosting

Application hosting configuration allows you to deploy, manage, and monitor applications within your network infrastructure.

## Enable IOx

The IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities.

Follow these steps to enable IOx.

### Procedure

**Step 1** Use the **enable** command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **iox** command to enable IOx.

**Example:**

```
Router(config)# iox
```

**Step 4** Use the **ip http server** command to enable the HTTP server on your IP or IPv6 system.

**Example:**

```
Router(config)# ip http server
```

**Note** In the steps that follow, the IP HTTP commands do not enable IOx, but they allow you to access the WebUI to connect to the IOx Local Manager.

**Step 5** Use the **ip http secure-server** command to enable a secure HTTP (HTTPS) server.

**Example:**

```
Router(config)# ip http secure-server
```

**Step 6** Use the **username** *name* **privilege** *level* **password** {**0** | **7** | *user-password*} *encrypted-password* command to establish a username-based authentication system and privilege level for the user.

**Example:**

```
Router(config)# username cisco privilege 15 password 0 cisco
```

**Note** The username privilege level must be configured as 15.

**Step 7** Use the **end** command to exit configuration mode and return to privileged EXEC mode.

**Example:**

```
Router(config)# end
```

## Configure a VirtualPortGroup to a Layer 3 data port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. VirtualPortGroups and Layer 3 data ports must be on different subnets.

Enable the `ip routing` command to allow external routing on the Layer 3 data port.

Follow these steps to configure a VirtualPortGroup to a Layer 3 data port.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use these steps for configuring the interface:

a) Use the **ip routing** command to enable IP routing.

**Example:**

```
Router(config)# ip routing
```

**Note** The `ip routing` command must be enabled to allow external routing on Layer 3 data ports.

b) Use the **interface** *type number* command to configure an interface and enter interface configuration mode.

**Example:**

```
Router(config)# interface gigabitethernet 0/0/0
```

c) Use the **no switchport** command to place the interface in Layer 3 mode so that it operates like a router interface rather than a switch port.

**Example:**

```
Router(config-if)# no switchport
```

d) Use the **ip address** *ip-address mask* command to configure an IP address for the interface.

**Example:**

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

e) Use the **exit** command to exit interface configuration mode and return to global configuration mode.

**Example:**

```
Router(config-if)# exit
```

**Step 3** Use these commands to configure the VirtualPortGroup interface:

a) Use the **interface** *type number* command to configure the VirtualPortGroup interface and enter interface configuration mode.

**Example:**

```
Router(config)# interface virtualportgroup 0
```

b) Use the **ip address** *ip-address mask* command to configure an IP address for the interface.

**Example:**

```
Router(config-if)# ip address 192.168.0.1 255.255.255.0
```

c) Use the **end** command to exit interface configuration mode and return to privileged EXEC mode.

**Example:**

```
Router(config-if)# end
```

**Step 4** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 5** Use the **app-hosting appid** *name* command to configure the application and enter application configuration mode.

**Example:**

```
Router(config)# app-hosting appid app1
```

**Step 6** Use the **app-vnic gateway0 virtualportgroup** *number* **guest-interface** *number* command to configure the application interface and the gateway of the application.

**Example:**

```
Router(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 0
```

**Step 7** Use the **guest-ipaddress** *ip-address* **netmask** *mask* command to configure the application Ethernet interface IP address.

**Example:**

```
Router(config-app-hosting-gateway0)# guest-ipaddress 192.168.0.2 netmask 255.255.255.0
```

**Step 8** Use the **app-default-gateway** *ip-address* **guest-interface** *number* command to configure the default gateway for the application.

**Example:**

```
Router(config-app-hosting-gateway0)# app-default-gateway 192.168.0.1 guest-interface 0
```

a)

**Step 9** Use the **end** command to exit application configuration mode and return to privileged EXEC mode.

**Example:**

```
Router(config-app-hosting-gateway0)# end
```

# Install and uninstall apps

Use this task to manage the complete lifecycle of applications on network devices, from installation through removal.

You can install apps from any local storage location, such as flash, bootflash, and usbflash0. The activation process validates all application resource requests before proceeding.

Follow these steps to install and uninstall apps.

### Procedure

**Step 1** Use the **enable** command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** Use the **app-hosting install appid** *application-name* **package** *package-path* command to install an app from the specified location.

**Example:**

```
Router# app-hosting install appid lxc_app package flash:my_iox_app.tar
```

**Note** You can install the app from any local storage location, such as flash, bootflash, and usbflash0.

**Step 3** Use the **app-hosting activate appid** *application-name* command to activate the application.

**Example:**

```
Router# app-hosting activate appid app1
```

**Note** This command validates all application resource requests. If all resources are available, the application is activated; if not, the activation fails.

**Step 4** Use the **app-hosting start appid** *application-name* command to start the application.

**Example:**

```
Router# app-hosting start appid app1
```

**Note** The application start-up scripts are activated.

**Step 5** Use the **app-hosting stop appid** *application-name* command to stop the application.

**Example:**

```
Router# app-hosting stop appid app1
```

**Step 6** Use the **app-hosting deactivate appid** *application-name* command to deactivate the application.

**Example:**

```
Router# app-hosting deactivate appid app1
```

**Note** This command deactivates all resources allocated for the application.

**Step 7** Use the **app-hosting uninstall appid** *application-name* command to uninstall the application.

**Example:**

```
Router# app-hosting uninstall appid app1
```

**Note** This command uninstalls all packaging and stored images. All changes and updates to the application are also removed.

# Override the app resource configuration

**Note** Resource changes take effect only after you configure the `app-hosting activate` command.

Follow these steps to override the app resource configuration.

**Procedure**

**Step 1** Use the **enable** command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **app-hosting appid** *name* command to enable application hosting and enter application hosting configuration mode.

**Example:**

```
Router(config)# app-hosting appid app1
```

**Step 4** Use the **app-resource profile** *name* command to configure the custom application resource profile and enter custom application resource profile configuration mode.

**Example:**

```
Router(config-app-hosting)# app-resource profile custom
```

**Note** Only the custom profile name is supported.

**Step 5** Use the **cpu** *unit* command to change the default CPU allocation for the application.

**Example:**

```
Router(config-app-resource-profile-custom)# cpu 800
```

**Note** Resource values are application-specific. Any adjustment to these values must ensure that the application can run reliably with the changes.

**Step 6** Use the **memory** *memory* command to change the default memory allocation.

**Example:**

```
Router(config-app-resource-profile-custom)# memory 512
```

**Step 7** Use the **vcpu** *number* command to change the virtual CPU (vCPU) allocation for the application.

**Example:**

```
Router(config-app-resource-profile-custom)# vcpu 2
```

**Step 8** Use the **end** command to exit custom application resource profile configuration mode and return to privileged EXEC mode.

**Example:**

```
Router(config-app-resource-profile-custom)# end
```

# Verify the application hosting configuration

Use this verification procedure to check the operational status of IOx services and application hosting on your device. This helps ensure that your application hosting environment is properly configured and running.

Follow these steps to verify the application hosting configuration.

**Procedure**

**Step 1** Use the **enable** command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** Use the **show iox-service** command to display the status of all IOx services.

**Example:**

```
Router# show iox-service
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)          : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage) : Running
Libvirtd 5.5.0             : Running
Dockerd 18.03.0            : Running
Router#
```

**Step 3** Use the **show app-hosting detail** command to display detailed information about the application.

**Example:**

```
Router# show app-hosting detail
App id                 : iperf
Owner                  : iox
State                  : RUNNING
Application
Type                 : lxc
Name                 : nt08-stress
Version              : 0.1
Description          : Stress Testing Application
Path                 : bootflash:sparrow_lxc.tar
URL Path             :
Activated profile name : custom

Resource reservation
Memory               : 64 MB
Disk                 : 2 MB
CPU                  : 500 units
CPU-percent          : 31 %
VCPU                 : 1

Attached devices
Type          Name               Alias
 ---------------------------------------------
serial/shell  iox_console_shell   serial0
serial/aux    iox_console_aux     serial1
serial/syslog iox_syslog          serial2
serial/trace  iox_trace           serial3

Network interfaces
---------------------------------------
eth0:
MAC address          : 52:54:dd:8e:55:19
IPv4 address         : 192.168.11.2
IPv6 address         : ::
Network name         : VPG1
```

**Step 4** Use the **show app-hosting list** command to display the list of applications and their status.

**Example:**

```
Router# show app-hosting list
App id                           State
---------------------------------------------------------
app1                             RUNNING
```

You have successfully verified the application hosting configuration. The IOx services status, detailed application information, and application list confirm the operational state of your application hosting environment.

# Configuration examples for application hosting

See the given examples:

## Example: Enable IOx

This example demonstrates the command sequence for enabling IOx functionality on a Cisco device, including the necessary HTTP server configuration and user authentication setup.

```
Device> enable
Device# configure terminal
Device(config)# iox
Device(config)# ip http server
Device(config)# ip http secure-server
Device(config)# username cisco privilege 15 password 0 cisco
Device(config)# end
```

## VirtualPortGroup configuration to a Layer 3 data port example

This example demonstrates the configuration steps for setting up a VirtualPortGroup interface with Layer 3 routing capabilities and connecting it to a data port.

```
Device> enable
Device# configure terminal
Device(config)# ip routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface virtualportgroup 0
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# end
```

## App installation and uninstallation commands

This reference shows the sequence of CLI commands used to manage IOx applications throughout their lifecycle on network devices, from initial installation through final removal.

```
Device> enable
Device# app-hosting install appid app1 package flash:my_iox_app.tar
Device# app-hosting activate appid app1
Device# app-hosting start appid app1
Device# app-hosting stop appid app1
Device# app-hosting deactivate appid app1
Device# app-hosting uninstall appid app1
```

## App resource configuration override example

This example demonstrates how to override the default app resource configuration by creating a custom profile with specific CPU, memory, and vCPU settings for an application.

```
Device# configure terminal
Device(config)# app-hosting appid app1
Device(config-app-hosting)# app-resource profile custom
Device(config-app-resource-profile-custom)# cpu 800
Device(config-app-resource-profile-custom)# memory 512
Device(config-app-resource-profile-custom)# vcpu 2
Device(config-app-resource-profile-custom)# end
```

# Native docker support

Native Docker Support is a capability that

- enables users to deploy docker applications on the IR1800
- follows a similar application lifecycle process to the procedure in the Installing and Uninstalling Apps section, and
- requires entry point configuration as part of the application configuration.

### Entry point configuration example

The example shows the entry point configuration for docker applications:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#app-hosting appid app3
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.7 netmask 255.255.255.0
Router(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0
Router(config-app-hosting)#app-resource docker
Router(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 10000'"
Router(config-app-hosting-docker)#end
Router#
```

The output for docker applications is shown in the example:

```
Router#show app-hosting detail
App id : app1
Owner : iox
State : RUNNING
Application
Type : docker
Name : aarch64/busybox
Version : latest
Description :
Path : bootflash:busybox.tar
Activated profile name : custom
Resource reservation
Memory : 431 MB
Disk : 10 MB
CPU : 577 units
VCPU : 1
Attached devices
Type Name Alias
---------------------------------------------
serial/shell iox_console_shell serial0
serial/aux iox_console_aux serial1
serial/syslog iox_syslog serial2
```

```
serial/trace iox_trace serial3
Network interfaces
---------------------------------------
eth0:
MAC address : 52:54:dd:e9:ab:7a
IPv4 address : 192.168.0.7
Network name : VPG0
Docker
------
Run-time information
Command :
Entry-point : /bin/sleep 10000
Run options in use : --entrypoint '/bin/sleep 10000'
Application health information
Status : 0
Last probe error :
Last probe output :
Router#
```

# Enable signed verification for Cisco signed applications

Cisco signed applications are supported on the IR1800. To install a signed application, you must enable signed verification on the device.

Follow these steps to enable signed verification for Cisco signed applications.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **app-hosting signed-verification** command to enable signed verification for applications.

**Example:**

```
Router(config)# app-hosting signed-verification
```

**Step 3** Use the **exit** command to exit configuration mode.

**Example:**

