Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide

First Published: 2021-07-09

Last Modified: 2024-10-10

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

© 2024 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.

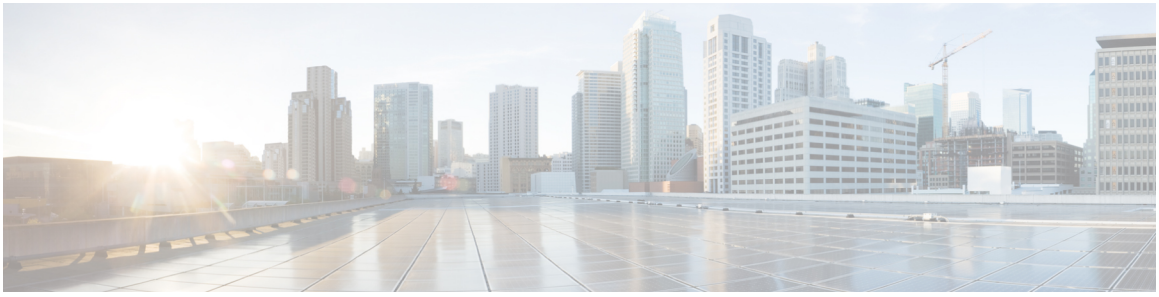
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

Introduction 1

Accessing the CLI Using a Router Console 2

Using the Console Interface 5

Initial Bootup Security 5

Enforce Changing Default Password 6

Telnet and HTTP 7

Accessing the CLI from a Remote Console 7

Preparing to Connect to the Router Console 7

Setting Up the IR8140H to Run SSH 8

Using Telnet to Access a Console Interface 9

CLI Session Management 10

Information About CLI Session Management 10

Changing the CLI Session Timeout 10

Locking a CLI Session 11

CHAPTER 2

New Features 13

New Features for Cisco IOS XE 17.15.1a 13

New Features for Cisco IOS XE 17.14.1a 13

New Features for Cisco IOS XE 17.8.1 13

Support IKEv2 for WPAN 13

Support High Availability for WPAN 13

Yang Model for WPAN 14

Yang Model for BBU 14
Yang Model for GPS 14
Itron CAM Module Support 14

CHAPTER 3 **Using Cisco IOS XE Software** 15
Understanding Command Modes 15
Keyboard Shortcuts 17
Using the no and default Forms of Commands 17
Using the History Buffer to Recall Commands 18
Managing Configuration Files 18
Saving Configuration Changes 18
Filtering Output from the show and more Commands 19
Finding Support Information for Platforms and Cisco Software Images 20
Using Cisco Feature Navigator 20
Getting Help 20
Finding Command Options: Example 21
Using Software Advisor 24
Using Software Release Notes 24

CHAPTER 4 **Basic Router Configuration** 25
IR8140H Interface Naming 25
Basic Configuration 26
Configuring Global Parameters 32
Configuring the Gigabit Ethernet Interface 33
Support for sub-interface on GigabitEthernet0/0/0 34
Configuring a Loopback Interface 34
Enabling Cisco Discovery Protocol 35
Configuring Command-Line Access 36
Configuring Static Routes 37
Configuring Dynamic Routes 39
Configuring Routing Information Protocol 39
Configuring Enhanced Interior Gateway Routing Protocol 40
Modular QoS (MQC) 40

CHAPTER 5 **Configuring Secure Shell** 43

Information About Secure Shell 43

Prerequisites for Configuring Secure Shell 43

Restrictions for Configuring Secure Shell 43

SSH And Router Access 44

SSH Servers, Integrated Clients, and Supported Versions 44

SSH Configuration Guidelines 45

How to Configure Secure Shell 45

Setting Up the IR8140H to Run SSH 45

Configuring the SSH Server 46

Monitoring the SSH Configuration and Status 48

Configuring the Router for Local Authentication and Authorization 48

Information about Secure Copy 49

Prerequisites for Secure Copy 50

Restrictions for Configuring Secure Copy 50

Configuring Secure Copy 50

Additional References 51

CHAPTER 6 **Installing the Software** 53

Installing the Software 53

Installing the Software 53

Cisco Software Licensing 53

Installing the Cisco IOS XE Release 54

ROMMON Images 56

File Systems 56

Autogenerated File Directories and Files 57

Flash Storage 57

Related Documentation 58

CHAPTER 7 **Software Maintenance Upgrade (SMU)** 59

Software Maintenance Upgrade (SMU) 59

SMU Workflow and Basic Requirements 59

SMU Example 60

Installing a Patch Image 60
Uninstalling the Patch Image 62
Uninstalling the Patch Image Using Rollback 63
Uninstalling the Patch Image Using Deactivate, Commit, and Remove 64

CHAPTER 8 **Smart Licensing Using Policy (SLP)** 67
SLP Overview 67
License Enforcement Types 67
SLP Architecture 68
Product Instance 68
Cisco Smart Software Manager (CSSM) 68
Cisco Smart Licensing Utility (CSLU) 69
Customer Topologies 69
License Installation Procedure - Full Offline Access Topology 70
Procedure to Register Product Instance in CSSM 70
Importing the ACK file from CSSM to your Device 73
Removing the Device from CSSM 74
License Installation Procedure - CSLU has No Access to CSSM 75
Procedure when devices are connected to the CSLU 76
Exporting the AuthRequest File to CSSM 80
Uploading the Authorization Request Code file into CSLU 85
License Installation Process in the Router 87

CHAPTER 9 **Battery Backup Unit (BBU)** 89
Battery Backup Unit Overview 89
Configuring BBU Mode 89
Enabling BBU 89
Disabling BBU 90
Reset BBU 91
Transportation Mode 92
Upgrade BBU 93

CHAPTER 10 **Tamper Detection** 97
Tamper Detection 97

CHAPTER 11 **Power Over Ethernet (PoE)** 99
Power over Ethernet 99
Device Detection and Power Allocation 99
Command Line Interface 99

CHAPTER 12 **12V DC Output for 3rd Party Device** 101
Enabling 12V DC Output 101

CHAPTER 13 **NTP Timing Based on GPS Clock** 103
Configuring NTP using GPS Time 103

CHAPTER 14 **vCPU and RAM Distribution** 105
Introduction 105
Distribution of vCPU and RAM Resources for Cisco IOx Applications 105
Higher CPU and RAM Allocation for IOx Applications 106
Configure Data Plane Heavy Template 106
Verify the Active vCPU and RAM Distribution 107
Configure Service Plane Heavy Template 107
Verify the Active vCPU and RAM Distribution 108

CHAPTER 15 **Cellular Pluggable Interface Module Configuration Guide** 109

CHAPTER 16 **Configuring Cisco Resilient Mesh and the WPAN Module** 111
Resilient Mesh and WPAN Module Overview 111
Configuring the WPAN Interface 112
Enabling dot1x, mesh-security and DHCPv6 112
Configuring IEEE154 Settings 113
Configuring Group Multicast 116
Configuring RPL 117
Configuring the Power Outage Server 119
Configuring Cisco Resilient Mesh Security 119
Configuring Mesh Key 119

Example Cisco Resilient Mesh Security Configuration 120
Verifying Cisco Resilient Mesh Security Configuration 121
Configuring the IPv6 Multicast Agent 122
Configuring IR8100 as PIM6 Router 124
Configuring DTLS Relay for EST 125
Configuring Wi-SUN Mode 125
Modulation and Data Rate (MDR) 127
Limited Function Node (LFN) 130
Direct Parenting of LFN Support in Wi-SUN Mesh Deployment 132
Verifying WPAN Configuration 133
Example IR8100 Basic WPAN Configuration 134
Example IR8100 Configuration for CG-Mesh 145
Example ASR Configuration for CG-Mesh 149
Checking and Upgrading the WPAN Firmware Version 154
Upgrading WPAN Firmware 155
Upgrading WPAN Firmware (CG-Mesh to WiSUN) 155

CHAPTER 17 **System Messages** 157
System Messages 157
Information About Process Management 157
How to Find Error Message Details 157

CHAPTER 18 **Environmental Monitoring** 163
Environmental Monitoring 163
Environmental Monitoring 163
Environmental Monitoring and Reporting Functions 163
Environmental Monitoring Functions 163
Environmental Reporting Functions 164
Additional References 173
Technical Assistance 174

CHAPTER 19 **IOx Application Hosting** 175
Application Hosting 175
Information About Application Hosting 175

Need for Application Hosting 175
IOx Overview 175
Cisco Application Hosting Overview 175
IOXMAN 176
Application Hosting on the IR8100 Industrial Integrated Services Router 176
VirtualPortGroup 177
vNIC 178
How to Configure Application Hosting 178
Enabling IOx 178
Configuring a VirtualPortGroup to a Layer 3 Data Port 180
Installing and Uninstalling Apps 183
Overriding the App Resource Configuration 184
Verifying the Application Hosting Configuration 186
Configuration Examples for Application Hosting 187
Example: Enabling IOx 187
Example: Configuring a VirtualPortGroup to a Layer 3 Data Port 187
Example: Installing and Uninstalling Apps 188
Example: Overriding the App Resource Configuration 188
Native docker support 188
Signed Application Support 189
Cisco Cyber Vision and Edge Intelligence 189

CHAPTER 20 **Cisco SD-WAN Support** 191
Cisco SD-WAN Overview 191
Related Documentation 192

CHAPTER 21 **ROM Monitor Overview** 193
ROM Monitor Overview and Basic Procedures 193
ROM Monitor Overview 193
Access ROM Monitor Mode 194
Checking the Current ROMMON Version 194
Commonly Used ROM Monitor Commands 195
Examples 195
Changing the ROM Monitor Prompt 196

Displaying the Configuration Register Setting 196
Environment Variable Settings 196
Frequently Used Environmental Variables 197
Displaying Environment Variable Settings 197
Entering Environment Variable Settings 197
Saving Environment Variable Settings 197
Exiting ROM Monitor Mode 197
Configuration Example 198
Upgrading the ROMmon for a Router 198

CHAPTER 22 **WAN Monitoring** 201
Information About WANMon 201
Built-in Recovery Actions 201
Prerequisites 202
Guidelines and Limitations 202
Configuring WANMon 202
Verifying WANMon Configuration 204
Configuration Examples 205
WANMon Cellular Interface Configuration Example 205
Multiple WAN Link Monitoring Example 205

CHAPTER 23 **Yang Data Models** 207
Support for YANG Data Models 207

CHAPTER 24 **Process Health Monitoring** 209
Process Health Monitoring 209
Monitoring Control Plane Resources 209
Avoiding Problems Through Regular Monitoring 209
Cisco IOS Process Resources 209
Overall Control Plane Resources 216
Monitoring Hardware Using Alarms 219
Router Design and Monitoring Hardware 219
BootFlash Disk Monitoring 219
Approaches for Monitoring Hardware Alarms 219

CHAPTER 25 **Troubleshooting** 221

Troubleshooting 221

Understanding Diagnostic Mode 221

Before Contacting Cisco or Your Reseller 222

show interfaces Troubleshooting Command 222

Software Upgrade Methods 222

Change the Configuration Register 223

Configuring the Configuration Register for Autoboot 224

Reset the Router 225

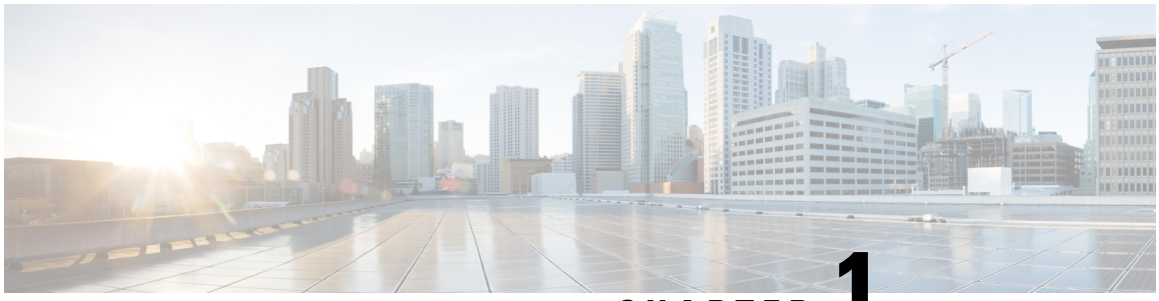
Recovering a Lost Password 226

Reset the Configuration Register Value 226

Configuring a Console Port Transport Map 227

Viewing Console Port, SSH, and Telnet Handling Configurations 229

Using the factory reset Commands 230



CHAPTER 1

Overview

- Introduction, on page 1
- Accessing the CLI Using a Router Console, on page 2
- Initial Bootup Security, on page 5
- Accessing the CLI from a Remote Console , on page 7
- CLI Session Management, on page 10

Introduction

The Cisco Catalyst IR8140 Heavy Duty Series Router (IR8140H) is the next generation modular IP 66/67 Industrial Router for outdoor use. There are two IR8140H models:

- IR8140H-P-K9 (PoE)
- IR8140H-K9 (Without PoE)

Note 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.

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

The IR8140H Series features 4 external module slots plus two onboard WAN ports and supports the following:

- 60W PSU
- GNSS onboard transceiver
- 900MHz WPAN – OFDM/FSK
- 4G/LTE IRMH modules

- mSATA module
- 1x 1Gbe SFP WAN
- 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)

Accessing the 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. The following is an example, and names and IP addresses are shown as examples.