```
Router(config)# exit
```

### What to do next

After you enable signed verification, follow the instructions in the Installing and Uninstalling Apps section under IOx Application Hosting to install the application.

# Cisco Cyber Vision and Edge Intelligence

Cisco Cyber Vision and Edge Intelligence are integrated solutions that:

- provide real-time monitoring and visibility into Industrial Control Systems (ICS) and Industrial IoT networks
- enable simplified data extraction, transformation, governance and delivery from IoT sensors to applications, and
- integrate with IoT IOS-XE platforms beginning with release 17.4 through IOX sensor deployment.

### Cyber Vision Center integration details

Cisco Cyber Vision Center (CVC) gives more visibility into Industrial IoT networks across Industrial Control Systems (ICS) with real-time monitoring of control and data networks. On IoT IOS-XE platforms beginning with release 17.4, integration of CVC is supported by deploying IOX Cyber Vision sensor. With this sensor deployed on IoT Routers, the platform can forward the traffic from IOX applications to Cyber Vision Center for real-time monitoring and we can forward any captured PCAP files to Vision center from IOX application. The minimum Cybervision release is 3.1.1 to work with the IR8100. For more information about CVC, see Deployment of Cyber Vision Center (CVC) on IOS-XE platform and Release Notes for Cisco Cyber Vision Release 3.1.1.

Cisco Edge Intelligence allows for simplified data extraction from IoT sensors, transformation, governance and delivery to applications that need this data. The release for the IR8100 is version 1.0.6, and is called:

ei_1.0.6_ir1101.K9.tar

Complete information about Cisco Edge Intelligence is found at:

https://developer.cisco.com/edge-intelligence/.

# Cisco ThousandEyes Enterprise Agent

A Cisco ThousandEyes Enterprise Agent is a network monitoring solution that

- runs a variety of tests using agents
- provides real-time monitoring of network and application performance, and
- offers multidimensional insights with routing and device data for end-to-end visibility.

### Additional information

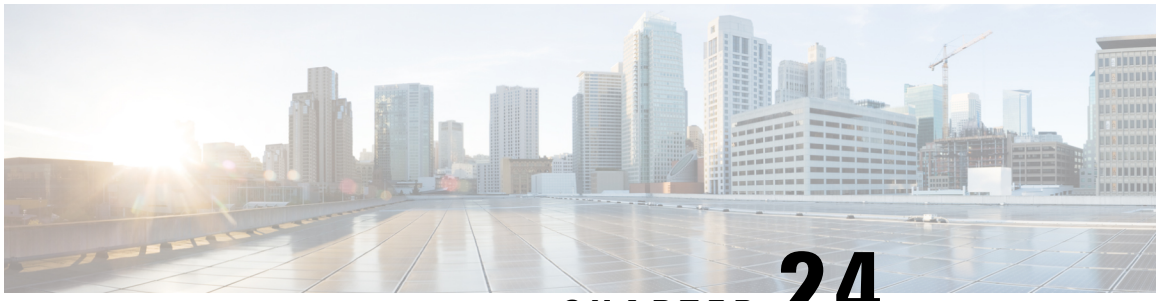
The Cisco ThousandEyes Enterprise Agent enables you to view end-to-end paths across networks and services affecting your business. It actively monitors network traffic paths across internal, external, and internet networks, helping analyze network performance and application availability.

You can use application-hosting features to deploy the Cisco ThousandEyes Enterprise Agent as a container application on Cisco Industrial IoT Routers. The agent runs as a Docker container using the Cisco IOx.

Starting with Cisco IOS XE Release 17.18.2, you can configure Cisco ThousandEyes Enterprise Agent in Controller mode.

For details about configuring Cisco ThousandEyes Enterprise Agent in controller mode, see Cisco SD-WAN Systems and Interfaces Configuration Guide.

For more information about Cisco ThousandEyes Enterprise Agent, see ThousandEyes Documentation.



CHAPTER 24

# Cisco SD-WAN support

This document outlines the supported features and operational requirements for Cisco SD-WAN integration.


- Cisco SD-WAN overview, on page 205
- Related documentation, on page 206

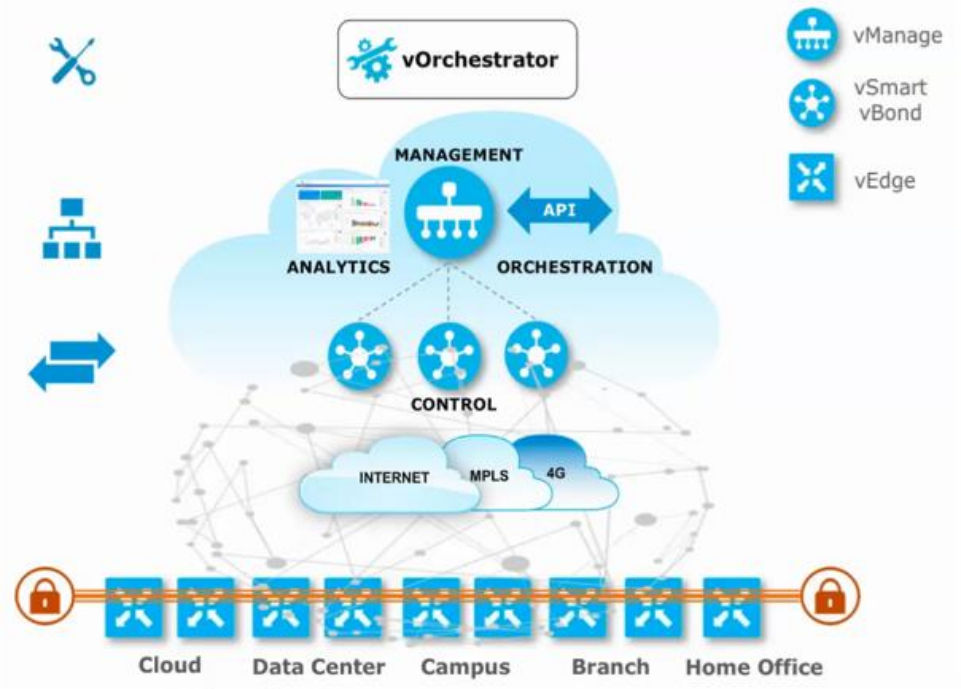

# Cisco SD-WAN overview

Provides an overview of the Cisco SD-WAN solution, which consists of vOrchestrator, vManage, vSmart, and vEdge components.

The following components perform specific roles within the SD-WAN solution:

- vOrchestrator: Responsible for launching all controller VMs in the cloud.
- vManage: Acts as the management plane for the overall SD-WAN solution and uses netconf/YANG to communicate with vEdge devices.
- vSmart: Serves as the control plane for the overall SD-WAN solution, acting as the route reflector, key reflector, and policy engine for vEdge devices.
- vEdge: Functions as the data plane of the SD-WAN solution, where the IR8100 platform communicates with vSmart and vManage as part of the network.

*Figure 5: High level architecture of SD-WAN*




# Related documentation

This topic identifies the primary online locations for accessing Cisco SD-WAN technical documentation and support materials.

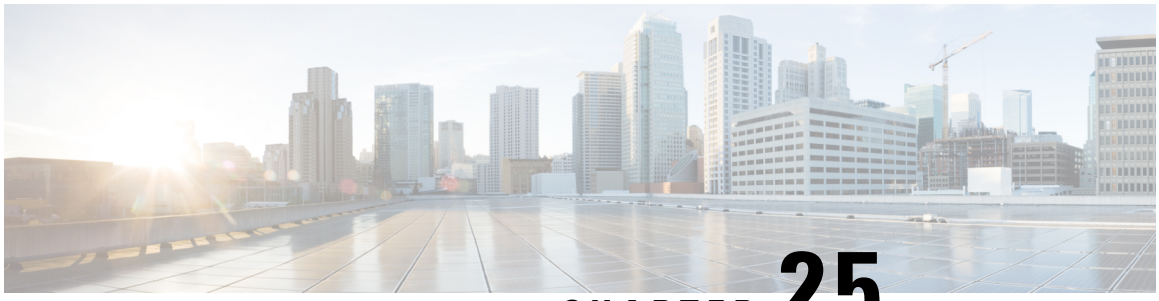
Cisco SDWAN documentation is available from the following sources:

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features

All of the technical documentation for Cisco SD-WAN can be found here:

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html



CHAPTER 25

# ROM Monitor overview

This reference describes the fundamental functions and operational context of the ROM Monitor.

• ROM Monitor overview and basic procedures, on page 207

# ROM Monitor overview and basic procedures

ROM Monitor is a bootstrap program that

- provides a recovery mechanism when the normal boot process fails
- enables basic system diagnostic and recovery functions, and
- allows manual system initialization and configuration.

## ROM Monitor

A 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
- displays the ROM Monitor (rommon 1>) prompt when you connect a terminal to the router in ROM Monitor mode, and
- operates as a separate program from the Cisco IOS XE software.

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*.

### ROM Monitor operational characteristics

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.

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.

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.

Environmental variables and configuration register provide the primary connections between ROM Monitor and Cisco IOS XE software:

- **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.
- **Configuration register**: 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.

Access and network management considerations apply when using ROM Monitor mode:

- **Terminal access**: 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.
- **Hardware availability**: The hardware is available, but no configuration exists to make use of the hardware. Basically, all Cisco IOS XE software resources are unavailable.
- **Management Ethernet interface configuration**: When the router is in ROM Monitor mode, 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.

**Note** TFTP access variables are currently not supported on the IR1800 platform.

# Access ROM Monitor mode

Access ROM Monitor mode is a boot process that allows network administrators to enter the device's low-level diagnostic and recovery environment when normal boot processes fail or when manual intervention is required.

### ROM Monitor mode access methods

These sections describe how to enter the ROMMON mode.

## Check the current ROMmon version

This task helps you identify the current ROMmon version and view all ROMmon variables configured on your router for troubleshooting and system verification purposes.

Follow these steps to check the current ROMmon version.

### Procedure

**Step 1** Use the **show rom-monitor** command to display the version of ROMmon running on the router.

**Example:**

```
Router# show rom-monitor r0
System Bootstrap, Version 1.4(DEV) [root-vganev 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2020 by cisco Systems, Inc.
Compiled at Mon Dec 7 18:02:07 2020 by root
```

**Step 2** Use the **show romvar** command to display all variables that are set in ROMmon.

**Example:**

```
Router# show romvar
ROMMON variables:
PS1 = rommon ! >
THRPUT =
LICENSE_BOOT_LEVEL = network-advantage,all:IR8100;
RET_2_RTS =
BOOT =
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148.SSA.bin,12;
CONSOLE_LOCK = 0
BSI = 0
RET_2_RCALTS =
RANDOM_NUM = 307121635
```

**Step 3** Use the **reload** command to reload the router and access ROMmon mode if your configuration register is set to the hex value 0x0 or 0x1820.

**Example:**

```
Router# reload
```

**Note** If your configuration register is set to the hex value 0x0 or 0x1820, the reload operation brings you to the ROMmon mode command prompt (rommon 1>).

**Step 4** Use the **set** command to display the same information as the **show romvar** command displays in Cisco IOS XE EXEC mode at the ROMmon prompt, .

**Example:**

```
rommon 1 > set
PS1=rommon ! >
THRPUT=
LICENSE_BOOT_LEVEL=network-advantage,all:IR8100;
RET_2_RTS=
BOOT=bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148.SSA.bin,12;
CONSOLE_LOCK=0
BSI=0
RANDOM_NUM=307121635
RET_2_RCALTS=1611876425
```

## 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 39: 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. |

## 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
```

## Change the ROM Monitor prompt

Changing the prompt is useful if you are working with multiple routers in ROM Monitor at the same time.

Follow these steps to change the ROM Monitor prompt:

**Procedure**

Use the **PS1=** command to change the prompt.

**Example:**

```
rommon 8 > PS1="IR1800 rommon ! > "
IR1800 rommon 9 >
```

This example specifies that the prompt should be "IR1800 rommon ", followed by the line number, and then followed by " > " by the line number.

# Display the configuration register setting

The configuration register setting determines various system behaviors, including boot options and console settings. You can display this information using ROM Monitor commands.

Follow these steps to display the configuration register setting.

**Procedure**

**Step 1** Use the **confreg** command without parameters to display the current configuration register setting.

**Example:**

```
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]:
```

**Note**

- The configuration register setting is labeled **Virtual Configuration Register**.
- The system displays the current configuration register settings and prompts whether you want to change the configuration.

**Step 2** Enter **no** to avoid changing the configuration register setting.

# Environment variable settings

Environment variable settings are ROM Monitor configuration parameters that:

- define the attributes of the ROM Monitor

- are entered like commands and are always followed by the equal sign (=), and
- are entered in capital letters, followed by a definition.

### Environment variable configuration details

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.

Environment variable settings are entered using the following format:

```
IP_ADDRESS=10.0.0.2
```

## 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 IR1800 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 40: 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. |

## Display environment variable settings

### Procedure

Enter the **showmon** command.

**Example:**

```
rommon 1 > showmon
System Bootstrap, Version 1.4(DEV) [root-vganev 100], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2020 by cisco Systems, Inc.
Compiled at Mon Dec 7 18:02:07 2020 by root

IR8140H-P-K9 platform with CPU platform IRMH-SUP-SP and 8388608 Kbytes of main memory

MCU Version - Bootloader : 0x22, App : 0x38
MCU is in Application mode.
```

The system displays the current environment variable settings including system bootstrap information, platform details, and MCU version information.

## 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 = IR8100-K9_image_name
```

## Save environment variable settings

Environment variable values that are not saved with the `sync` command are discarded whenever the system is reset or booted.

Follow these steps to save the environment variable settings.

**Procedure**

Use the **sync** command to save the current environment variable settings.

**Example:**

```
rommon > sync
```

# Exit ROM Monitor mode

To exit ROM Monitor mode, you must change the configuration register and reset the router.

Follow these steps to exit ROM Monitor mode.

**Procedure**

**Step 1** Use the **confreg** command to initiate the configuration register configuration prompts.

**Example:**

```
rommon 1> confreg
```

**Note** Respond to each prompt as instructed. For more information, see the example that follows this procedure.

**Step 2** Use the **reset** command to reset and initialize the router.

**Example:**

```
rommon 2> reset
```

## Configuration example

This example demonstrates the configuration register setup process through ROM Monitor interface, showing the interactive prompts and default settings available during system configuration.

```
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]:
```

## Upgrade the ROMmon for a router

The ROMmon upgrade on the IR1800-K9 router is done automatically when the image is booted. The latest version of the ROMmon is bundled with the Cisco IOS XE image. An algorithm detects whether 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 so that the new version is loaded and executed.

Follow these steps to upgrade the ROMmon for a router.

### Procedure

**Step 1** (Optional) Use the **show rom-monitor slot** command on the router to display the current release numbers of the ROMmon on the hardware.



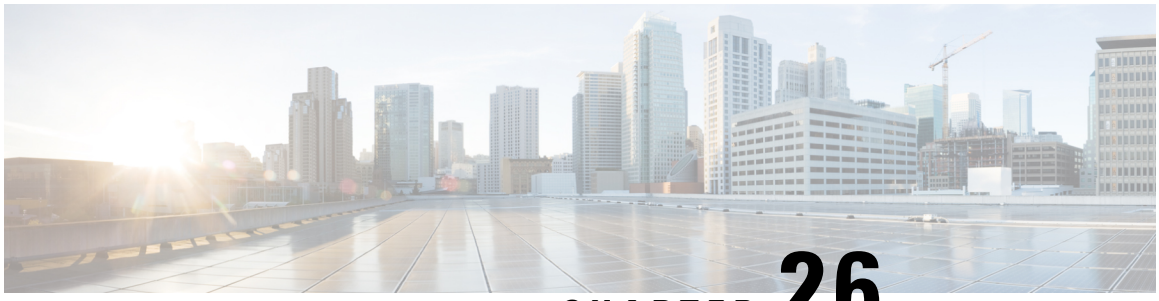
**Note** For information about interpreting the output of this command, see the relevant command reference.

**Step 2** If autoboot is not enabled using the **config-register 0x2102** command, use 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.

**Note** The ROMmon upgrade is not permanent for any piece of hardware until the Cisco IOS XE image is booted.

**Step 3** Use the **enable** command at the user prompt to enter privileged EXEC mode after the boot is complete.

**Step 4** Use the **show rom-monitor slot** command to verify whether the ROMmon has been upgraded.



CHAPTER 26

# WAN Monitoring

This reference outlines the monitoring features and diagnostic tools used to track WAN performance and status.


- WANMon, on page 217
- Prerequisites, on page 218
- Guidelines and limitations, on page 219
- Configure WANMon, on page 219
- Verify WANMon configuration, on page 221
- Configuration examples, on page 221


## WANMon

WANMon is a flexible solution that:

- addresses WAN link recovery requirements for physical networks and virtual links
- monitors WAN links for failure detection, and
- initiates link recovery actions on receipt of link failure triggers.

### Supported products and interfaces

WANMon supports the following networks and interfaces:

- Physical networks: 4G LTE and Ethernet (WAN port)
- Virtual links: Non-crypto map based IPSec tunnels (either legacy or FlexVPN); that is, any IPSec tunnel you configure as an interface.

## Built-in recovery actions

The following are the three levels of built-in recovery processes specific to the link type:

| Link Type | Recovery Actions | | |
|---|---|---|---|
| | Level 0 (Immediate) | Level 1 (Active) | Level 2 (Last-Resort) |
| 4G LTE | Clear interface, and then shut/no-shut | Module reload | System reload |
| Ethernet | Clear interface, and then shut/no-shut | No action taken | System reload |
| Tunnel | Shut/no-shut | No action taken | System reload |

Each level has two time-based thresholds based on which built-in recovery actions are taken. The following are the default settings for each level:

- *threshold* is the wait time in minutes after receipt of a link failure trigger to initiate the recovery action as set in the specified level.
- *mintime* is the frequency to perform the recovery action if the link remains down.

The built-in values are:

| Level | threshold | mintime | Description |
|---|---|---|---|
| Level 0 | 10 min | 10 min | Triggers Level 0 actions 10 minutes after the link went down. Repeat no more than every 10 minutes. |
| Level 1 | 60 min | 60 min | Triggers Level 1 actions 10 minutes after the link went down. Repeat no more than every 60 minutes. |
| Level 2 | 480 min | 60 min | Triggers Level 2 actions 480 minutes after the link went down. Repeat no more than every 60 minutes. |



**Note** If threshold values are specified as 0, no recovery actions are taken for that level. You can use this to avoid system reload (the built-in Level 2 recovery action) on receipt of a link failure trigger where other WAN links may be operational.

# Prerequisites

Provides the requirements for the WANMon module, specifically the inclusion of the **tm_wanmon.tcl** policy file in the IOS-XE image.

Ensure that the WANMon module is available. The WANMon module is included in the IOS-XE image as the **tm_wanmon.tcl** policy file.

# Guidelines and limitations

This section outlines the functional behavior of WANMon regarding IP address checking and event triggering, along with necessary precautions for live network environments.

These guidelines apply to WANMon operations:

- WANMon automatically performs IP address checking (no user configuration) as required for cellular interfaces.
- For all other interfaces, WANMon never performs IP address checking.
- WANMon indirectly triggers user-specified actions by generating an application event that link resetter applets monitor.
- If your network is live, ensure that you understand the potential impact of any command.

# Configure WANMon

You can enable WANMon on the router and assign WANMon support to specific interfaces. Optionally, you can override the built-in recovery actions, define custom recovery links, and define an event manager environment policy to set the track object value and disable IP address checking.



**Note** WANMon is disabled by default.

Follow these steps to configure WANMon.

**Procedure**

**Step 1** Use the **event manager policy tm_wanmon.tcl authorization bypass** command to enable the WANMon link recovery module.

**Example:**

```
Router(config)# event manager policy tm_wanmon.tcl authorization bypass
```



**Note** Use the `authorization bypass` keywords to avoid authorization for CLIs invoked by this policy.

**Step 2** Use the **event manager environment wanmon_if_list** *instance* {*interface-name* {**ipsla** *instance*}} command to configure WANMon for the interfaces in your WAN.

**Example:**

```
Router(config)# event manager environment wanmon_if_list1 {cellular0/4/0 {ipsla 1}}
Router(config)# event manager environment wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}
```

**Note**

- Any environment variable with the prefix `wanmon_if_list` constitutes an interface configuration.
- Multiple interfaces are allowed by specifying an instance.
- Be sure to specify the full interface name (for example, `cellular0/4/0` or `cellular0/5/0`).
- You can set the IP SLA `icmp-echo` trigger, if desired. Multiple IP SLA triggers are allowed by specifying an instance.
- WANMon only looks at the status of the SLA ID. Although `icmp-echo` is most common, you can use any other type of SLA probe (for example, `udp-echo`) instead, if needed.

**Step 3** (Optional) Use the **event manager environment wanmon_if_list***x* {*interface-name* {**recovery** *Level0* {*Level1*} *Level2*}} command to override the built-in thresholds.

**Step 4** (Optional) Use the **publish-event sub-system 798 type 2000 arg1** *interface-name* **arg2** *level* command to configure custom recovery actions using link resetter applets.

**Note**

- *interface-name* is the full interface name (for example, `cellular0/4/0` or `cellular0/5/0`).
- *level* is 0, 1, or 2 to match the desired link recovery action.

**Step 5** (Optional) Use the {**stub** *track-stub-id*} keyword to allow an event manager environment policy to set the track object value.

**Note** WANMon can set a track-stub-object value to reflect the link state so that an external applet can track the stub object.

**Step 6** (Optional) Use the **event manager environment wanmon_if_list***x* {*interface-name* {**checkip** *instance*}} command to disable IP address checking.

The following example enables the WANMon link recovery module:

```
Router(config)# event manager policy tm_wanmon.tcl authorization bypass
```

The following examples configure cellular and Ethernet interfaces:

```
Router(config)# event manager environment wanmon_if_list1 {cellular0/4/0 {ipsla 1}}
Router(config)# event manager environment wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}
```

The following example sets custom recovery thresholds:

```
Router(config)# event manager environment wanmon_if_list {cellular0/4/0 {recovery 20 {90
75} 600}
```

In this example:

- The Level 0 threshold is set to 20 minutes after the link failure trigger. Level 0 recovery actions are performed for the cellular interface and repeat indefinitely, no more than every 10 minutes (default).
- The Level 1 threshold is set to 90 minutes. Level 1 recovery actions are performed for the cellular interface and repeat no more frequently than every 75 minutes.
- The Level 2 threshold is set to 600 minutes (10 hours).

The following example sets the track-stub-object value to 21:

```
Router# configure terminal
Router(config)# track 21 stub-object
Router(config)# event manager environment wanmon_if_list {cellular0/4/0 {ipsla 1} {stub 21}
```

# Verify WANMon configuration

Follow these steps to verify your WANMon configuration.

**Procedure**

**Step 1** Use the **show event manager policy registered** command to display the WAN monitoring policy.

**Example:**

```
Router# show event manager policy registered
1    script    system  multiple   Off   Thu Jan 16 18:44:29 2014  tm_wanmon.tcl
```

**Step 2** Use the **show event manager environment** command to display the interface environment variables set during interface configuration.

**Example:**

```
Router# show event manager environment
1 wanmon_if_list   {cell0/4/0 {ipsla 1}}
```

# Configuration examples

The following examples are provided:

## WANMon cellular interface configuration example

This configuration example demonstrates the setup of WANMon for a cellular interface, including IP SLA tracking, ICMP echo configuration, and event manager policy settings.

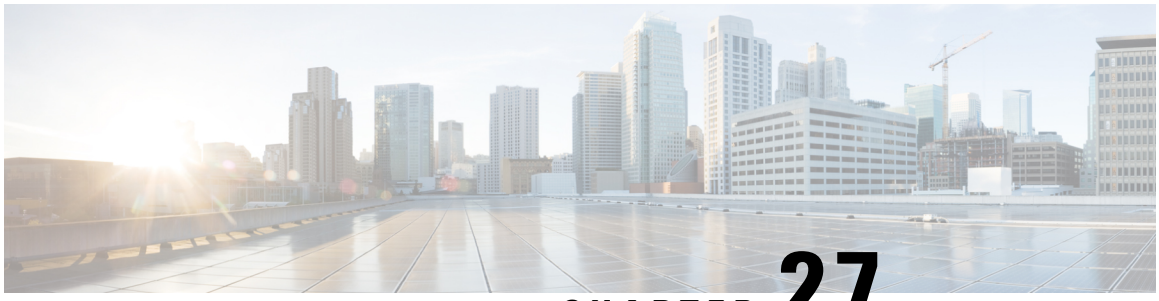
```
track 1 ip sla 1
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
```

```
 frequency 300
ip sla schedule 1 life forever start-time now
event manager environment wanmon_if_list {cellular0/4/0 {ipsla 1}}
event manager policy tm_wanmon.tcl authorization bypass
```

# Multiple WAN link monitoring example

This example demonstrates how to configure multiple WAN link monitoring using IP SLA operations with track objects and event manager policies. The configuration includes ICMP echo operations for two different target addresses with associated tracking objects and stub objects for failover scenarios.

```
track 1 ip sla 1
track 21 stub-object
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now
track 2 ip sla 2
track 22 stub-object
ip sla 2
 icmp-echo 10.27.16.25
 timeout 6000
 frequency 300
ip sla schedule 2 life forever start-time now
event manager environment wanmon_if_list1 {cellular0/4/0 {ipsla 1} {stub 21}}
event manager policy tm_wanmon.tcl authorization bypass
```



CHAPTER 27

# Yang data models

This document outlines the structure and application of Yang data models within the system environment.

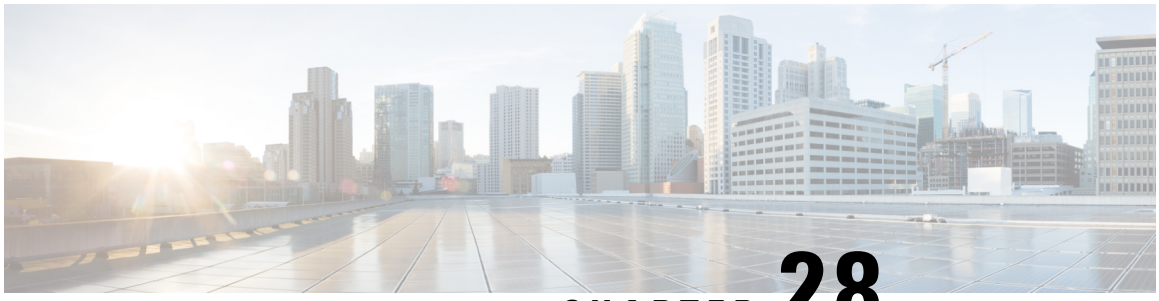

- Support for YANG data models, on page 223


# Support for YANG data models

Provides access to the supported YANG data models for the IR1840H, maintaining parity with previous Cisco IOS XE software releases.

The YANG models supported are similar to the earlier releases of Cisco IOS XE, and the same is supported for the release of IOS XE on the IR1840H. The following references are available for earlier YANG models:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe



CHAPTER 28

# Process health monitors

This chapter describes how to manage and monitor the health of various components of your router.


- Control plane resources, on page 225
- Monitoring hardware using alarms, on page 229


# Control plane resources

Control plane resources refer to the memory and CPU components that are monitored to ensure optimal operation of the Cisco IOS process and the overall control plane.

- Includes monitoring of both memory and CPU usage.
- Focuses on the Cisco IOS process and the overall control plane.
- Helps in identifying and preventing potential resource-related issues.

### Details of memory and CPU monitoring for control plane resources

These sections provide more information about monitoring memory and CPU resources in the control plane:


- System process monitors, on page 225
- View Cisco IOS process resource
- Overall Control Plane resources, on page 227


## System process monitors

Regular monitoring is a proactive approach that ensures system processes and resources are functioning correctly by providing status notifications and enabling timely intervention.

- Processes provide monitoring and notification of their status or health.
- Syslog error messages are displayed when a process fails, is stuck, or crashes.
- Automatic actions include restarting the process or rebooting the router if necessary.

### System resources and process health

Monitoring system resources enables early detection of potential problems, helps avoid outages, and establishes a baseline for normal system load.

Consider an scenario where after upgrading hardware or software, you can compare current resource usage with the established baseline to determine if the upgrade has affected system performance. This explains how the system resources monitoring helps maintain the process health.

# View Cisco IOS process resource

You can use the **show memory** and **show process cpu** commands to view CPU and memory utilization statistics for active processes in Cisco IOS. 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.

### Procedure

**Step 1** Use the Enter the **show memory** command in privileged EXEC mode to display memory usage for the Cisco IOS process.

**Example:**

```
Router# show memory
Tracekey : 1#b93c0f1c0d5d16ddc3ab8e54342a8dd5
Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  7F5F358048   1997625144   290200588   1707424556   487419128   1509949348
reserve P  7F5F3580A0      102404          92      102312      102312      102312
lsmpi_io  7F5D9901A8     6295128     6294304         824         824         412
Dynamic heap limit(MB) 1440      Use(MB) 0
Processor memory
Address      Bytes      Prev       Next    Ref   PrevF     NextF          what
   Alloc PC
7F5F358048 0000102408 00000000 7F5F3710A8 001  -------- -------- *Init*
:555F22A000+5E5691C
7F5F3710A8 0000000056 7F5F358048 7F5F371138 001  -------- -------- *Init*
:555F22A000+5E56938
7F5F371138 0000008224 7F5F3710A8 7F5F3731B0 001  -------- -------- *Init*
:555F22A000+5E56958
 ...
7F5F594D38 0000020008 7F5F5942B8 7F5F599BB8 001  -------- -------- Peer uid cb chu
:555F22A000+ACBBE98
```

The output displays memory usage statistics for the Cisco IOS process, including total, used, and free memory, as well as detailed memory allocation information.

**Step 2** Use the **show process cpu** command to display CPU utilization for the Cisco IOS process.

**Example:**

```
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
1           8          31        258  0.00%  0.00%  0.00%   0 Chunk Manager
2           8       10141          0  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
...
45          0           1          0  0.00%  0.00%  0.00%   0 IPC Seat Manager
```

This command displays CPU utilization averages for five seconds, one minute, and five minutes, as well as per-process statistics for the Cisco IOS process.

**Step 3** Use the **show process cpu platform sorted** command to view platform-level CPU utilization.

**Example:**

```
show process cpu platform sorted
CPU utilization for five seconds:  9%, one minute: 10%, five minutes: 10%
Core 0: CPU utilization for five seconds:  3%, one minute:  4%, five minutes:  4%
Core 1: CPU utilization for five seconds:  4%, one minute:  4%, five minutes:  4%
Core 2: CPU utilization for five seconds:  2%, one minute:  2%, five minutes:  2%
Core 3: CPU utilization for five seconds: 38%, one minute: 38%, five minutes: 38%
Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
-----------------------------------------------------------------------------
18700   18679     44%     44%     44%  S           235192  qfp-ucode-avent
5226    5216      2%      3%      3%  S           697124  linux_iosd-imag
24238   24231      1%      1%      1%  S             8288  ngiolite
...
13884   13874      0%      0%      0%  S             2816  flash_check.sh
```

This command provides CPU utilization statistics for each core and process on the platform, allowing you to identify resource usage beyond the Cisco IOS process.

# Overall Control Plane resources

Provides visibility into control plane resource utilization using the **show platform software status control-processor brief** and **how platform software status control-processors** commands.

Identifies the status values for control processors:

- Healthy: The processor is operating within normal parameters.
- Warning: The router is operational, but the operating level requires review.
- Critical: The router is nearing failure.

Outlines recommended actions when a Warning or Critical status is observed:

- Reduce static and dynamic loads on the system by limiting configuration elements or dynamic service capacity.
- Reduce the number of routes, adjacencies, and ACL rules.

### 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 indicates the percentage of time the CPU is busy, 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

```
Router# show platform software status control-processor
RP0: online, statistics updated 10 seconds ago
Load Average: healthy
1-Min: 1.28, status: healthy, under 5.00
5-Min: 0.74, status: healthy, under 5.00
15-Min: 0.78, status: healthy, under 5.00
Memory (kb): healthy
Total: 8154204
Used: 2282364 (28%), status: healthy
Free: 5871840 (72%)
Committed: 2025108 (25%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User:  2.46, System:  5.53, Nice:  0.00, Idle: 90.87
IRQ:  0.82, SIRQ:  0.20, IOwait:  0.10
CPU1: CPU Utilization (percentage of time spent)
User:  2.24, System:  5.91, Nice:  0.00, Idle: 90.91
IRQ:  0.71, SIRQ:  0.20, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
User:  0.50, System:  1.82, Nice:  0.00, Idle: 97.16
IRQ:  0.50, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
User: 13.03, System: 12.88, Nice:  0.00, Idle: 62.51IRQ: 11.55, SIRQ:  0.00, IOwait:  0.00
```

```
Router# show platform software status control-processor brief
Load Average
Slot  Status  1-Min  5-Min 15-Min
RP0 Healthy   0.99   0.72   0.77
Memory (kB)
Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
RP0 Healthy  8154204  2281012 (28%)  5873192 (72%)   2032232 (25%)
CPU Utilization
Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
RP0    0   1.02   1.84   0.00  96.30   0.61   0.10   0.10
1   0.72   1.85   0.00  96.60   0.61   0.20   0.00
2   0.50   1.62   0.00  97.25   0.60   0.00   0.00
3  11.78  14.28   0.00  62.44  11.34   0.14   0.00
```

```
Boot Flash Disk Monitoring
Aug 24 07:48:31.088 GMT: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota
exceeded
[free space is 83820 kB] - Please clean up files on flash1.
```

# Monitoring hardware using alarms

This reference provides information on monitoring hardware components using system alarms.

## 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

Ensures the bootflash disk maintains enough free space to store two core dumps.

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

Provides an overview of the monitoring strategies used to identify and respond to hardware-related alerts.

### Viewing the console or syslog for alarm messages

The network administrator monitors alarm messages by reviewing messages sent to the system console or to a system message log (syslog).

#### Enabling the logging alarm command

The **logging alarm** command allows the system to transmit alarm messages to configured logging destinations.

The **logging alarm** command is not enabled by default. You can specify the severity level of the alarms to be logged, where all alarms at and above the specified threshold generate alarm messages.

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