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

```
--- 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 23:53:09.788: AUTOINSTALL: Obtain siaddr 192.168.0.2 (as config server)
*Jan 27 23:53:09.788: AUTOINSTALL: Setting hostname Router from DHCP reply
*Jan 27 23:53:10.899: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
administratively down
*Jan 27 23:53:11.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
 changed state to down
*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 23:53:29.883: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(1/3) by (pid=656, pname=PnP Agent Discovery, time=23:53:29 UTC Wed Jan 27 2021)
*Jan 27 23:53:30.893: %PNP-6-PNP_SUDI_UPDATE: Device SUDI [PID:IR8140H-P-K9,SN:FDO2438J8UN]
 identified
*Jan 27 23:53:30.893: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (1/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:53:30.894: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:53:35.635: %PNP-6-PNP_RELOAD_INFO_STOPPED: Reload reason (PnP Service Info
2408-Unknown reason) stopped by (profile=pnp_cco_profile, host=devicehelper.cisco.com.,
port=443)
*Jan 27 23:53:56.755: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(1/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
*Jan 27 23:54:07.900: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (1/10) by (pid=656, pname=PnP Agent Discovery, time=23:54:07
 UTC Wed Jan 27 2021)
*Jan 27 23:54:07.900: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(1/3) by (pid=656, pname=PnP Agent Discovery, time=23:54:07 UTC Wed Jan 27 2021)
*Jan 27 23:54:07.901: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:54:07.909: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:54:13.907: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (4/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:13 UTC Wed Jan
27 2021)
*Jan 27 23:54:13.907: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (5/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:13 UTC Wed Jan 27 2021)
*Jan 27 23:54:29.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (6/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:29 UTC Wed Jan
27 2021)
*Jan 27 23:54:29.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (7/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:29 UTC Wed Jan 27 2021)
*Jan 27 23:54:37.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (8/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:37 UTC Wed Jan
27 2021)
*Jan 27 23:54:37.911: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (9/10) on
(WPAN0/1/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:37 UTC Wed Jan 27 2021)
*Jan 27 23:54:53.914: %PNP-3-PNP_DOMAIN_NAME_NOT_FOUND: Domain name not found (10/10) on
(GigabitEthernet0/0/0) by (pid=656, pname=PnP Agent Discovery, time=23:54:53 UTC Wed Jan
27 2021)
*Jan 27 23:55:20.100: %PNP-6-PNP_CCO_SERVER_IP_RESOLVED: CCO server (devicehelper.cisco.com.)
 resolved to ip (18.205.166.131) by (pid=656, pname=PnP Agent Discovery, time=23:55:20 UTC
 Wed Jan 27 2021)
*Jan 27 23:55:20.100: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(2/3) by (pid=656, pname=PnP Agent Discovery, time=23:55:20 UTC Wed Jan 27 2021)
```

```
*Jan 27 23:55:21.107: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (2/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:55:21.108: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:55:32.751: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(2/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:55:43.108: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (2/10) by (pid=656, pname=PnP Agent Discovery, time=23:55:43
 UTC Wed Jan 27 2021)
*Jan 27 23:55:43.108: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(2/3) by (pid=656, pname=PnP Agent Discovery, time=23:55:43 UTC Wed Jan 27 2021)
*Jan 27 23:55:43.109: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:55:43.113: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:56:55.316: %PNP-6-PNP_PROFILE_CREATED: PnP profile (pnp_cco_profile) created
(3/3) by (pid=656, pname=PnP Agent Discovery, time=23:56:55 UTC Wed Jan 27 2021)
*Jan 27 23:56:56.323: %PNP-6-PNP_RELOAD_INFO_ENCODED: Reload reason (PnP Service Info
2408-Unknown reason) encoded (3/3) by (pid=656, pname=PnP Agent Discovery)
*Jan 27 23:56:56.324: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

*Jan 27 23:57:09.810: AUTOINSTALL: script execution not successful for Gi0/0/0.
*Jan 27 23:57:10.829: %SYS-5-CONFIG_P: Configured programmatically by process DHCP Autoinstall
 from console as vty0
*Jan 27 23:58:10.003: %PNP-6-PNP_BACKOFF_NOW: PnP Backoff now for (60) seconds requested
(3/3) by (profile=pnp_cco_profile, host=devicehelper.cisco.com., port=443)
*Jan 27 23:58:21.323: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (3/10) by (pid=656, pname=PnP Agent Discovery, time=23:58:21
 UTC Wed Jan 27 2021)
*Jan 27 23:58:21.323: %PNP-6-PNP_PROFILE_DELETED: PnP profile (pnp_cco_profile) deleted
(3/3) by (pid=656, pname=PnP Agent Discovery, time=23:58:21 UTC Wed Jan 27 2021)
*Jan 27 23:58:21.324: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:58:21.327: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:59:34.507: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:59:59.507: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (4/10) by (pid=656, pname=PnP Agent Discovery, time=23:59:59
 UTC Wed Jan 27 2021)
*Jan 27 23:59:59.508: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 27 23:59:59.511: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:01:12.715: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:22.715: %PNP-3-PNP_CCO_PROFILE_UNCONFIGURED: CCO Server profile
(pnp_cco_profile) unconfigured (5/10) by (pid=656, pname=PnP Agent Discovery, time=00:02:22
 UTC Thu Jan 28 2021)
*Jan 28 00:02:22.716: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
```

```
Discovery from console as vty0
*Jan 28 00:02:22.719: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
Router>en
Router#sh ip in
*Jan 28 00:02:42.724: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as console
*Jan 28 00:02:42.724: %PNP-6-PNP_SAVING_TECH_SUMMARY: Saving PnP tech summary
(/pnp-tech/pnp-tech-discovery-summary)... Please wait. Do not interrupt.t b
*Jan 28 00:02:42.877: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:42.924: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:43.394: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0
*Jan 28 00:02:43.494: %PNP-6-PNP_TECH_SUMMARY_SAVED_OK: PnP tech summary
(/pnp-tech/pnp-tech-discovery-summary) saved successfully (elapsed time: 1 seconds).
*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#
```

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

Using the Console Interface

Procedure

Step 1 Enter the following command:

```
Router > enable
```

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

```
Password: enablepass
```

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

```
Router#
```

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

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

```
Router# quit
```

Initial Bootup Security

This section contains the following:

Enforce Changing Default Password

When the device is first booted after factory reset or fresh from the factory, the following prompt is received on the console:

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

In previous documentation, Cisco recommended using the **enable secret** command instead of the **enable password** command because this offers an improved encryption algorithm.

The initial dialog forces setting a new enable password, and also using the **enable secret** command instead. The following is an example:

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

Autoinstall trying DHCP on GigabitEthernet0/0/0
Autoinstall trying DHCPv6 on GigabitEthernet0/0/0

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: **********

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!
*Feb 12 00:14:14.305: %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to
administratively down
*Feb 12 00:14:14.308: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
administratively down
*Feb 12 00:14:15.306: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to down
Router>
*Feb 12 00:14:15.653: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: SLA-TrustPoint created succesfully
*Feb 12 00:14:15.657: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM[OK]
Router>
Router>en
Password:
*Feb 12 00:14:18.878: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
```

```
 file
*Feb 12 00:14:18.910: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
Router#sh run | inc sec
*Feb 12 00:14:26.299: %SYS-5-CONFIG_P: Configured programmatically by process PnP Agent
Discovery from console as vty0ret
enable secret 9 $9$rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPhKZeKJsEe./CPEzl.
Router#
```

After the enable secret is prompted during the first login, and the admin enters a password, the admin entered password will be always masked. If the admin enters a weak password, they will be prompted again to enter strong password (i.e. the standard mix of upper/lower case characters, special characters, numbers etc.). The prompting will continue until the admin enters a strong password. The admin will be prompted to enter the strong secret password twice for confirming that admin is sure that it is the secret that they want to configure.

Telnet and HTTP

There has been a change in the telnet and http boot configuration as of release 17.5.1. When the device is first booted after factory reset or fresh from the factory, the following takes place:

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

Accessing the CLI from a Remote Console

The remote console of the IR8100H can be accessed through Telnet or SSH. Telnet is disabled by default, and the more secure SSH should be used. For details on SSH access see the SSH chapter.

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

Preparing to Connect to the Router Console

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

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

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

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

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

If you are using authentication, authorization, and accounting (AAA), configure the **login authentication** command. To prevent disabling login on a line for AAA authentication when you configure a list with the

login authentication command, you must also configure that list using the **aaa authentication login** global configuration command.

For more information about AAA services, see the Cisco IOS XE Security Configuration Guide: Secure Connectivity and the Cisco IOS Security Command Reference documents. For more information about the **login line-configuration** command, see the Cisco IOS Terminal Services Command Reference document.

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

Setting Up the IR8140H to Run SSH

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Router(config)# hostname your_hostname`	Configures a hostname and IP domain name for your device. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 3	**ip domain-name** *domain_name* **Example:** `Router(config)# ip domain-name your_domain_name`	Configures a host domain for your device.
Step 4	**crypto key generate rsa** **Example:** `Router(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer

	Command or Action	Purpose
		modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Using Telnet to Access a Console Interface

Procedure

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

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

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

The following example shows how to use the **telnet** command to connect to a router named **router**:

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

Step 2 Enter your login password:

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

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

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

```
Router> enable
```

Step 4 At the password prompt, enter your system password:

```
Password: enablepass
```

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

```
Router#
```

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

Step 7 To exit the Telnet session, use the **exit** or **logout** command.

```
Router# logout
```

CLI Session Management

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

Information About CLI Session Management

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

Changing the CLI Session Timeout

Procedure

Step 1 **configure terminal**

Enters global configuration mode

Step 2 **line console 0**

Step 3 **session-timeout** *minutes*

The value of *minutes* sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for *minutes* to disable session timeout.

Step 4 **show line console 0**

Verifies the value to which the session timeout has been set, which is shown as the value for `" Idle Session "`.

Locking a CLI Session

Before you begin

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

Procedure

Step 1 `Router# configure terminal`

Enters global configuration mode.

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

`Router(config)# line console 0`

Step 3 `Router(config)# lockable`

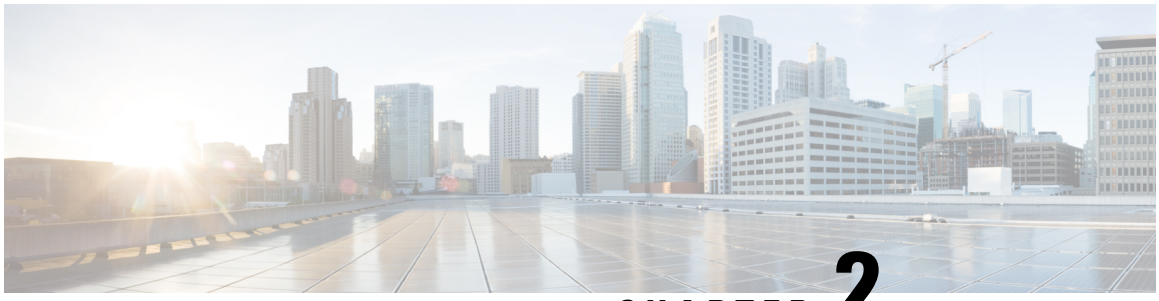
Enables the line to be locked.

Step 4 `Router(config)# exit`

Step 5 `Router# lock`

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

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



CHAPTER 2

New Features

- New Features for Cisco IOS XE 17.15.1a, on page 13
- New Features for Cisco IOS XE 17.14.1a, on page 13
- New Features for Cisco IOS XE 17.8.1, on page 13

New Features for Cisco IOS XE 17.15.1a

New features in this release are listed below:

- Higher CPU and RAM Allocation for IOx Applications

New Features for Cisco IOS XE 17.14.1a

New features in this release are listed below:

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

New Features for Cisco IOS XE 17.8.1

Support IKEv2 for WPAN

The IR8140H supports IKEv2 dynamic routing from Cisco IOS-XE Release 17.8.1. The router can redistribute WPAN external routes (for example, Mapping of Address and Port-Translation Mode (MAP-T) routes) into IKEv2 and supports spoke and hub distribution.

Support High Availability for WPAN

The IR8140H will now support High Availability for WPAN between two routers (each with one WPAN module). WPAN HA uses HSRP to track state between the two routers. The WPAN state (RPL routes, mesh-security sessions and keys, multicast sequence numbers) is synchronized between the two routers using a reliable UDP based protocol.

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

Yang operational model support has been added for the information that is currently available through WPAN show commands. This includes commands for the following:

- 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

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**.

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 GPS

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:

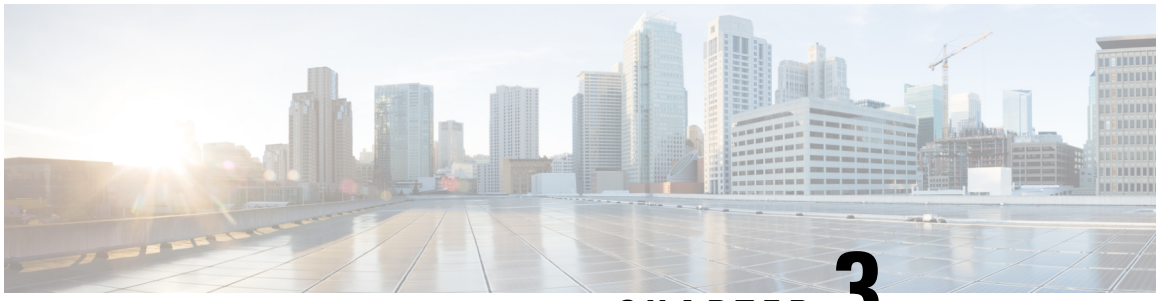
https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

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

Itron CAM Module Support

The IR8140H 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

- Understanding Command Modes, on page 15
- Keyboard Shortcuts, on page 17
- Using the no and default Forms of Commands, on page 17
- Using the History Buffer to Recall Commands, on page 18
- Managing Configuration Files, on page 18
- Saving Configuration Changes, on page 18
- Filtering Output from the show and more Commands, on page 19
- Finding Support Information for Platforms and Cisco Software Images, on page 20

Understanding Command Modes

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

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

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

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

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

Table 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 terminal** command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.
Diagnostic	The router boots up or accesses diagnostic mode in the following scenarios: • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload. • A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) is entered and the router is configured to go to diagnostic mode when the break signal is received.	`Router(diag)#`	If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI.

Command Mode	Access Method	Prompt	Exit Method
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon#>`	To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

Keyboard Shortcuts

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

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

Table 2: Keyboard Shortcuts

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

Using the no and default Forms of Commands

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

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

Using the History Buffer to Recall Commands

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

The following table lists the history substitution commands.

Table 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.

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

Managing Configuration Files

The startup configuration file is stored in the nvram: file system and the running configuration files are stored in the system: file system. This configuration file storage setup is also used on several other Cisco router platforms.

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

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

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

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

Saving Configuration Changes

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

```
Router# copy running-config startup-config
Destination filename [startup-config]? enter
```

```
Building configuration...
[OK]
IR1101#
*Sep 24 08:50:26.666: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
 file
```

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

This task saves the configuration to the NVRAM.

Filtering Output from the show and more Commands

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

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

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

The output matches certain lines of information in the configuration file.

Example

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

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is 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
```

Finding Support Information for Platforms and Cisco Software Images

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

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

The group of feature sets that are available for a specific platform depends on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or see the https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/series.html.

Using Cisco Feature Navigator

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

Getting Help

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

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

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

Finding Command Options: Example

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

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

The following table shows examples of using the question mark (**?**) to assist you in entering commands.

Table 4: Finding Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a " # " from the " > ", for example, `Router>` to `Router#`

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router (config)#`

`Router(config)# interface GigabitEthernet ?`
`<0-0> GigabitEthernet interface number`
 	
`Router(config)# interface GigabitEthernet 0/?`
`<0-0> Port Adapter number`
 	
`Router (config)# interface GigabitEthernet 0/0/?`
`<0-1> GigabitEthernet interface number`
 	
`Router (config)# interface GigabitEthernet 0/0/0?`
`.  <0-1>`
 	
`Router(config-if)#`
	Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.
	Enter **?** to display what you must enter next on the command line.
	When the <cr> symbol is displayed, you can press **Enter** to complete the command.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol`
`  config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation`
`  for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an`
`  interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list`
`  or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	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 ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  bandwidth-percent  Set EIGRP bandwidth limit`
`  broadcast-address  Set the broadcast address of an interface`
`  cgmp  Enable/disable CGMP`
`  directed-broadcast  Enable forwarding of directed broadcasts`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  helper-address  Specify a destination address for UDP broadcasts`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	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 ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	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.
	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 ?`
`  A.B.C.D  IP subnet mask`
`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.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.
	<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 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`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.
	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**.
	<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` `Router(config-if)#`	Press **Enter** to complete the command.