```
Router(config)# logging alarm critical
```

### Network management system alerts a network administrator when an alarm is reported through SNMP

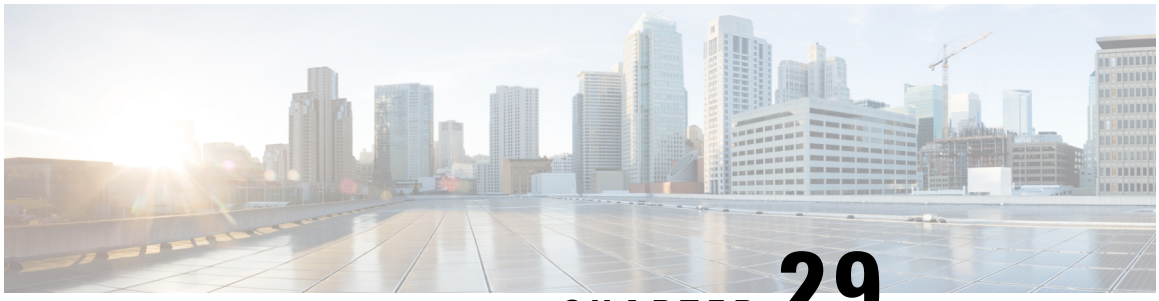
SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

- Provides notification of faults, alarms, and conditions that might affect services.
- Allows a network administrator to access router information through a network management system (NMS).
- Eliminates the need for manual log reviews, device polling, or log report analysis.

### SNMP alarm notification MIB requirements

To use SNMP to get alarm notification, use these 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 29

# Unified Threat Defence

This reference provides the necessary information to configure and manage Unified Threat Defence features within the network security architecture.


- Unified threat defense, on page 231
- Unified threat defense restrictions, on page 232
- License requirements for UTD features, on page 232
- References for unified threat defense configuration on IR8140, on page 232


## Unified threat defense

Unified Threat Defense (UTD) is Cisco's premier network security solution which provides a comprehensive suite of security features, such as:

- Enterprise Firewall
- Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
- Advanced Malware Protection
- URL Filtering, and
- DNS Security

***Table 41: Feature History Table***

| Feature name | Release information | Feature description |
|---|---|---|
| Unified Threat Defense | Release 26.1.1 | For enhanced protection across network, you can leverage Unified Threat Defense (UTD) which is Cisco's premier network security solution, to access a comprehensive suite of security features including:<br>• Enterprise Firewall, IPS/IDS<br>• Advanced Malware Protection<br>• URL Filtering, and DNS Security |

# Unified threat defense restrictions

These product-specific restrictions apply.

- UTD container requires a minimum space of 1.8 GB.
- UTD is supported in both autonomous mode and controller mode, but in autonomous mode, only IPS/IDS features are supported.
- The UTD configuration supports the Cloud-Low profile only.
- On-Box Web-Filtering database is not supported.
- TLS decryption is not supported.

# License requirements for UTD features

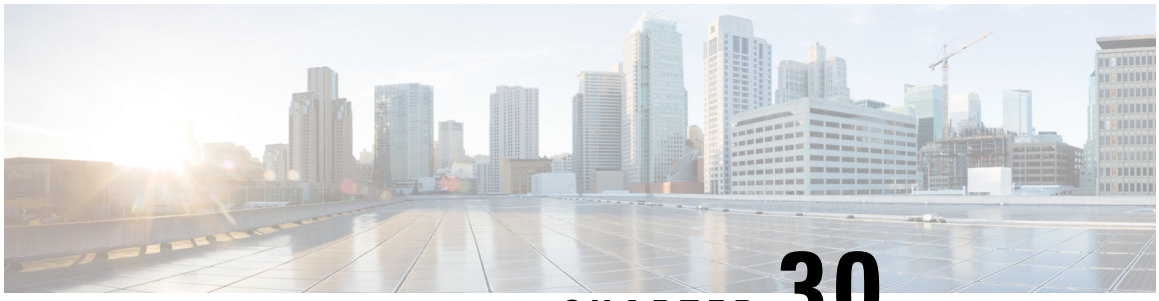
To enable UTD features, these licensing requirements apply:

- To enable UTD features in SD-Router (autonomous mode), you must have both a DNA Essentials license and a Network Essentials license.
- To use Cisco Secure Malware Analytics, you must have both a DNA Advantage license and a Network Advantage license.

# References for unified threat defense configuration on IR8140

Configuration on the IR8140 is the same as on other products. For configuration information refer to:

- Unified Threat Defense Resource Profiles
- Intrusion Prevention System
- URL Filtering
- Advanced Malware Protection



CHAPTER 30

# Cisco Network Plug and Play Agent

This chapter contains the following sections:


- Prerequisites for Cisco Network Plug and Play Agent, on page 233
- Restrictions for Cisco Network Plug and Play Agent, on page 234
- Information About Cisco Network Plug and Play Agent, on page 234
- Security Methods for the PnP Discovery Process, on page 249
- Security Methods for Post-PnP Discovery Process, on page 255
- How to Configure Cisco Network Plug and Play Agent, on page 258
- Troubleshooting and Debugging, on page 269
- Glossary, on page 270
- Additional References for Open Plug-n-Play Agent, on page 270


## Prerequisites for Cisco Network Plug and Play Agent

- Cisco Network Plug and Play (PnP) deployment method depends on the type of discovery process as required by the customer.
- Deploy the discovery mechanism, either a DHCP server discovery process or a Domain Name Server (DNS) discovery process, before launching the PnP.
- Configure the DHCP server or the DNS server before deploying the PnP.
- Ensure that the PnP server talks to the PnP agent.
- Ensue that the Cisco Network PnP Agent has connectivity with the PnP Server. The Cisco Network PnP Agent should be able to PING server.
- The PnP agent enforces the PnP server to send user credentials for every request. Cisco recommends the usage of HTTP secure (HTTPS) protocol.

**Note**

- The terms Cisco Network Plug and Play, PnP are interchangeably used in this guide and all mean the same.
- The terms PnP agent, agent, and deployment agent are interchangeably used in this guide and all mean the same.
- The terms PnP server, server, and deployment server are interchangeably used in this guide and all mean the same.

# Restrictions for Cisco Network Plug and Play Agent

- Cisco Network Plug and Play (PnP) agent facilitates HTTP and HTTP secure (HTTPS) transport based communication with the server.
- HTTPS cannot be used on platforms where crypto-enabled images are not supported (also, do not use Secure Sockets Layer [SSL] or Transport Layer Security [TLS] protocols if crypto-enabled images are used).
- Non-VLAN 1 configuration-Cisco Network Plug and Play supports devices using VLAN 1 by default. To use a VLAN other than 1, adjacent upstream devices must use supported releases and configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp startup-vlan x**. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, all the active interfaces on the upcoming Plug and Play device are changed to the specified VLAN. This guideline applies to both routers and switches.
- PnP is only supported on GigabitEthernet 0/0/0 and GigabitEthernet 0/0/1 port and Cellular PIMs.

**Note** When performing a firmware upgrade during the PNP process, it is best to remove any old images on the router to prevent an incorrect image from loading.

Further details are available by viewing CSCwd68868.

# Information About Cisco Network Plug and Play Agent

## Cisco Network Plug and Play Deployment Solution

The Cisco Network PnP Agent is a part of Cisco Network Plug and Play solution. The Cisco initiated Network Plug and Play (PnP) deployment solution supports the concept of redirection and includes a PnP agent, a PnP server, and other components. Simplified deployment process of any Cisco device automates the following deployment related operational tasks:

- Establishing initial network connectivity for the device

- Delivering device configuration
- Delivering software and firmware images
- Delivering licenses
- Delivering deployment script files
- Provisioning local credentials
- Notifying other management systems about deployment related events

Simplified deployment reduces the cost and complexity and increases the speed and security of deployments.

Cisco Network Plug and Play (PnP) agent is a software application that is running on a Cisco IOS or IOS-XE device. The PnP agent together with the PnP deployment server provides effortless deployment services. When a device is powered on for the first time, the PnP agent process wakes up in the absence of the startup config, user input on the device's console, and attempts to discover the address of the PnP server. The PnP agent uses methods like DHCP, Domain Name System (DNS), and others to acquire the desired IP address of the PnP server. When the PnP agent successfully acquires the IP address, it initiates a long lived, bidirectional layer 3 connection with the server and waits for a message from the server. The PnP server application sends messages to the agent requesting for information and services to be performed on the device.

The PnP agent converges existing solutions into a unified agent and adds functionality to enhance the current solutions. The main objectives of PnP agent are:

- Provide consistent day 1 deployment solution for all the deployment scenarios.
- Add new features to improve existing solutions.
- Provide day 2 management framework mainly in the context of configuration and image upgrades.

## Cisco Network Plug and Play Features

Some of the features that the Cisco Network Plug and Play agent provides:

- Day 0 boot strapping—Configuration, image, licenses, and other files
- Day 2 management—Configuration and image upgrades and on-going monitoring of Simple Network Management Protocol (SNMP) and syslog messages.
- Open communication protocol—Enables customers and partners to write applications
- XML based payload over HTTP between the server and the agent.
- Security—Authentication and encrypted communication channel between the management app and the agent
- Deployment and management of devices behind firewall and Network Address Translation (NAT).
- Support for one-to-one and one-to-many communication
- Support for policy based deployment (product ID or location of the device)
- Deployment based on unique ID (Unique Device Identifier [UDI] or MAC)
- Unified solution across Cisco platforms (including IOS classic)
- Support for various deployment scenarios and use cases

- Zero-touch when possible, low-touch when needed

## Cisco Network Plug and Play Agent Services and Capabilities

The services and capabilities of the Cisco Network Plug and Play agent are as follows:

1. Backoff
2. CLI execution
3. Configuration upgrade
4. Device information
5. File transfer
6. Image install
7. License install
8. PnP tagging
9. Script execution
10. Topology information



**Note** The PnP server provides an optional checksum tag to be used in the image installation and config upgrade service requests by the PnP agent. When the checksum is provided in the request, the image install process compares the checksum against the current running image checksum.

If the checksums are same, the image being installed or upgraded is the same as the current image running on the device. The image install process will not perform any other operation in this scenario.

If the checksums are not same, then the new image will be copied to the local file system, and checksum will again be calculated and compared against the checksum provided in the request. If same, the process will continue to install the new image or upgrade the device to new image. If now, the checksums are not same, the process will exit with error.

### Backoff

A Cisco IOS device that supports PnP protocol (that uses HTTP transport), requires the PnP agent to send the work request to the PnP server continuously. In case the PnP server does not have any scheduled or outstanding PnP service for the PnP agent to execute, the continuous no operation work requests exhausts both network bandwidth and device resource. This PnP backoff service allows the PnP server to inform the PnP agent to rest for the specified time and call back later.

### CLI Execution

Cisco IOS supports two modes of command execution—EXEC mode and global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved when a device reboots. Configuration modes allow user to make changes to the running configuration. If you save the configuration, these commands are saved when a device reboots.

**Note** For **show** command request and response details and for all PnP configuration commands, see *Cisco Network Plug and Play Agent Command Reference*.

### Configuration Upgrade

There are two types of configuration upgrades that can happen in a Cisco device—copying a new configuration files to startup configuration and copying new configuration files to running configuration.

Copying a new configuration files to startup configuration— The new configuration file is copied from the file server to the device through **copy** command and file check is performed to check the validity of the file. If the file is valid, then the file is copied to startup configuration. Backing up the previous configuration file will be done if there is enough disk space available. The new configuration is seen when the device reloads again.

Copying new configuration files to running configuration— The new configuration file is copied from the file server to the device through **copy** command or **configure replace** command. Configuration file replace and rollback may leave the system in an unstable state if rollback is performed efficiently. So configuration upgrade by copying the files is preferred.

### Device Information

The PnP agent provides capability to extract device inventory and other important information to the PnP server on request. The following five types of device-profile requests are supported:

1. all—returns complete inventory information, which includes unique device identifier (UDI), image, hardware and file system inventory data.
2. filesystem— returns file system inventory information, which includes file system name and type, local size in bytes, free size in bytes, read flag, and write flag.
3. hardware— returns hardware inventory information, which includes hostname, vendor string, platform name, processor type, hardware revision, main memory size, I/O memory size, board ID, board rework ID, processor revision, midplane revision, and location.
4. image—returns image inventory information, which includes version string, image name, boot variable, return to rommon reason, bootloader variable, configuration register, configuration register on next boot, and configuration variable.
5. UDI— returns device UDI.

### File Transfer

The PnP file server hosts files that can be copied over by the deploying devices in the network. The file server can be a dedicated server hosting files or a part of the device hosting the PnP server. The PnP agent uses standard file transfer protocols to copy files from the remote file server to the device. If the device is running a crypto image then secured file transfer protocols such as SFTP, SCP, HTTPS are supported. For devices running non-crypto images, the PnP agent supports unsecured copy protocols such as FTP, TFTP, HTTP.

### Image Install

Image installation service enables a PnP-enabled device to perform image upgrade on receiving a request from the PnP server.

### Standalone Devices

When the PnP agent on a standalone device receives a request from the PnP server, the agent parses the XML payload and identifies the request as an Image Upgrade request. The agent then creates an ImageInstall process, which identifies the request as a standalone image install request. The PnP agent populates the data structure defined by the ImageInstall service and passes it to the ImageInstall service.

The Image Install service then performs the following operations to successfully load the device with the new image:

1. Copies the image from the file server to a local disk (the file server information is provided by the PnP server in the request).
2. Configures the device to load the new image on next reload by executing the **boot system** command.
3. Reloads the device and sends a message to the PnP server.

### PnP Tagging

Cisco IOS provides capability to assign tags to the devices for better grouping and tracking of all Cisco devices. The PnP agent provides XML service for configuring the tag information on the device and for propagating the tag information within the network using Cisco Discovery Protocol (CDP). The purpose of this service is for the PnP agents to get to know their tag information and to pass on this information to the PnP server upon request.

### Topology Information

By default, every Cisco device on the network runs Cisco Discovery Protocol (CDP). Through CDP, devices in the network discover their immediate neighbors and populate their databases with the attributes learnt or derived through the protocol. This neighbor information is stored in the database and is available on demand by the device to the PNP server. Typical neighbor information comprises neighboring device ID, software version, hardware platform, interface ip, and the port on which CDP messages are sent or received.

## Software Maintenance Upgrade

The software maintenance upgrade (SMU) is a package that contains fixes for a specific defect or security resolution to a released image. SMUs are created to respond to immediate issues and do not include new features. SMUs do not have a large impact on router operations. SMU versions are synchronized to the package major, minor, and maintenance versions they upgrade.

To install and activate a software maintenance upgrade package:

### Procedure

**Step 1** Use the **install add** <*filename*> command to unpack the package software file and copy it to the boot device (usually disk0). If the file is on a remote source, use the tftp/ftp option to copy the file to the device.

After the file is copied to the device, information within the package is used to verify compatibility with the target cards and with the other active software. Actual activation is performed only after the package compatibility and application program interface (API) compatibility checks are passed.

**Step 2** To activate a package, use the **install activate** <*filename*> command. The activate operation will run the compatibility checks and install the software maintenance upgrade package. If it is a reload software maintenance upgrade, it will automatically initiate a reload.

**Step 3** Use the **install commit** command to commit the changes

**Step 4** To deactivate the package, use the **install deactivate** <*filename*> command.

**Step 5** If you find that you prefer a previous package set over the currently active package set, you can use the **install rollback to committed** command to make a previously active package set active again

**Step 6** To remove the installed version, use the **install remove** <*filename*> command.

This example shows how to install and remove the software maintenance upgrade package on a device.