Using Software Advisor

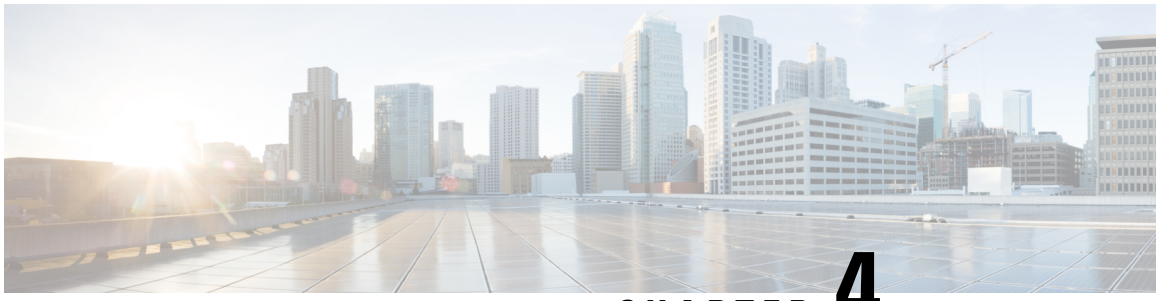
Cisco maintains the Software Advisor tool. See Tools and Resources. Use the Software Advisor tool to see if a feature is supported in a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router. You must be a registered user on Cisco.com to access this tool.

Using Software Release Notes

See the release notes for information about the following:

- 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, refer to the Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.



CHAPTER 4

Basic Router Configuration

This chapter contains the following sections:

- IR8140H Interface Naming, on page 25
- Basic Configuration, on page 26
- Configuring Global Parameters, on page 32
- Configuring the Gigabit Ethernet Interface, on page 33
- Support for sub-interface on GigabitEthernet0/0/0, on page 34
- Configuring a Loopback Interface, on page 34
- Enabling Cisco Discovery Protocol, on page 35
- Configuring Command-Line Access, on page 36
- Configuring Static Routes, on page 37
- Configuring Dynamic Routes, on page 39
- Modular QoS (MQC), on page 40

IR8140H Interface Naming

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

Hardware Interface	Naming Convention
Gigabit Ethernet ports	GigabitEthernet0/0/0 GigabitEthernet0/0/1
Cellular Interface	Cellular0/2/0 Cellular0/2/1 Cellular0/3/0 Cellular0/3/1
mSATA SSD	msata
GPIO	alarm contact 1-2
WPAN	Wpan0/1/0

Basic Configuration

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

```
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
```

Configuring Global Parameters

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

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode when using the console port.
		Use the following to connect to the router with a remote terminal:
		`telnet router-name or address`
		`Login: login-id`
		`Password: *********`
		`Router> enable`

Step 2	**hostname** *name* **Example:** `Router(config)# hostname Router`	Specifies the name for the router.
Step 3	**enable password** *password* or **enable secret password** *password* **Example:** `Router(config)# enable password cr1ny5ho`	Specifies a password to prevent unauthorized access to the router. **Note** In this form of the command, password is not encrypted. To encrypt the password use enable secret password as noted in the previously mentioned Device Hardening Guide.

Configuring the 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

	Command or Action	Purpose
Step 1	**configure terminal**	

Step 2	**ipv6 unicast-routing**
	Example:
	`Router#configure terminal`
	`Router(config)# ipv6 unicast-routing`
		Enables forwarding of IPv6 unicast data packets.

Step 3	**interface GigabitEthernet** *slot/bay/port* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Enters the configuration mode for an interface on the router.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.
Step 5	**ipv6 address** *ipv6-address/prefix* **Example:** `Router(config-if)# ipv6 address 2001.db8::ffff:1/128`	Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address. IPv6 unicast-routing needs to be set-up as well, see further information in the **IPv6 Addressing and Basic Connectivity Configuration Guide** located here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html
Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface and changes its state from administratively down to administratively up.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits the configuration mode of interface and returns to the global configuration mode.

Support for sub-interface on GigabitEthernet0/0/0

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

```
Router(config)#interface g0/0/0.?
  <1-4294967295>  GigabitEthernet interface number
Router(config-subif)#encapsulation ?
  dot1Q            IEEE 802.1Q Virtual LAN
```

Configuring a Loopback Interface

Before you begin

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

To configure a loopback interface, follow these steps.

Procedure

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

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the loopback interface and returns to global configuration mode.

Example

Verifying Loopback Interface Configuration

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

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

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

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

Enabling Cisco Discovery Protocol

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

For more information on using CDP, see Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S.

Configuring Command-Line Access

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

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

Procedure

	Command or Action	Purpose
Step 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **Example:** `Router(config)# line console 0`	Enters line configuration mode, and specifies the type of line. The example provided here specifies a console terminal for access.
Step 2	**password** *password* **Example:** `Router(config-line)# password 5dr4Hepw3`	Specifies a unique password for the console terminal line.
Step 3	**login** **Example:** `Router(config-line)# login`	Enables password checking at terminal session login.

Step 4	**exec-timeout** *minutes* [*seconds*]
	Example:
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		Sets the interval during which the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, adds seconds to the interval value.
		The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of **0 0** specifies never to time out.

Step 5	**exit** **Example:** `Router(config-line)# exit`	Exits line configuration mode to re-enter global configuration mode.

Step 6	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	Example:
	`Router(config)# line vty 0 4`
	`Router(config-line)#`
		Specifies a virtual terminal for remote console access.

Step 7	**password** *password* **Example:**	Specifies a unique password for the virtual terminal line.

	Command or Action	Purpose
	`Router(config-line)# password aldf2ad1`	
Step 8	**login** **Example:** `Router(config-line)# login`	Enables password checking at the virtual terminal session login.
Step 9	**end** **Example:** `Router(config-line)# end`	Exits line configuration mode, and returns to privileged EXEC mode.

Example

The following configuration shows the command-line access commands. Note that 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**. These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

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

Configuring Static Routes

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

To configure static routes, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	(Option 1) **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **Example:**	Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the **ipv6 route** command described below.)

	Command or Action	Purpose
	`Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2`	
Step 2	(Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} **Example:** `Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0`	Specifies a static route for the IP packets. See additional information for IPv6 here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html
Step 3	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

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

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

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

Verifying Configuration

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

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

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, GigabitEthernet0
```

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

```
Router# show ipv6 route
```

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

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

Configuring Dynamic Routes

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

All of the Cisco IOS-XE configuration guides can be found here: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-amsterdam-17-3-1/model.html

Configuring Routing Information Protocol

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

Procedure

	Command or Action	Purpose
Step 1	**router rip** **Example:** `Router(config)# router rip`	Enters router configuration mode, and enables RIP on the router.
Step 2	**version** {**1** | **2**} **Example:** `Router(config-router)# version 2`	Specifies use of RIP version 1 or 2.

Step 3	**network** *ip-address*
	Example:
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
		Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.

Step 4	**no auto-summary** **Example:**	Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.

	Command or Action	Purpose
	`Router(config-router)# no auto-summary`	
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode, and enters privileged EXEC mode.

Example

Verifying Configuration

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

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

Gateway of last resort is not set

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

Configuring Enhanced Interior Gateway Routing Protocol

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

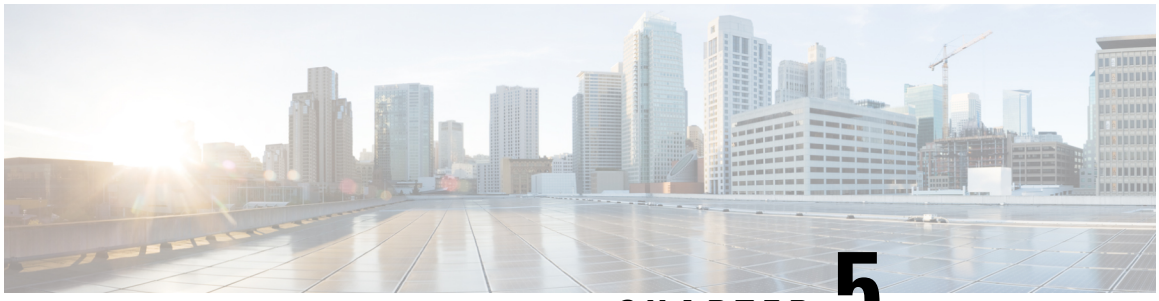
The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by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

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

Modular QoS (MQC)

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

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



CHAPTER 5

Configuring Secure Shell

This section contains the following topics:

- Information About Secure Shell , on page 43
- How to Configure Secure Shell, on page 45
- Information about Secure Copy, on page 49
- Additional References, on page 51

Information About Secure Shell

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

Prerequisites for Configuring Secure Shell

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

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

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the 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.

Note Cisco highly recommends the 3DES encryption as it is stronger.

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

- This software release supports IP Security (IPSec).
- The 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.

SSH And Router Access

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

SSH Servers, Integrated Clients, and Supported Versions

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

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

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

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

- TACACS+
- RADIUS
- Local authentication and authorization

SSH Configuration Guidelines

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

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

How to Configure Secure Shell

Setting Up the IR8140H to Run SSH

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**hostname** *hostname* **Example:** `Router(config)# hostname your_hostname`	Configures a hostname and IP domain name for your device. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 3	**ip domain-name** *domain_name* **Example:** `Router(config)# ip domain-name`	Configures a host domain for your device.

	Command or Action	Purpose
	your_domain_name	
Step 4	**crypto key generate rsa** **Example:** `Router(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the device as an SSH server.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring the SSH Server

Follow these steps to configure the SSH server:

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `IR8100# configure terminal`	Enters global configuration mode.
Step 2	**ip ssh version** [2] **Example:** `IR8100(config)# ip ssh version 2`	(Optional) Configures the device to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client.

	Command or Action	Purpose
		For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

Step 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
	Example:
	`IR8100(config)# ip ssh timeout 90`
	`ip ssh authentication-retries 2`
		Configures the SSH control parameters:
		• 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 when configuring both parameters.

Step 4	Use one or both of the following:
	• **line vty** *line_number* [*ending line number*]
	• **transport input ssh**
	Example:
	`IR8100(config)# line vty 1 10`
	or
	`IR8100(config-line)# transport input ssh`
		(Optional) Configures 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	**end** **Example:** `IR8100(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.

Monitoring the SSH Configuration and Status

Table 5: Commands for Displaying the SSH Server Configuration and Status

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

Configuring the Router for Local Authentication and Authorization

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

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

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `IR8100# configure terminal`	Enters global configuration mode.
Step 2	aaa new-model **Example:** `IR8100(config)# aaa new-model`	Enables AAA
Step 3	aaa authentication login default local **Example:** `IR8100(config)# aaa authentication login default local`	Sets the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports.

	Command or Action	Purpose
Step 4	aaa authorization exec local **Example:** `IR8100(config-line)# aaa authorization exec local`	Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.
Step 5	aaa authorization network local **Example:** `IR8100(config-line)# aaa authorization network local`	Configures user AAA authorization for all network-related service requests.
Step 6	**username** *name* **privilege** *level* **password** *encryption-type password* **Example:** `IR8100(config-line)# username your_user_name privilege 1 password 7 secret567`	Enters the local database, and establishes a username-based authentication system. 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	**end** **Example:** `IR8100(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.

Information about Secure Copy

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

Prerequisites for Secure Copy

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

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

Restrictions for Configuring Secure Copy

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

Configuring Secure Copy

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Sets AAA authentication at login.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Enables the AAA access control system.

	Command or Action	Purpose
	Example: `Device(config)# aaa authentication login default group tacacs+`	
Step 5	**username** *name* [**privilege** *level*] **password** *encryption-type encrypted-password* **Example:** `Device(config)# username superuser privilege 2 password 0 superpassword`	Establishes a username-based authentication system. **Note** You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.
Step 6	**ip scp server enable** **Example:** `Device(config)# ip scp server enable`	Enables SCP server-side functionality.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	**show running-config** **Example:** `Device# show running-config`	(Optional) Displays the SCP server-side functionality.
Step 9	**debug ip scp** **Example:** `Device# debug ip scp`	(Optional) Troubleshoots SCP authentication problems.

Example

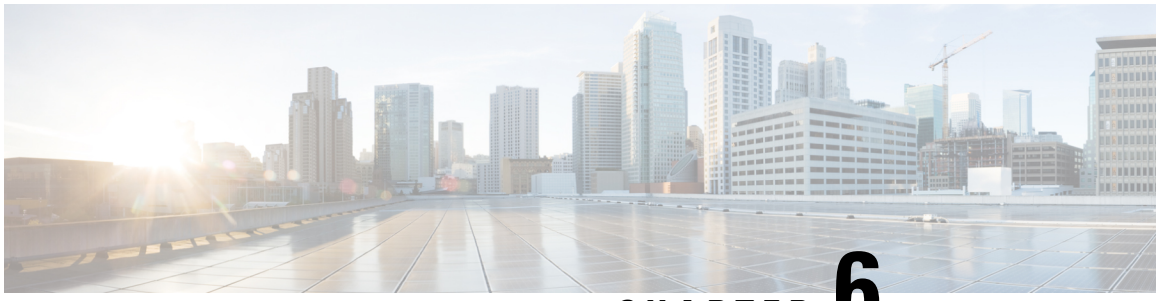
IR8100# **copy scp <*somefile*> your_username@remotehost:/<*some/remote/directory*>**

Additional References

The following sections provide references related to the SSH feature.

Related Topic	Document Title
Configuring Identity Control policies and Identity Service templates for Session Aware networking.	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE: https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf

Related Topic	Document Title
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

Installing the Software

This chapter contains the following sections:

- Installing the Software, on page 53

Installing the Software

This chapter contains the following sections:

Installing the Software

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

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

Cisco Software Licensing

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

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

The IR8100 uses Smart Licensing Using Policy (SLP), which is discussed in detail in Smart Licensing Using Policy (SLP), on page 67.

Consolidated Packages

To obtain software images for the router, go to: https://software.cisco.com/download/home/286200112

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.

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

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

- Network-Essentials
- Network-Advantage

Note Details of the Network-Essentials and Network-Advantage contents can be found in the IR8100 product data sheet.

Network-Essentials

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

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

Network-Advantage

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

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

Related Documentation

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

Installing the Cisco IOS XE Release

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

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

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

```
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#
*Nov  7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
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
Router#

Router#show run | inc license
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2441J91D
license boot level network-advantage
Router#
Router#reload ?
  /noverify  Don't verify file signature before reload.
  /verify    Verify file signature before reload.
  at         Reload at a specific time/date
  cancel     Cancel pending reload
  in         Reload after a time interval
  pause      Pause during reload
  reason     Reload reason
  <cr>       <cr>

Router#reload /verify

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 Images

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

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

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

File Systems

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

Table 6: Router File Systems

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 above.
msata:	Directory or Filename
null:	Directory or Filename
nvram:	Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.
system:	System memory file system, which includes the running configuration.
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 table above.