```
install add <filename>
install activate <filename>
install commit
install rollback to committed
install remove <filename>
```

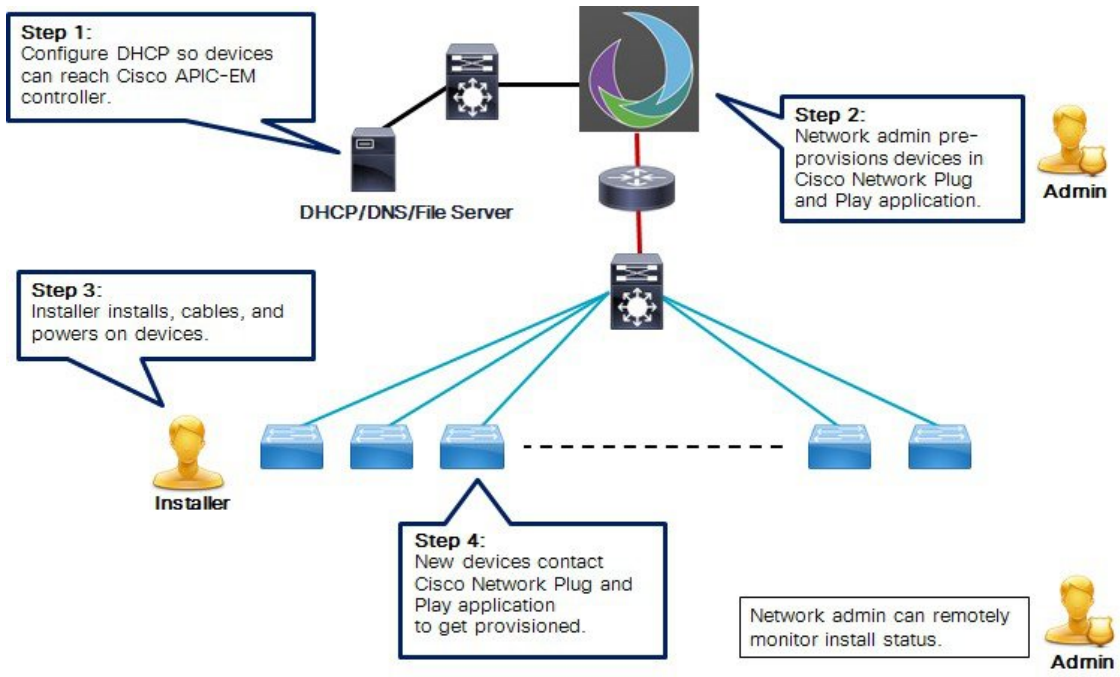
## Cisco Network Plug and Play Agent

The Cisco Network Plug and Play agent is an embedded software component that is present in all Cisco network devices that support simplified deployment architecture. The PnP agent understands and interacts only with a PnP server. The PnP agent first tries to discover a PnP server, with which it can communicate. Once a server is found and connection established, the agent performs deployment related activities like configuration, image, license, and file updates by communicating with the server. It also notifies the server of all interesting deployment related events like out-of-band configuration changes and a new device connection on an interface.

## Cisco Network Plug and Play Server

The Cisco Network Plug and Play server is a central server that encodes the logic of managing and distributing deployment information (images, configurations, files, and licenses) for the devices being deployed. The server communicates with the agent on the device that supports the simplified deployment process using a specific deployment protocol.

*Figure 6: Simplified Deployment Server*




The PnP server also communicates with proxy servers like deployment applications on smart phones and PCs, or other PnP agents acting as Neighbor Assisted Provisioning Protocol (NAPP) servers, and other types of proxy deployment servers like VPN gateways.

The PnP server can redirect the agent to another deployment server. A common example of redirection is a PnP server redirecting a device to communicate with it directly after sending the bootstrap configuration through a NAPP server. A PnP server can be hosted by an enterprise. This solution allows for a cloud based deployment service provided by Cisco. In this case, a device discovers and communicates with Cisco's cloud based deployment service for initial deployment. After that, it can be redirected to the customer's deployment server.

In addition to communicating with the devices, the server interfaces with a variety of external systems like Authentication, Authorizing, and Accounting ( AAA) systems, provisioning systems, and other management applications.

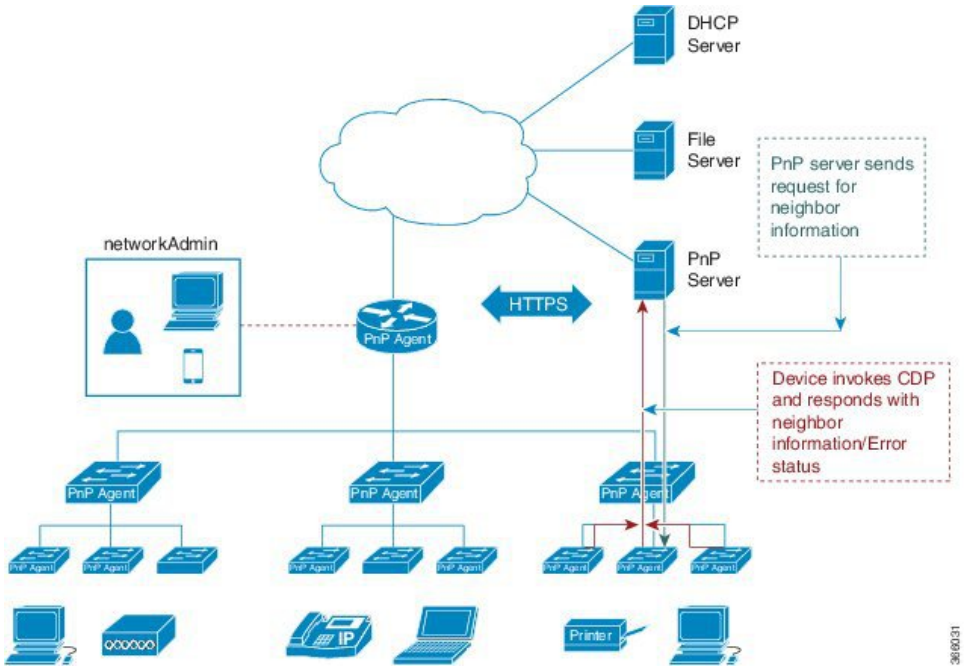
## Cisco Network Plug and Play Agent Deployment

The following steps indicate the Cisco Network Plug and Play agent deployment on Cisco devices:

1. The Cisco device, having PnP agent contacts the PnP server requesting for a task, that is, the PnP Agent sends its unique device identifier (UDI) along with a request for work.
2. The PnP server if it has any task for the device, sends a work request. For example, image install, config upgrade, and so on.
3. When the PnP agent receives the work request, executes the task and sends back a reply to the PnP server about the task status, whether it is a success or error, and the corresponding information requested.

# Cisco Network Plug and Play Agent Network Topology

*Figure 7: Network Topology of Cisco Network Plug and Play Agent Deployment*



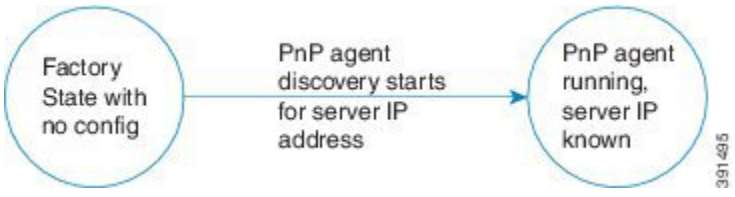

# Cisco Network Plug and Play Agent Initialization

The Cisco Network Plug and Play agent software is currently available on all Cisco IOS XE platforms, and is enabled by default. The PnP agent can be initiated on a device by the following ways:

## Absence of Startup Configuration

New Cisco devices are shipped to customers with no startup configuration file in the NVRAM of the devices. When a new device is connected to a network and powered on, the absence of a startup configuration and the user input file on the device, it will automatically trigger the Cisco Network Plug and Play agent to discover the PnP server IP address.

*Figure 8: State Diagram for PnP Trigger with no Startup Configuration*




## CLI Configuration for Open Plug-n-Play Agent

Network administrators may use CLI configuration mode to initiate the Open Plug-n-Play (PnP) agent process at any time. By configuring a PnP profile through CLI, a network administrator can start and stop the PnP agent on a device. When the PnP profile is configured with CLI, the device starts the PnP agent process which, in turn, initiates a connection with the PnP server using the IP address in the PnP profile.

*Figure 9: State Diagram for PnP Trigger with CLI Configured PnP Profile*




# Cisco Network Plug and Play Agent Deployment Solutions

This section discusses the functionality of the Cisco Network Plug and Play agent, exposed to the PnP server, for device deployment and management. The PnP agent deployment solution comprises the discovery process initiated by the agent, communication between the device, agent, and the server, and the PnP agent services. The PnP solution is described in detail in the following sections:

## Cisco Network Plug and Play Agent Discovery Process

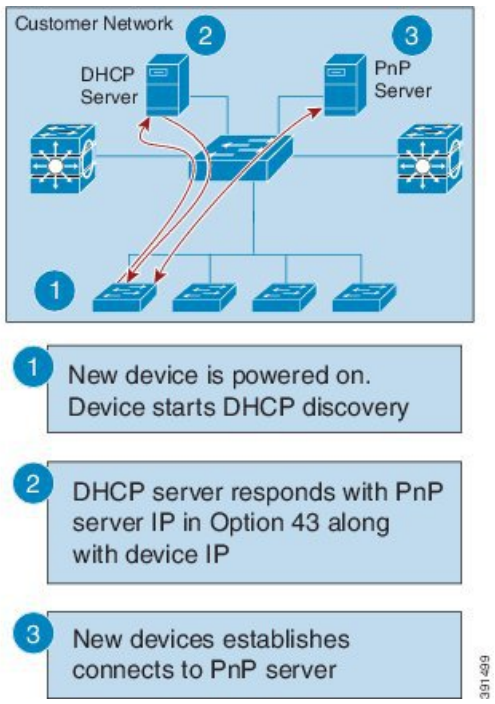
When the device boots up, the absence of any startup config on the NVRAM triggers the PnP discovery agent to acquire the IP address of the PnP server. In order to acquire the IP address of the PnP server, the PnP agent goes through one of the following discovery mechanisms:

1. PnP discovery through DHCP server
2. PnP discovery through DHCP snooping
3. PnP discovery through DNS lookup
4. PnP proxy for layer 2 and layer 3 devices
5. PnP deployment application

### Cisco Network Plug and Play Discovery through DHCP Server

Device with no startup configuration in the NVRAM triggers the Cisco Network Plug and Play agent to initiate a DHCP discovery process which acquires the IPv4 configuration from the DHCP server required for the device. The DHCP server can be configured to insert additional information using vendor specific option 43 upon receiving option 60 from the device with the string ‘cisco pnp’, to pass on the IPv4 address or hostname of the PnP server to the requesting device. When the DHCP response is received by the device, the PnP agent extracts the option 43 from the response to get the IP address or the hostname of the PnP server. PnP agent then uses this IPv4 address or hostname to communicate with the PnP server.

*Figure 10: DHCP Discovery Process for PnP server*




**Assumptions:**

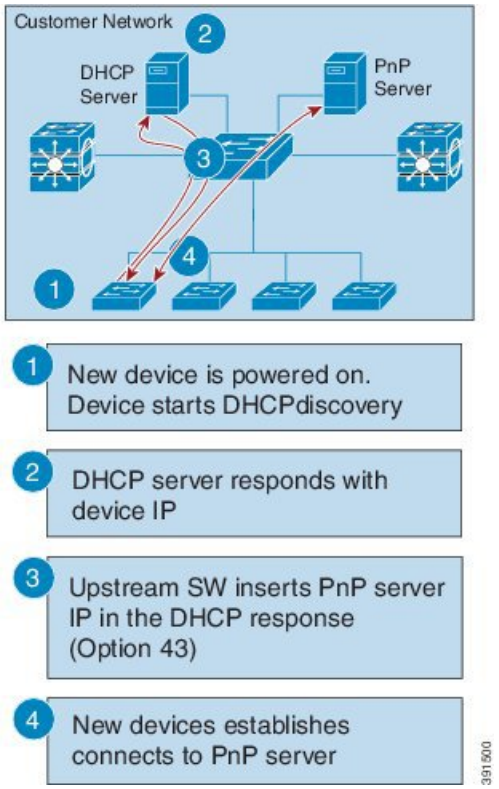
- New devices can reach DHCP server
- Customer is willing to configure DHCP server for network devices

## Plug-n-Play Discovery through DHCP Snooping

If a third party DHCP server cannot be configured to insert any vendor specific options, an existing Cisco Open Plug-n-Play (PnP) enabled device can be configured to snoop in to the DHCP response and insert PnP specific option 43 with the PnP server IP address.

Before inserting the option 43, the snooping agent verifies if the DHCP message is from a Cisco device in the network. The remaining DHCP discovery process is same as described in the previous section.

*Figure 11: DHCP Snooping by PnP Server*



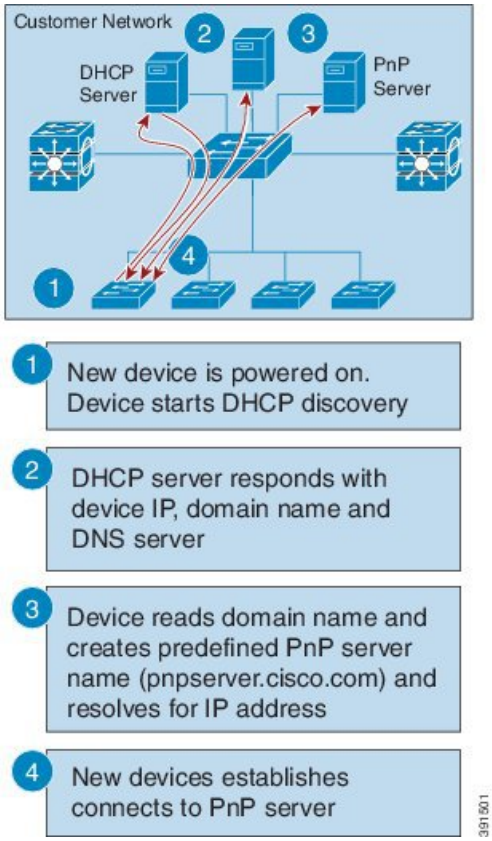

**Assumptions:**

- New devices can reach DHCP server
- New devices can reach DNS server
- Customer is not willing to configure DHCP server for network devices
- Upstream switch (SW) is configured to snoop DHCP and insert PnP server IP

## Cisco Network Plug and Play Discovery through DNS Lookup

When the DHCP discovery fails to get the IP address of the Cisco Network Plug and Play server, the agent falls back on Domain Name System (DNS) lookup method. PnP agent then uses a preset deployment server name. The agent obtains the domain name of the customer network from the DHCP response and constructs the fully qualified domain name (FQDN). The following FQDN is constructed by the PnP agent using a preset deployment server name and the domain name information for the DHCP response, *deployment.customer.com*. The agent then looks up the local name server and tries to resolve the IP address for the above FQDN.

*Figure 12: DNS Lookup for deployment.customer.com*



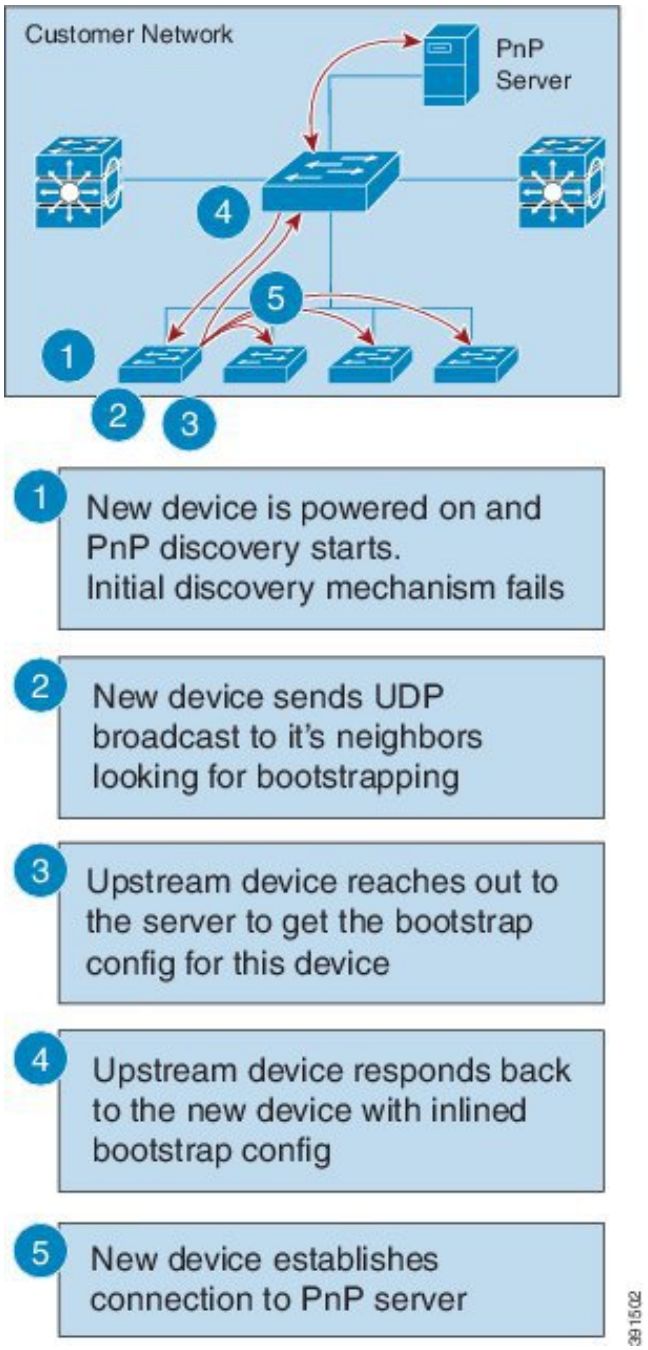

**Assumptions:**

- New devices can reach DHCP server
- Customer deployed PnP server in the network with the name “pnpserver”

## Cisco Network Plug and Play Proxy Server for Layer 3 and Layer 2 Devices

This device listens to a specific port for any incoming PnP messages. The Cisco device which is trying to come up as a PnP device sends a UDP broadcast message to its network every 30 min for ten times. Hence, if the device does not receive a response, the broadcasts stop after 300 min.

*Figure 13: DNS Lookup for Layer 3 and Layer 2 Devices*




When the device hosting the proxy server process receives the incoming broadcasts, it verifies the version field in the request and forwards the request to the PnP server if version validation is successful. The proxy server process also caches the unique device identifier (UDI) of the requesting client coming in via incoming datagram before forwarding the request to PnP server.

Upon receiving the configlet datagram from PnP server, the proxy server validates UDI in the incoming datagram with the entries in the UDI cache. If validation is successful, proxy server process broadcasts the datagram to a specific port number reserved for the proxy client processes to receive datagrams.

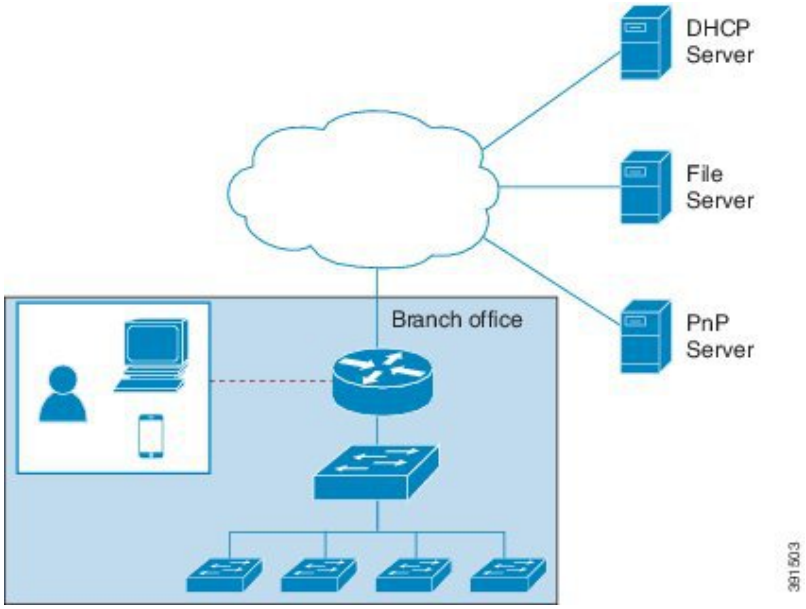
Upon receiving the datagrams, devices running proxy client processes, parse the incoming datagram for the target UDI. If the target UDI in the datagram matches the UDI of the device, proxy client process proceeds with framing, error control and configuring the configlet.

If the target UDI in the datagram fails to match UDI of the device, the packet is dropped.

### Plug-n-Play Agent Deployment Application

A Cisco device can alternatively be manually configured by the network administrator using a deployment application running on their PC or on a smart phone. The PC or the smart phone can be connected to the device using an USB or an Ethernet cable.

***Figure 14: Manually Configured PnP Agent***




## Plug-n-Play Agent Deployment Protocol

Deployment can be run over different transports. These transports include Ethernet and IP with Transport Layer Security (TLS). Layer 2 transport is typically used between a deployment agent and a proxy deployment server like a deployment application or as a deployment agent acting as a proxy. Transport between an agent and a server is over an IP connection with TLS for security. Transport between a proxy deployment server and a deployment server is also over IP with TLS.

### Plug-n-Play Agent Application Protocol

The Cisco Open Plug-n-Play (PnP) agent application protocol is an XML-based protocol that defines a mechanism that allows network devices to be monitored and controlled by a remote application. The PnP agent is a software module running on a Cisco device. The PnP server is an application running as the network manager that remotely manages the network devices. The main features of the PnP protocol are as follows:

1. Supports HTTP protocols

2. Supports Transport Level Security (TLS) based encryption for HTTP
3. Uses HTTP secure (HTTPS) certificate for TLS handshake

### Plug-n-Play Transport over Ethernet

Cisco Open Plug-n-Play (PnP) agent uses the Ethernet based transport in the following two scenarios:

- **Deployment agent communicating with a deployment application on a PC**: In this case, the PC is connected to the device being deployed using an Ethernet cable. The deployment application advertises itself as a deployment server supporting Ethernet transport.
- **Deployment agent communicating with an already deployed device acting as a proxy deployment server**: In this case, the new device being deployed has an Ethernet connection to an already deployed device. The deployment agent on the deployed device responds to the discovery requests and acts as a proxy deployment server for the new device.

Once discovery is complete, the deployment agent starts an unsecured XML stream with the deployment server over Ethernet. This protocol reserves an Ethertype (0xXX TBD) for this purpose. The deployment agent and the server then negotiate to use Extensible Authentication Protocol–Transport Layer Security (EAP-TLS) to protect the communication and complete the EAP-TLS session establishment. The deployment server then authenticates the device with the HTTP secure (HTTPS) certificate or some other supported mechanism.

### Plug-n-Play Transport over IP

In Cisco Network Plug-n-Play (PnP) agent, the deployment agent opens TCP connection to the deployment server and starts an XML stream of messages. The server can request the use of Transport Layer Security (TLS) at this time. The agent closes the existing XML stream, initiates a TLS connection to the server, and then restarts the XML stream. The server can request agent authentication over the TLS connection.

## Plug-n-Play Agent Security

Security to all Cisco Open Plug-n-Play (PnP) devices is provided at both transport level as well as the application level. The following sections describe the security mechanisms in detail:

### Plug-n-Play Transport Layer 3 Security

For non-crypto or non-crypto-enabled images, TLS security choice is not possible. One alternative minimum security is to have the PnP agent initiate the connection to the specified trusted PnP server on port 5222.

### Authentication and Authorization between Plug-n-Play Agent and Server

Once the Cisco Open Plug-n-Play (PnP) deployment agent discovers the PnP server, the agent engages the server in a Transport Layer Security (TLS) handshake. In order to authenticate itself to the server, the agent presents its HTTP secure (HTTPS) certificate. The administrator for the PnP server sets device authentication mechanisms which are acceptable for a particular deployment.

The deployment server presents its certificate to the deployment agent so that the agent can authenticate the server. Irrespective of whether the agent is able to verify the server certificate, the agent engages the deployment server in a post-TLS authorization exchange. In this exchange the agent requests the server to present its server authorization token. In response to this request the server presents the authorization token it had obtained from Cisco. The agent verifies the signature on the authorization token. If the authorization token is specific to a Unique Device Identifier (UDI), the agent also ensures its UDI is listed in the authorization-token. At the

end of this step, a secure communication channel is established between the deployment agent and the server. This secure communication channel is leveraged by the server to send deployment information to the agent.

# Security Methods for the PnP Discovery Process

This section describes the methods that are used to secure the PnP agent-server communication in various scenarios. The security options are used by the PnP agent during the zero-touch PnP server discovery.

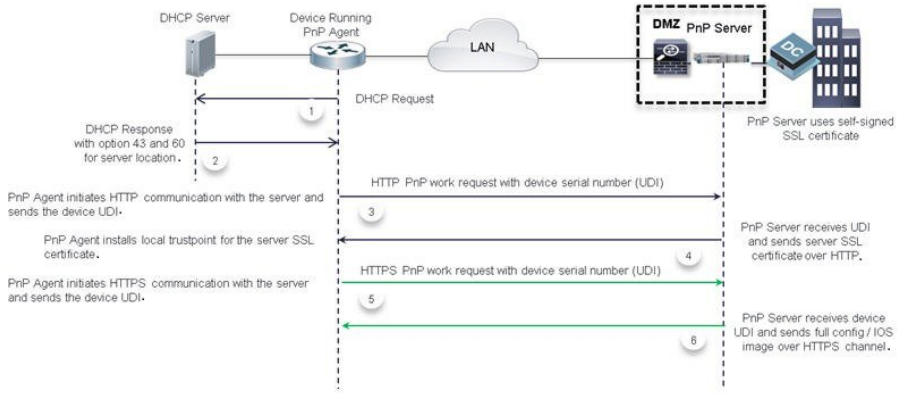
## Self-Signed Certificate Based Authentication

The PnP server has an option to use a self-signed SSL certificate for server side authentication. When the PnP server uses a self-signed certificate, the PnP discovery cannot be used for automatically initiating secured communication from the agent to the server. The device goes through usual PnP discovery mechanisms and when it finds the server, the agent sends a work-request over HTTP. The server should use the PnP certificate-install service to instruct the agent to install the server self-signed certificate, and then automatically reconnect back to the server over HTTPs.

To keep the solution secured, it is recommended that you use the unsecured port 80 of server to deliver the one-time certificate installation to the devices. All other services should be sent over the secured port.

The following figure shows the end-to-end secured PnP workflow using a self-signed server SSL certificate.

***Figure 15: PnP Deployment with Self-Signed Certificate***

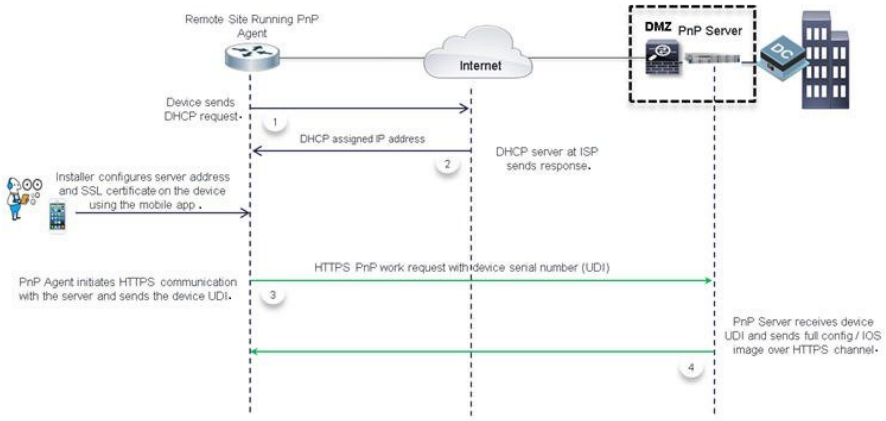



## Mobile Device Based Secured Installation

As part of this solution, an application for mobile devices is available to configure the bootstrap on the devices. The mobile application can be used to install the server certificate directly on each device along with other bootstrap configuration and then allow the PnP agent initiate secured communication with the server. In this method, the server does not open up any unsecured port for certificate-install.

The following figure shows the end-to-end secured PnP workflow using the application on the mobile devices.

*Figure 16: Secured PnP Deployment with the Mobile Application*




# CA-Signed Certificate based Authentication

Cisco distributes certificates signed by a signing authorities in a tar file format and signs the bundle with Cisco Certificate Authority (CA) signature. This certificate bundle is provided by Cisco infoSec for public downloads on cisco.com.

The certificates from this bundle can be installed on the Cisco IOS device for server side validation during SSL handshake. It is assumed that the server uses a certificate, which is signed by one of the CA that is available in the bundle.

The PnP agent uses the built-in PKI capability to validate the certificate bundle. As the bundle is signed by Cisco CA, the agent is capable of identifying the bundle that is tampered before installing the certificates on the device. After the integrity of the bundle is ensured by the agent, the agent installs the certificates on the device. After the certificates are installed on the device, the PnP agent initiates an HTTPs connection to the server without any additional steps from the server. The following mechanisms helps the PnP agent to initiate a zero-touch secured communication.

## DHCP Option based Discovery over an IPv4 Network

The DHCP option 43 and option 60 is a vendor specific identifier which is used by the PnP agent to locate and connect to the PnP server. To support multiple vendors, the PnP agent in Cisco device sends out a case-sensitive “ciscopnp” as the option 60 string during the DHCP discovery. The DHCP server can be configured with multiple classes matching with a different option 60 string that comes from each network device. After the option 60 string matches, the DHCP server sends out the corresponding option 43 string back to the device. The following is the format for defining the option 43 for PnP deployments:

*option 43 ascii "5A;K5;B2;I10.30.30.10;J443;**Ttftp://10.30.30.10/ ios.p7b**;Z10.30.30.1*

The field ‘T’ in the PnP string provides an option for the network administrator to specify the location of the certificate bundle, which can be hosted on a local or remote file server.

If the certificate bundle is available at the specified location, then the agent:

1. Downloads the bundle from the file server to the device.
2. Checks the signature of the downloaded bundle to ensure it has a genuine Cisco signature.
3. Installs the certificates on the device.

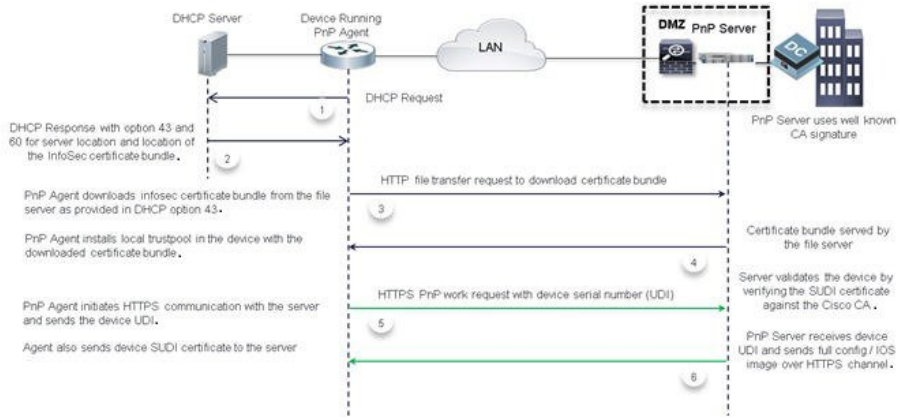
If the ‘T’ option is not specified and the transport mechanism is specified in the option 43 string as HTTPs, the PnP agent looks for the Cisco signed certificate bundle in the default folder of the same server *http://10.30.30.10:443/certificates/default/cert.p7b* .

If the certificates are available at the default location then the agent performs the steps mentioned above to install the certificates.

After the certificates are installed and the server discovery is complete, the agent initiates the HTTPs connection with the server without any additional configuration. During the HTTPs handshake, the device uses the certificates installed from the bundle to validate the server certificate.

The following figure shows the end-to-end secured PnP workflow using the CA bundle-based certificate.

***Figure 17: Secured PnP Deployment with Trustpool***




This flow works only if the server is using a certificate signed by one of the known signing authorities that is available in the bundle. If the server uses a certificate that is not a part of the bundle then the HTTPs handshake will fail. When you specify the option 43 string with HTTPs as a transport option and if the bundle download fails, the agent will not fall back to any of the unsecured communication protocol even if the server is reachable. If the transport option is specified as HTTP with a parameter 'T' pointing to a valid certificate bundle location, the agent overrides the transport option HTTP and changes it to HTTPs for secured communication. Generally, the agent will choose the most secured communication from the available options.

The path specified in the DHCP option 43 to locate the certificate bundle file can be an absolute URL or a relative URL. If you specify a relative URL, the agent forms a full URL with the server IP address or hostname as specified in the option 43 string and uses HTTP as the file transfer protocol.

Also, to install the certificates, the agent expects the device to have an updated system clock. Because, you configure the DHCP server first, you cannot specify the current time in the DHCP server. In such a scenario, an IP address or a URL can be specified as an alternative parameter in the option 43 with the prefix 'Z', which can point the device to a NTP server. The agent synchronizes the clock on the device with the NTP server and then installs the certificates.

## DHCP Option based Discovery over an IPv6 Network

Cisco Network PnP uses the DHCP Option 16 and Option 17 for an IPv6 DHCP discovery process.The Option 16 and Option 17 are vendor specific identifiers. These are used by the Cisco Network PnP agent to locate and connect to the Cisco Network PnP server. The DHCP server can be configured to insert an additional information using the vendor specific Option 17. When the DHCP server receives an Option 16 from the device with the string *cisco pnp* , and if it matches the Option 17 string, the server passes the IP address or the hostname of the Cisco PnP server to the requesting device. When the device receives the DHCPv6 response,

the Cisco Network PnP agent extracts the option from the response and identifies the IPv6 address of the Cisco PnP server. Cisco PnP agent uses this IPv6 address to communicate with the Cisco PnP server. To obtain and install the certificate, use the same process explained in the DHCP Option based Discovery over an IPv4 Network section.

The following example shows how to configure a pool (DHCPv6-pool) with the vendor-specific options:

```
ipv6 dhcp pool dhcpv6-pool
 address prefix 2003::/64 lifetime infinite infinite
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;K4;B3;IFE80::2E0:81FF:FE2D:3799;J6088"
```

## DNS-based Discovery

In DNS-based discovery, a DHCP server receives the domain name of the customer network. The domain name is used to create a PnP-specific, fully qualified domain name (FQDN) such as *pnpserver.<domain_name>*. In this method, the customer network resolves this URL to a valid PnP server IP address. Because, there is no mechanism to specify the certificate location, the agent locates the server certificate to initiate the HTTPs connection without manual intervention.

During the system boot up, the device acquires IP network information from a DHCP server along with the domain name. With the customer specific domain name, the Cisco PnP agent creates the following URL *pnpserver.<domain_name>* and looks for the Cisco signed certificate bundle in a default folder of the server *<domain_name>/ca/trustpool/cabundle.p7b*.

If the certificate bundle is available at the specified location, then the agent:

1. Downloads the bundle from the file server to the device.
2. Checks the signature of the downloaded bundle to ensure it has genuine Cisco signature.
3. Installs the certificates on the device.

If the certificate bundle is not available at the specified location, the PnP agent use a predefined URL,*pnpcertserver.<domain_name>* and looks for the Cisco signed certificate bundle in the default folder of the server, *<domain_name>/ca/trustpool/cabundle.p7b*.

If the certificates are available at the specified location, then the agent performs the steps specified above to install the certificates.

After the certificates are installed and the server discovery is complete, the agent initiates the HTTPs connection with the server at the URL, *pnpserver.<domain_name >* without any additional configuration. During the HTTPs handshake, the device uses the certificates that are installed from the bundle to validate the server certificate.

Also, to install the certificates, the agent expects the device to have an updated system clock. Because, you configure the DHCP server first, you cannot specify the current time in the DHCP server. In such a scenario, the agent uses a predefined URL, *pnpntpserver.<domain_name>* which needs to be mapped to a NTP sever to synchronize the clock on the device, and then installs the certificates.

However, if the certificate is not present at either URL, the Cisco PnP agent will fall back and establish the HTTP connection to the server using the created FQDN pnpserver.<domain_name>. With this workflow, the agent expects the server to use the certificate-install service to install the self-signed certificates first and then start the provisioning steps.

## DNS-based Discovery over an IPv6 Network

To enable DNS-based discovery over an IPv6 network:

### Procedure

**Step 1** Configure the DNS server with an IPv6 option. To enable the Cisco Network PnP DNS discovery, configure the DNS server as shown in this example:

```
ip host pnpntpserver.domain.com 2001::1
ip host pnptrustpool.domain.com 2001::2
ip host pnpserver.domain.com   2001::3
```

**Step 2** DHCPv6 server is discovered through DHCP bootstrap process. The following example shows how to configure the DHCP server:

```
ipv6 unicast routing
ipv6 cef

ipv6 dhcp pool test
dns-server 2001::4
domain-name example.com
```

The device sends the DHCPv6 packets to the server over an IPv6 network. After receiving the DHCPv6 packets, the DNS server information and the domain-name are returned to the device as Option 23 and Option 24 respectively.

**Step 3** Configure the NTP server. The following example shows how to configure the NTP server:

```
ntp master 1
```

**Note** Similarly, the device NTP configuration should use the NTPv4 option.

**Step 4** Host the trustpool server on an IPv6 network. Trustpool is supported only on DHCP Options T and Z. If the Option T is configured, specify the URL of the trustpool CA bundle. If the Option Z is configured, specify the NTP server IP address.

**Note** When the Cisco Network PnP agent attempts to download the trustpool bundle over HTTP by using an IPv6 option, the trustpool server should support HTTP over an IPv6 network. Also, the clock must be syncronized before configuring the trustpool.

**Step 5** Host the Cisco Network PnP server on an IPv6 network.

## Cisco Cloud Redirection over an IPv4 and IPv6 Network

Cisco Cloud Redirection service supports Cisco Network PnP zero-touch discovery. It is supported on both IPv4 and IPv6 based Cisco Cloud discovery.

**Note** Some of the Cisco PnP devices may have root certificate embedded in the devices. These devices will communicate with the CCO server using HTTPS from the beginning. If the device does not have the embedded certificate then the legacy behavior is initiated.

When the device boots up without any start-up configuration or authentication certificates, and if the DHCP and DNS discovery fails, the device tries to contact the Cisco Cloud server at *devicehelper.cisco.com*.

If the *devicehelper.cisco.com* is reachable, the Cisco Network PnP agent downloads the trustpool bundle and establishes a secure HTTP connection with the Cisco Cloud Redirection service. When the device tries the Cisco cloud discovery for the first time, Cisco Network PnP agent downloads the trustpool from this location *devicehelper.cisco.com/ca/trustpool* and saves it to the local flash memory. This location is shared with a Public Key Infrastructure for a trustpool installation. If the Cisco cloud discovery fails, trustpool bundle is retained in the flash memory and Cisco Network PnP checks for a copy of the trustpool bundle in the local device flash memory. If the copy is not available in the local flash memory, it retries to download the trustpool bundle from this location *devicehelper.cisco.com/ca/trustpool download*.

Cisco Network PnP agent sends a HTTPS hello message to the Cisco cloud. The Cisco Network PnP redirection service running at Cisco cloud server replies to the HTTP request. A Cisco cloud server PnP profile is created on the device as shown in this example.