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 7: Autogenerated Files

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

Important Notes 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

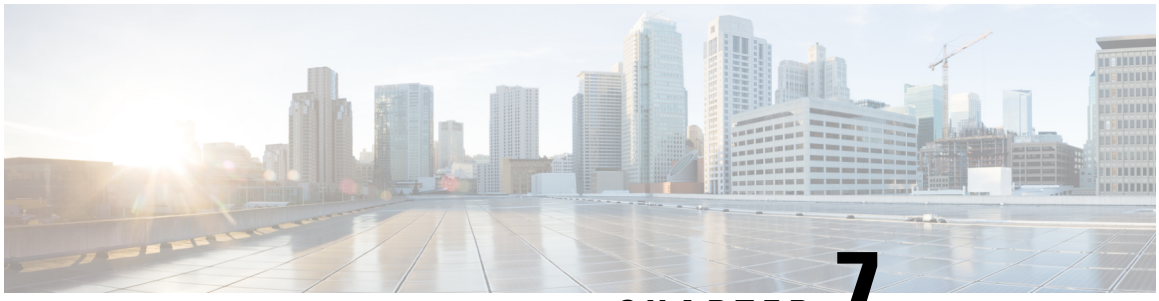
Subpackages are installed to local media storage, such as flash. For flash storage, use the **dir bootflash:** command to list the file names.

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

Related Documentation

For further 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 (SMU)

- Software Maintenance Upgrade (SMU), on page 59

Software Maintenance Upgrade (SMU)

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.

Some of the caveats of the SMU are:

- Provided on a per release, per component basis and is 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 then automatically integrated into the upcoming maintenance releases.
- The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install non-compatible SMUs. This is based on rules/limitations for a SMU change-set.
- An SMU provides a significant benefit over classic IOS software as it allows you to address the network issue quickly while reducing the time and scope of the testing required.
- 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 maintenance release X.1
- SMU is NOT an upgrade path from release X to release Y

The device only supports “Hot Patching”. This means:

- 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 where the patch redirects the program run

SMU Workflow and Basic Requirements

The workflow for the patch requires that you complete the following sequence of operation 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.

SMU Example

This section shows 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.

Installing a Patch Image

Perform the following steps to install the patch image:

Procedure

Step 1 Show a standard command.

```
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 Watts
Router#
```

Step 2 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 3 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:975352C1562A492D582D09D5BB91230863F6CC18E6F9C0EB512AF27CC0C77E2C05F29596AD34AD7808C9B39EC23D4412F0D3AFA707BC906FE03D554A845E42D4
/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 4 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 5 Show the status summary of the installation procedure.

```
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 6 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#
```

Uninstalling the Patch Image

There are two methods to remove or uninstall the patch image.

- Restoring the image to its original version by using the following command:
  - **install rollback to base**
- Specific removal of a patch by using the following commands in sequence:
  - **install deactivate file flash:**<*file*>
  - **install commit**
  - **install remove file flash:**<*file*>

Uninstalling the Patch Image Using Rollback

This section shows an example of using the rollback method.

Show what patches are installed:

```
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#
```

The following commands are available:

```
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
```

The **install rollback to base** command removes the entire patch and returns to the base image version with the found defect.

```
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#
```

Show what patches are installed:

```
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.

Verify the result of the patch by showing the same command.

```
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#
```

Uninstalling the Patch Image Using Deactivate, Commit, and Remove

In the following sequence, there are two patches installed on the device: CSCvq11111 and CSCvt22222. Only CSCvt22222 will be removed.

Show what patches are installed.

```
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
```

Procedure

Step 1 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
```

Show what patches are installed:

```
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 2 Commit the action.

```
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
```

Show what patches are installed:

```
Router# show install summary
```

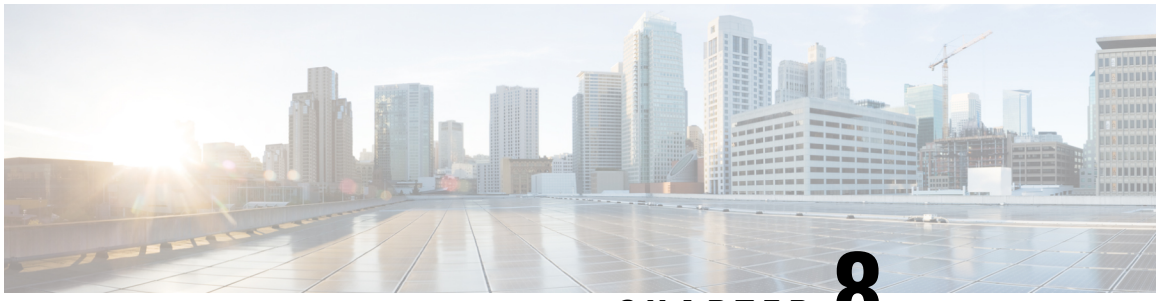
```
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir8100-universalk9.<release>.CSCvt11111.SPA.smu.bin
SMU   I    /flash1/ir8100-universalk9.<release>.CSCvt22222.SPA.smu.bin
IMG   C    <release>
```

Step 3 Remove the patch.

```
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:

```
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
IMG   C    <release>
```



CHAPTER 8

Smart Licensing Using Policy (SLP)

- SLP Overview, on page 67
- Customer Topologies, on page 69
- License Installation Procedure - Full Offline Access Topology, on page 70
- License Installation Procedure - CSLU has No Access to CSSM, on page 75

SLP Overview

Smart Licensing Using Policy (SLP), was previously referred to as Smart Licensing Enhanced (SLE), and is the default mode starting with IOS-XE release 17.3.2. SLE replaced Smart Software Licensing. The IR8140H only supports SLP. Some of the feature differences are:

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

License Enforcement Types

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

- Unenforced or Not Enforced

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

- Enforced

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

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

- Export-Controlled

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

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

SLP Architecture

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

Product Instance

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

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

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

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

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

Cisco Smart Software Manager (CSSM)

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

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

In CSSM you can:

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

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

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

Click on the **View Video** button.

Cisco Smart Licensing Utility (CSLU)

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

This utility performs the following key functions:

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

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

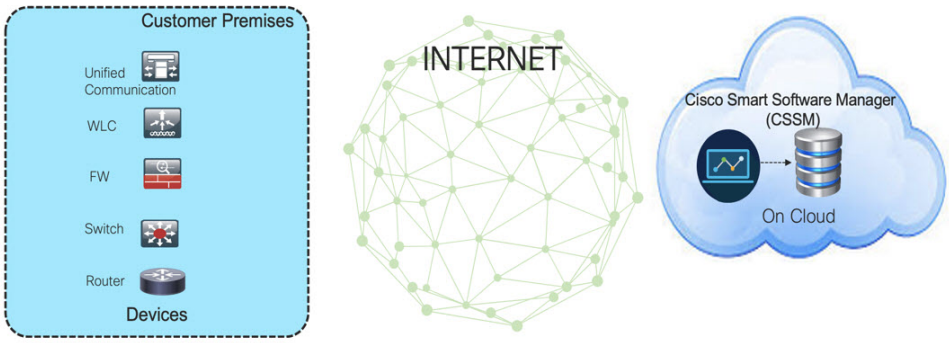
- Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.
- Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited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

Customer Topologies

IoT Routing platforms use two different topologies.