```
pnp profile pnp_cco_profile
transport https host devicehelper.cisco.com port 443
```

After the Cisco cloud profile is created, the device sends a work-information message with its unique device identifier information to the Cisco cloud server. Cisco Cloud Redirection service sends a redirection non-backoff PnP request with the Cisco Network PnP server information. It can be an IPv4 address, IPv6 address, or a hostname. When the redirection is successful, the following redirection profile is configured on the device.

```
pnp profile pnp_redirection_profile
transport https ipv4 172.19.153.133 port 443
```

If the non-backoff PnP request is not received within default wait time, Cisco Network PnP discovery process continues with the next discovery mechanism.

## Cisco Network PnP Discovery Over 4G Interface

Cisco Network PnP over 4G interface is available on platforms that have 4G NIMs and running Cisco IOS XE.When a device with an activated SIM card boots up, the 4G interface is activated and used for the Cisco Network PnP cloud discovery process. When a device without an activated SIM card boots up, the non-4G interfaces are preferred for the discovery process. Cisco Network PnP cloud discovery over 4G interfaces is attempted when the non-4G interfaces are not available or if the Cisco Network PnP discovery does not succeed on the non-4G interfaces. When the device has multiple 4G interfaces with active SIM cards, the Cisco Network PnP tries the cloud discovery on all the 4G interfaces one after the other until one of them succeeds.

**Note** To use the 4G interface for the Cisco Network PnP discovery, the 4G NIMs should have an activated SIM card on it.

Cisco Network PnP Cloud discovery over 4G interfaces works when all the 4G interfaces are activated during the device bootup by default. In the absence of a startup configuration, the device attempts to bring up the 4G

inutrafec by default and attempts Cicso PnP over cloud. After the device is redirected, the device connects to the Cisco Network PnP server and downloads the appropriate image and configuration to the device.

**Note** The DNS server is available as part of the 4G network and the cloud portal should be programmed to redirect the calling device to an appropriate Cisco Network PnP server for provisioning the device. Currently, Cisco Network PnP support over 4G interface uses only the IPv4 network.

Ensure that the configuration pushed through the Cisco Network PnP server contains a route to Cisco Network PnP server over the 4G interface. This can be a default route and should retain the Cisco Network PnP agent and server communication to continue to work over the 4G interface, after the provisioning is completed.

## Cisco Network PnP Discovery over a Management Interface

Cisco Network PnP Agent supports discovery and four-way handshake over a management interface with a default VPN Routing/Forwarding (VRF). To send and receive the DHCP traffic over an VRF interface, you have to configure the IOS DHCP server . This feature helps the new devices to access the Cisco Network PnP features when only the management interface is active.

When the device boots up, the management interface under the default VRF is assigned an IP address though DHCP. This interface establishes a connection to a Cisco Network PnP server and the Cisco Network PnP agent on the device records this information (VRF name and source interface). This information is used for future PnP communication with the Cisco Network PnP server. In this case, the Cisco PnP profile that is created on the device will have an extra keyword **VRF** attached to it.

## Cisco PnP over an EtherChannel

When you deploy an access switch by using the Cisco Network Plug and Play, the existence of LACP EtherChannels on the provisioned switch (which acts as trunk) does not allow you to configure the device. When the access device tries to connect through the provisioned switch over an L2 EtherChannel using LACP, it breaks the connectivity. Since the configuration does not exists on the access device, the access device cannot bring up the EtherChannel with the switch. This results in keeping the EtherChannel ports in suspended state and breaks the L2 connectivity. Cisco Network PnP Agent detects the presence of EtherChannels and auto-configures the EtherChannel on the device to bring up the Layer 2 connectivity automatically for the day-zero configuration.

# Security Methods for Post-PnP Discovery Process

This section explains the methods provided by the Cisco PnP agent which can be, used by the Cisco PnP server to secure the client-server communication after completing the discovery process. This section includes the following topic:

• Certificate Install Service, on page 255

# Certificate Install Service

The Cisco PnP agent provides a mechanism to manage SSL certificates on the device by providing the certificate-install service to the Cisco PnP server. The certificate-install service provides a simple XML to install the server's self-signed certificates or certificates signed by standard CA certificates on the device,

before initiating an HTTPs connection. The certificate-install service also provides an option to install the client SSL certificate and instruct the device to use the same SSL certificate during the next device authentication process.

# SUDI-based PnP Application Level Authentication

The SSL communication ensures encryption of the data packets exchanged between the server and the device, but does not provide a solution to authenticate the device.

To ensure that the server is talking to a genuine Cisco device, the agent uses the built-in Secure Unique Device Identifier (SUDI) certificate support on the device. SUDI is a X.509 compliant device certificate burnt into the device's secured chip (ACT2) during the manufacture time. The SUDI certificate contains the device's serial number, private-public keys, and the Cisco CA signature. The agent provides the following mechanisms that can be used by the server to authenticate the device as a genuine Cisco device:


- SUDI-based Client Certificate Validation, on page 256
- SUDI-based Serial Number, on page 256


## SUDI-based Client Certificate Validation

Before the agent initiates an HTTPs connection with the server, the agent checks whether the device has a built-in SUDI certificate. If the device has a certificate, then the agent sends the SUDI certificate to the client during the SSL handshake for validating. Optionally, the HTTPs server may choose to validate the device using the SUDI certificate during the SSL handshake. After validating, the HTTPs server allows the device to connect to the server. To validate the device's SUDI certificate, the server should use Cisco CA to complete the validation.

## SUDI-based Serial Number

If the device is loaded with SUDI certificate, the PnP agent reads the serial number from the SUDI certificate and presents the same information as an additional tag in the work-request body for all communication with the server. To achieve this, the following optional tag is added in the work-info message, which goes out from the device in every work-request. This field is optional and does not show up for devices that does not have SUDI certificate.

There is no change in the existing UDI mechanism that is read from the chassis inventory. The agent continues to be backwards compatible by sending the chassis UDI as the primary identifier. The server can use the additionally provided SUDI-based serial number to authenticate the device and then continue to use the primary UDI. For the devices without a SUDI certificate, the agent does not send this additional SUDI-based serial number. Therefore, the server should continue with the primary UDI for authentication and further communication.

There is no mechanism available to read the SUDI-based serial number from member hardware and there is no change in how UDI is read from other members on a stack or HA unit. The agent will continue to read the UDI from all the hardware units as it does presently.

## SUDI-Based Device Authentication

In SUDI-based device authentication, the agent checks whether the device has a built-in SUDI certificate at the boot-up time. If the device is loaded with the SUDI certificate, the agent provides a new PnP service, which allows the server to help the device to identify itself. The availability of this new service depends on the presence of the SUDI certificate and is listed in the agent's capability service.

Along with the above change in the capability-service, the agent adds an additional field under the hardware-info section of the device-info response, to specify and check whether the SUDI certificate is built into the device.

After, the agent initiates an HTTPs connection with the server and sends a work-request, the server should be able to use the device authentication service for a challenge request-response. The device authentication service requires a minimum of one field to generated a string by the server. Optionally, the server can send a list of encryptions and hashing methods that it can support. The agent checks whether it has the capability to use any of the listed encryption methods specified by the server, uses the encryption method and sends a notification to the server. If the agent does not have the capability to use any of the methods specified by the server, then the agent responds with an error message.

When the server sends a device authentication service request to the agent, the agent does the following:

1. Uses one of the specified encryption and hashing methods.
2. If the agent does not have capability to use one of the specified encryption and hashing methods, the agent responds with an error message.
3. Encrypts the challenge string provided by the server using the private key using the PKI APIs.
4. Sends a response back with the following:
   a. Cipher text
   b. Methods used to cipher
   c. Certificate (SUDI or client installed certificate)

After, the server receives the above response from the device, the server does the following:

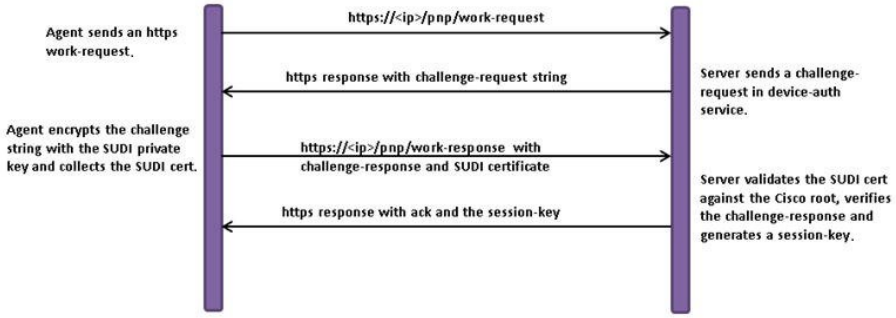
1. Verifies the SUDI or the client certificate against the Cisco or customer CA.
2. Decrypts the cipher-string using the public key that is available in the SUDI or client certificate.
3. Verifies whether the deciphered string matches the original version.
4. Generates a session key (string) and sends it back to the device as an acknowledgment.

After the agent receives the final acknowledgment from the server with the session-key, it associates the corresponding profile with the provided session-key and sends it to the server as an attribute in the root PnP section of all the subsequent messages that the agent sends.

The server validates the session-key before sending any message from the device. Optionally, the server maintains a timer for the session-keys and moves to invalid status when the timer expires. If the agent sends a message with an expired session-key, the server repeats the device authentication process and generate a new session-key before sending to the same device again. If the device sends a request without any session-key, then the server performs the device authentication process and generates a new session-key before sending to the same device.

The following figure displays the message sequence between the agent and the server to accomplish the device authentication using the SUDI certificate.

*Figure 18: Message Sequence*




# How to Configure Cisco Network Plug and Play Agent

## Configuring Cisco Network Plug and Play Agent Profile

Perform the following task to create a Cisco Network Plug and Play agent profile:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Network Plug and Play Agent Device

Perform the following task to create a Cisco Network Plug and Play agent device:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **device** {**username** *username* } {**password {0 \| 7}** *password*}<br>**Example:**<br>`Device(config-pnp-init)# device username sjohn password 0 Tan123` | Configures the PnP agent on the device.<br>• Establishes a username and password based authentication system.<br>• *username*—User ID<br>• *password*—Password that a user enters<br>• **0**—Specifies that an unencrypted password or secret (depending on the configuration) follows.<br>• **7**—Specifies that an encrypted ( hidden) password follows. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Cisco Network Plug and Play Reconnect Factor

Perform the following task to configure the time to wait before attempting to reconnect a session in either fixed-interval-backoff, exponential-backoff, or random-exponential-backoff mode:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **reconnect** [*pause-time* [*exponential-backoff-factor* [**random**] ] ]<br>**Example:**<br>`Device(config-pnp-init)# reconnect 100 2 random` | Specifies the time for the PnP agent initiator profile to wait before attempting to reconnect a session.<br>• The pause-time value is the time to wait, in seconds, before attempting to reconnect after a connection is lost. The range is from 1 to 2000000. The default is 60.<br>• Exponential backoff factor value is the value that triggers the reconnect attempt exponentially. The range is from 2 to 9. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Cisco Network Plug and Play HTTP Transport Profile

Perform the following task to create a HTTP transport profile of the Cisoc Plug and Play agent manually on a device.

Both IPv4 and IPv6 addresses can be used for PnP server IP configuration. Alternately, a hostname can also be used in the configuration to connect to the PnP server.

Every profile can have one primary server and a backup server configuration. The Cisco PnP agent attempts to initiate a connection with the primary server first and if it fails, it will try the backup server. If the backup

server fails, the Cisco PnP agent will attempt to connect to the primary server again. This will continue until a connection is established with one of the servers.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **transport http host** *host-name* [**port** *port-number* ] [**source** *interface-type*]<br>**Example:**<br>`Device(config-pnp-init)# transport http host hostname-1 port 1 source gigabitEthernet 0/0/0` | Creates a HTTP transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.<br>• The value of the host specifies the host name, port, and source of the server.<br>• The value of the port-number specifies the port that is used.<br>• The value of the interface-type specifies the interface on which the agent is connected to the server. |
| **Step 5** | **transport http ipv4** *ipv4-address* [**port** *port-number* ] [**source** *interface-type*]<br>**Example:**<br>`Device(config-pnp-init)# transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0` | Creates a HTTP transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed. |
| **Step 6** | **transport http ipv6** *ipv6-address* [**port** *port-number* ] [**source** *interface-type interface-number* ]<br>**Example:** | Creates a HTTP transport configuration for the PnP agent profile based on the IPv6 address of the server on which the PnP agent is deployed. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-pnp-init)# transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1` | |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Cisco Network Plug and Play HTTPS Transport Profile

Perform the following task to create a HTTP Secure (HTTPS) transport profile of the Cisco Network Plug and Play agent manually on a device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **transport https host** *host-name* [**port** *port-number* ][**source** *interface-type* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:**<br>`Device(config-pnp-init)# transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz` | Creates a HTTPS transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.<br>• The value of *localcert* specifies the trustpoint used for client-side authentication during the transport layer security (TLS) handshake.<br>• The value of *remotecert* specifies the trustpoint used for server certificate validation. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** Configure the trustpoint-nam |
| **Step 5** | **transport https ipv4** *ipv4-address* [**port** *port-number* ][**source** *interface-type* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:**<br>`Device(config-pnp-init)# transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz` | Creates a HTTPS transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed. |
| **Step 6** | **transport https ipv6** *ipv6-address* [**port** *port-number* ][**source** *interface-type interface-number* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:**<br>`Device(config-pnp-init)# transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz` | Creates a HTTPS transport configuration for the PnP agent profile based on the IPv6 address of the server on which the PnP agent is deployed. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Backup Cisco Network Plug and Play Device

Perform the following task to create a backup profile and to enable or disable Cisco Network Plug and Play agent manually on a device:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# configure terminal` | |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **backup device** {**username** *username* } {**password {0 \| 7}** *password*}<br>**Example:**<br>`Device(config-pnp-init)# backup device username sjohn password 0 Tan123` | Configures the PnP agent backup profile on the device.<br>• Establishes a username and password based authentication system.<br>• *username*-User ID<br>• *password*-Password that a user enters<br>• 0—Specifies that an unencrypted password or secret (depending on the configuration) follows.<br>• 7—Specifies that a hidden password follows. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Backup Cisco Network Plug and Play Reconnect Factor

Perform the following task to configure backup reconnection of the Cisco Network Plug and Play (PnP) agent to the server in either fixed-interval-backoff, exponential-backoff, or random-exponential-backoff manner :

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **backup reconnect** [*pause-time* [*exponential-backoff-factor* [**random**] ] ]<br>**Example:**<br>`Device(config-pnp-init)# backup reconnect 100 2 random` | Specifies the time for the PnP agent initiator profile to wait before attempting to reconnect a session.<br>• The pause-time value is the time to wait, in seconds, before attempting to reconnect after a connection is lost. The range is from 1 to 2000000. The default is 60.<br>• Exponential backoff factor value is the value that triggers the reconnect attempt exponentially. The range is from 2 to 9. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Backup Cisco Network Plug and Play HTTP Transport Profile

Perform the following task to create a backup HTTP transport profile of the Cisco Network Plug and Play agent manually on a device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:** | Creates a PnP agent profile and enters the PnP profile initialization mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# pnp profile test-profile-1` | • String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **backup transport http host** *host-name* [**port** *port-number* ] [**source** *interface-type*]<br>**Example:**<br>`Device(config-pnp-init)# backup transport http host hostname-1 port 1 source gigabitEthernet 0/0/0` | Creates a backup HTTP transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.<br>• The value of the host specifies the host name, port, and source of the server.<br>• The value of the port-number specifies the port that is used.<br>• The value of the interface-type specifies the interface on which the agent is connected to the server. |
| **Step 5** | **backup transport http ipv4** *ipv4-address* [**port** *port-number* ] [**source** *interface-type*]<br>**Example:**<br>`Device(config-pnp-init)# backup transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0` | Creates a backup HTTP transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed. |
| **Step 6** | **backup transport http ipv6** *ipv6-address* [**port** *port-number* ] [**source** *interface-type interface-number* ]<br>**Example:**<br>`Device(config-pnp-init)# backup transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1` | Creates a backup HTTP transport configuration for the PnP agent profile based on the IPv6 address of the server on which the PnP agent is deployed. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Backup Cisco Network Plug and Play HTTPS Transport Profile

Perform the following task to create a backup HTTPS transport profile of the Cisco Network Plug and Play agent manually on a device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp profile** *profile-name*<br>**Example:**<br>`Device(config)# pnp profile test-profile-1` | Creates a PnP agent profile and enters the PnP profile initialization mode.<br>• String of alphanumeric characters that specify a name for the PnP agent profile. Profile names cannot be duplicated. |
| **Step 4** | **backup transport https host** *host-name* [**port** *port-number* ][**source** *interface-type* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:**<br>`Device(config-pnp-init)# backup transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz` | Creates a HTTPS backup transport configuration for the PnP agent profile based on the hostname of the server on which the PnP agent is deployed.<br>• The value of *localcert* specifies the trustpoint used for client-side authentication during the transport layer security (TLS) handshake.<br>• The value of *remotecert* specifies the trustpoint used for server certificate validation. |
| **Step 5** | **backup transport https ipv4** *ipv4-address* [**port** *port-number* ][**source** *interface-type* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:**<br>`Device(config-pnp-init)# backup transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz` | Creates a HTTPS backup transport configuration for the PnP agent profile based on the IPv4 address of the server on which the PnP agent is deployed. |
| **Step 6** | **backup transport https ipv6** *ipv6-address* [**port** *port-number* ][**source** *interface-type interface-number* ][**localcert** *trustpoint-name* ][**remotecert** *trustpoint-name* ]<br>**Example:** | Creates a HTTPS backup transport configuration for the PnP agent profile based on the IPv6 address of the server on which the PnP agent is deployed. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-pnp-init)# backup transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz` | |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-pnp-init)# end` | Exits the PnP profile initialization mode and returns to privileged EXEC mode. |

# Configuring Cisco Network Plug and Play Agent Tag

Perform the following task to create a Cisco Network Plug and Play agent tag information:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **pnp tag** *tag-name*<br>**Example:**<br>`Device(config)# pnp tag xyz` | Use the **pnp tag** command to configure the tag for the device. The neighboring Cisco devices will receive this tag information through Cisco Discovery Protocol (CDP).<br>**Note** If there is an existing tag for the the PnP server to change the tag<br>• String of alphanumeric characters that specify a name for the PnP agent tag. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits the global configuration mode and returns to privileged EXEC mode. |

# Troubleshooting and Debugging

To run the debugging on the Cisco Network Plug and Play ( server, start the server, configure the PnP profile and PnP transport. For example, start the service interaction between PnP agent and PnP server.

You can capture the debugs by executing the **debug pnp service** command. When you report a problem, collect all the pnp* files in the PnP agent flash" to the guide.

**Note** To collect Cisco Plug and Play server log, see the Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide.

To troubleshoot the device, server and Cisco PnP Agent, use the following commands:

***Table 42: Troubleshooting the Device, Server, and Cisco PnP Agent***

| Command | Description |
|---|---|
| **dir nvram** | Use this command to ensure tht the device does not have left over certificates. |
| **ping vrf interface-name** *<controller_ip>* | Use this command to ensure the the device can ping the controller. |
| **show auto install trace** | Use this command to view auto install trace log. |
| **show boot** | Use the show boot command to display the current value for the BOOTLDR variable. |
| **show cdp neighbor** | Use this command to display all CDP neighbors. |
| **Show crypto pki trustpoint** | Use this command to view the PKI trustpoint. |
| **Show crypto pki trustful** | Use this command to view the PKI trustful. |
| **show ip interface brief** | Use this command to view a summary of the router interfaces. |
| **show ipv6 interface brief** | Use this command to display the IPv6 interfaces. |
| **show run \| inc pnp** | Uset this command to ensure that only one PnP profile installed |
| **show pnp trace** | Use this command to ensure that the device does not have start-up configuration. |
| **show pnp tech** | Use this command to view active connections for the Cisco Plug and Play IOS Agent. |
| **show vlan** | Use this command to view the VLAN information. |
| **show ntp status** | Use this command to view the NTP status. |

| Command | Description |
|---|---|
| **show version** | Use this command to ensure that the device is running the latest CCO image |

# Glossary

**PnP Agent**: An embedded agent on the device to automate deployment process

**PnP Helper Applications**: Applications on smart phones and personal computers that facilitate deployment. PnP helper applications are not specific to a customer or device and can be used in any deployment scenario. May be needed in limited scenarios

**PnP Protocol**: Protocol between the PnP agent and PnP server. This is an open protocol allowing third-party development of PnP servers

**PnP Server**: A central server that manages and distributes deployment information (images, configurations, files, and licenses) for the devices being deployed. Cisco Network Plug and Play server provides a north bound interface for management applications and communicates with the PnP agents on the devices using the PnP protocol.

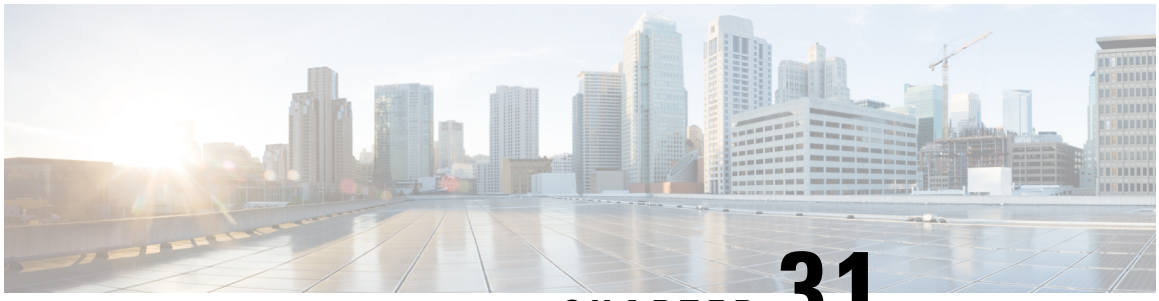
# Additional References for Open Plug-n-Play Agent

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| PnP commands: Complete command syntax, command mode, command history, defaults, usage guidelines, and examples | Cisco IOS PnP Command Reference |
| Cisco Network Plug and Play solution | Solution Guide for Cisco Network Plug and Play. |
| How to use the Cisco Network Plug and Play in the APIC-EM to configure Cisco network devices. | Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM. |
| How to deploy the APIC-EM. | Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide. |
| Getting started with the APIC-EM. | Cisco APIC-EM Quick Start Guide. |

### MIBs

| MIB | MIBs Link |
|---|---|
| • CISCO-BULK-FILE-MIB<br>• CISCO-DATA-COLLECTION-MIB<br>• CISCO-PROCESS-MIB<br>• Expression-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |



CHAPTER 31

# Troubleshooting

This reference outlines the standard procedures for diagnosing and correcting operational errors.


- Troubleshooting, on page 273
- Diagnostic mode, on page 273
- Recommendation: prepare information before contacting support, on page 274
- Show interfaces troubleshooting command, on page 274
- Software upgrade methods, on page 275
- Change the configuration register, on page 275
- Recover a lost password, on page 278


# Troubleshooting

This section describes the troubleshooting scenarios for the router.

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.

# Diagnostic mode

Diagnostic mode is a router operating mode that

- provides access to a subset of user EXEC mode commands for troubleshooting when the IOS process fails
- enables inspection of router states, configuration management, and process restart capabilities
- offers a more comprehensive troubleshooting interface than limited access methods like ROMMON.

### Diagnostic mode access scenarios

The router boots up or accesses diagnostic mode in these 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.

# Recommendation: prepare information before contacting support

If you cannot locate the source of a problem, contact your local reseller for advice. Prepare this information before you call:

- 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. describes messages in the command output.

The IR1800 supports these interfaces:

- GigabitEthernet 0/0/0 and 0/0/1
- Cellular 0/2/0, Cellular 0/2/1, Cellular 0/3/0, and Cellular 0/3/1
- msata

- WPAN 0/1/0

# Software upgrade methods

Software upgrade methods are techniques that

- copy new software images to flash memory over the WAN interface when the existing Cisco IOS software image is in use
- copy new software images over the console port while in ROM monitor mode, and
- boot the router from a software image loaded on a TFTP server from ROM monitor mode when the TFTP server is on the same network as the router.

# Change the configuration register

The configuration register controls various boot-time settings on Cisco routers. You may need to modify this register to enable break functionality or change other boot parameters.

Follow these steps to change the configuration register.

### Procedure

**Step 1** Connect a PC to the CONSOLE port on the router.

**Step 2** At the privileged EXEC prompt, use the **show version** command to display the existing configuration register value.

**Example:**

```
Router# show version
            Cisco IOS XE Software, Version
BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148
            Cisco IOS Software [Bengaluru], ISR Software
(ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M), Experimental Version 17.5.20210124:064309
[S2C-build-v175_throttle-507-/nobackup/mcpre/BLD-BLD_V175_THROTTLE_LATEST_20210124_063209
226]
            Copyright (c) 1986-2021 by Cisco Systems, Inc.
            Compiled Sun 24-Jan-21 06:10 by mcpre

            ROM: 1.4(REL)

            UUT3_Sec uptime is 17 hours, 37 minutes
            Uptime for this control processor is 17 hours, 38 minutes
            System returned to ROM by reload
            System image file is
"bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210124_063209_V17_5_0_148.SSA.bin"

            Last reload reason: Reload Command

            Technology Package License Information:

            ------------------------------------------------------------------
            Technology Type    Technology-package    Technology-package
```

```
Current              Next Reboot
------------------------------------------------------------
Smart License      Perpetual            network-advantage    network-advantage

Smart License      Subscription          None                 None

The current throughput level is 50000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco IR8140H-P-K9 (1RU) processor with 1948753K/6147K bytes of memory.
Processor board ID FDO2438J89L
Router operating mode: Autonomous
2 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8116912K bytes of physical memory.
8032254K bytes of Bootflash at bootflash:.

Configuration register is 0x2102

Router#
```

**Note** The configuration register value is shown at the bottom of the output (in this example, `Configuration register is 0x2102`).

**Step 3** Record the setting of the configuration register.

**Step 4** Use the **config-register** *value* command from privileged EXEC mode to enable or disable the break setting (indicated by the value of bit 8 in the configuration register).

**Note**

- Break enabled — Bit 8 is set to 0.
- Break disabled (default setting) — Bit 8 is set to 1.

The configuration register value is updated with the new setting, which takes effect after the next router reload.

# Configure the configuration register for autoboot

The configuration register controls how the router boots and can be used to change router behavior for advanced troubleshooting scenarios.

**Caution** Perform this configuration only with guidance from Cisco support, as altering the configuration register is intended for advanced troubleshooting purposes.

Follow these steps to configure the configuration register for autoboot.

### Procedure

**Step 1** Set the configuration register to 0x0 to boot into ROM, using one of the following methods.

a) In Cisco IOS configuration mode, use the **config-register 0x0** command.

**Example:**

```
Router(config)# config-register 0x0
```

b) From the ROMmon prompt, use the **confreg 0x0** command.

**Example:**

```
rommon> confreg 0x0
```

**Step 2** Use the **config-register 0x2102** command to set the router to autoboot the Cisco IOS XE software.

**Example:**

```
Router(config)# config-register 0x2102
```

The configuration register is set to control the router boot behavior as specified.

# Reset the router

Reset the router to restore factory defaults or recover from configuration issues by bypassing the current running configuration. Use this procedure when you need to reset a router to factory defaults or recover from a configuration that prevents normal operation. This process uses ROM monitor (ROMmon) mode to bypass the existing configuration.

Follow these steps to reset the router.

### Procedure

**Step 1** If the break is disabled, turn off the router, wait for 5 seconds, and turn the router back on. Within 60 seconds, push the Reset button.

The terminal displays the ROMmon prompt.

```
rommon 1>
```

**Step 2** Use the **confreg 0x2142** command to ignore the running configuration.

**Example:**

```
rommon 2> confreg 0x2142
```

**Step 3** (Optional) Use the **DEVICE_MANAGED_MODE=autonomous** command to set the device managed mode to autonomous.

**Example:**

```
rommon 3> DEVICE_MANAGED_MODE=autonomous
```

**Note** Do not configure this command unless the router is in controller mode and needs to be changed to autonomous mode.

**Step 4** Use the **sync** command to sync the configuration changes.

**Example:**

```
rommon 4> sync
```

**Step 5** Use the **reset** command to reset the router and apply the configuration register value.

**Example:**

```
rommon 5> reset
resetting...
```

**Note** The router reloads with the reset.

**Step 6** Use the **confreg** command to verify that the correct value (0x2142) was applied. When prompted to change the configuration, enter **n**.

**Example:**

```
rommon 1> confreg
            Configuration Summary
            (Virtual Configuration Register: 0x2142)
            enabled are:
            [ 0 ] console baud: 9600
            boot:...... image specified by the boot system commands
            do you wish to change the configuration? y/n [n]: n
```

**Step 7** Use the **boot** *filesystem:/image-name* command to boot the image with the configuration register value 0x2142.

**Example:**

```
rommon 2> boot
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210207_015223_V17_5_0_161.SSA.bin
```

The router resets and boots with the specified image, bypassing the previous running configuration. You can now reconfigure the device as needed.

# Recover a lost password

Use this task to regain access to your router when you have forgotten or lost the password.

**Note** Password recovery is possible only when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Follow these steps to recover a lost password.

### Procedure

**Step 1** Reset the router.

**Step 2** Change the configuration register to 0x2142.

**Step 3** Boot the router with the configuration register value 0x2142 from ROMmon.

**Step 4** If you used the Reset button, use the **configure terminal** and **license smart reservation** commands to add the license.

**Example:**

```
Router# configure terminal
Router(config)# license smart reservation
```

You have successfully recovered access to your router.

### What to do next

For additional reset details, see .

# Reset the configuration register value

Reset the configuration register value after password recovery or reconfiguration to restore normal device operation. Perform this task after you have recovered or reconfigured a password and need to restore the configuration register to its original value.

Follow these steps to reset the configuration register value after you have recovered or reconfigured a password.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 2** Use the **config-register** *value* command with the original configuration register value that you recorded.

**Example:**

```
Router(config)# config-register value
```

**Step 3** Use the **exit** command to exit configuration mode.

**Example:**

```
Router(config)# exit
```

**Note** To return to the configuration that was 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.

The configuration register is reset to its original value, and the router operates with the recovered password configuration.

# Configure a console port transport map

Configure a transport map to define policies for console port connections, including how connections wait for VTY lines and what banner messages are displayed to users. This task describes how to configure a transport map for a console port interface on the router.

Follow these steps to configure a console port transport map.

### Procedure

**Step 1** Use the **enable** command to enable privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Router# configure terminal
```

**Step 3** Use the **transport-map type console** *transport-map-name* command to create and name a transport map for handling console connections, and to enter transport map configuration mode.

**Example:**

```
Router(config)# transport-map type console consolehandler
```

**Step 4** Use the **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] command to specify how a console connection is handled using this transport map.

**Example:**

```
Router(config-tmap)# connection wait none
```

**Note**

- `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. Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.
- `none` — The console connection immediately enters diagnostic mode.

**Step 5** (Optional) Use the **banner** [**diagnostic** | **wait**] *banner-message* command to create a banner message that is seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.

**Example:**

```
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)#
```

**Note**
- `diagnostic` — Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
- `wait` — Creates a banner message seen by users waiting for the Cisco IOS VTY line to become available.
- *banner-message* — The banner message, which begins and ends with the same delimiting character.

**Step 6** Use the **exit** command to exit transport map configuration mode and re-enter global configuration mode.

**Example:**

```
Router(config-tmap)# exit
```

**Step 7** Use the **transport type console** *console-line-number* **input** *transport-map-name* command to apply the settings defined in the transport map to the console interface.

**Example:**

```
Router(config)# transport type console 0 input consolehandler
```

**Note** The *transport-map-name* for this command must match the *transport-map-name* defined in the `transport-map type console` command.

The transport map is configured and applied to the console port, defining how console connections are handled according to the specified policies.

# View console port, SSH, and telnet handling configurations

Use the console port, SSH, and Telnet handling configuration commands to view transport map configurations and current access policies for incoming connections. These commands help you verify connection handling settings and banner configurations.

### Commands

Use these 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.

**showtransport-map** [**all | name***transport-map-name*| **type**[**console** ]]

This command can be used either in user EXEC mode or privileged EXEC mode.

### Example

This 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

This 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 :
```

# Factory reset commands

Factory reset commands are network management utilities that:

- remove all customer-specific data on a router or switch that has been added
- erase configuration, log files, boot variables, core files, bootflash, nvram, rommon variables, licenses, and logs, and
- restore the platform to boot up as if new from the factory.

### Factory reset command details

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.

**Caution** Use of the factory reset command should not be done lightly. All customer configurations will be deleted and the platform will boot up as if new from the factory.

**Note** factory-reset all does not work if IOS-XE is running in controller mode. Please refer to SDWAN configuration information.

Boot sequence after factory reset includes booting the image and loading the configuration:

Booting the image:

- The bootloader attempts to boot "golden.bin" from the bootflash: partition
- If no "golden.bin" is present, then boot the first image.

Loading the configuration:

- IOS looks for "golden.cfg" file on nvram: partition and applies it upon booting.
- If no "golden.cfg" is present on nvram: then IOS looks for "golden.cfg" file on bootflash: partition and applies it upon booting.
- If no "golden.cfg" is present on bootflash: then configurations are erased and Software Configuration dialog is used.

Example: Factory reset command execution

```
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
```