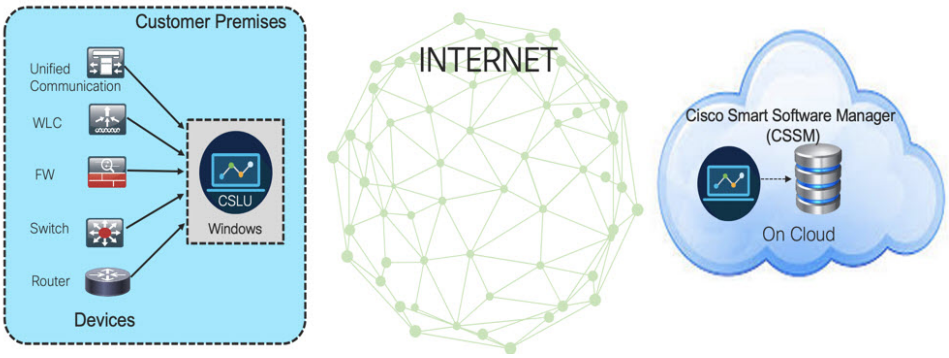
- Full Offline Access
- CSLU has No Access to CSSM

The following figure illustrates the Full Offline Access:



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

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



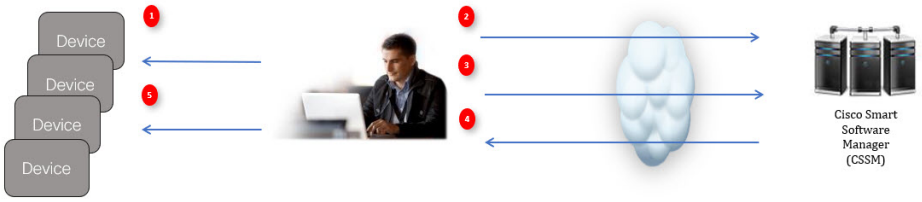
In this topology the devices are connected to the CSLU controller, but there is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com).

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

License Installation Procedure - Full Offline Access Topology

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

Refer to the following graphic for the flow of information:



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

Procedure to Register Product Instance in CSSM

Procedure

Step 1 Generate a license usage file from the Router.

In exec mode, perform the following:

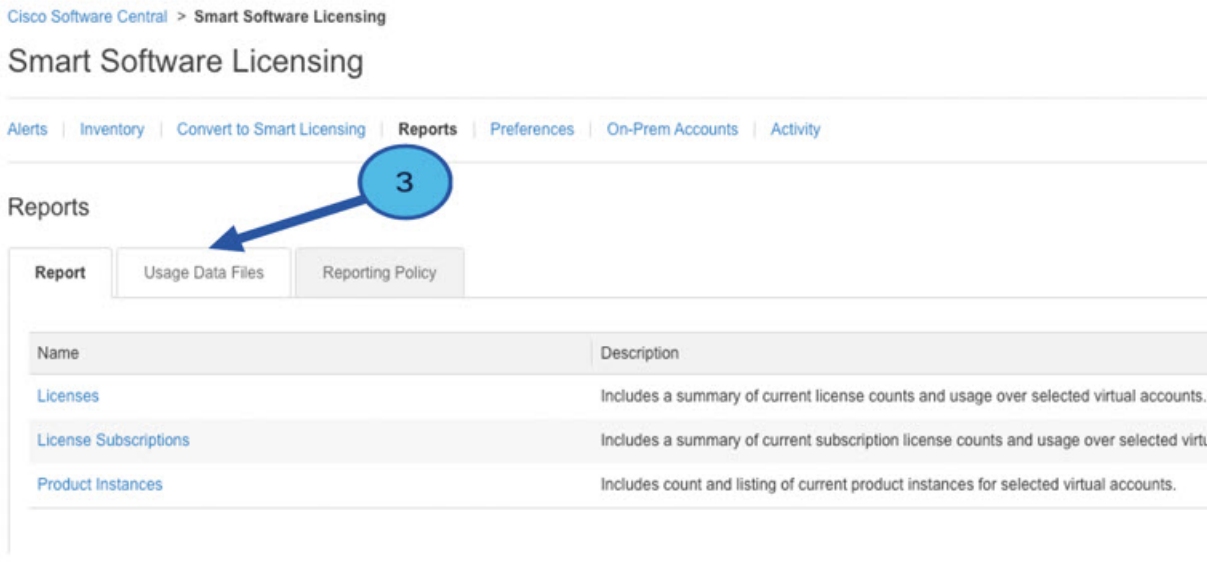
Example:

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

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

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

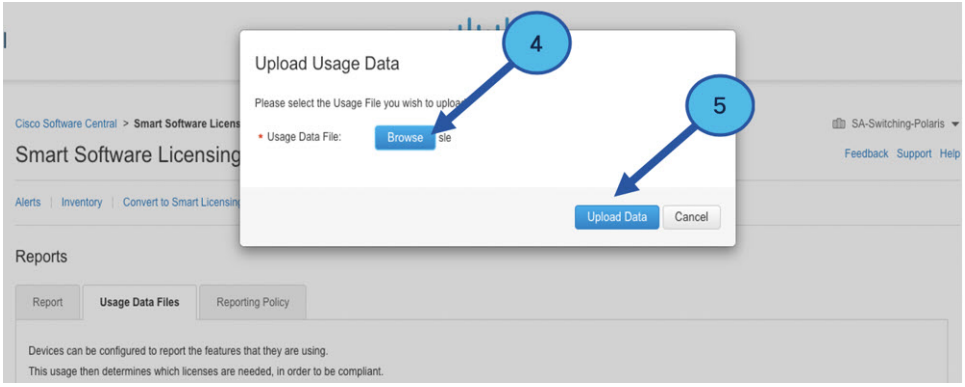
Figure 1: Usage Data File



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

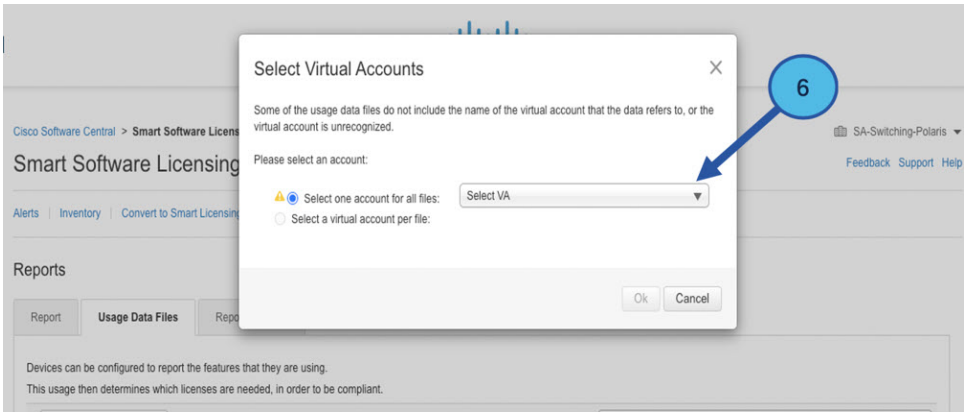
Step 5 Click on **Upload Data**.

Figure 2: Browse and Upload



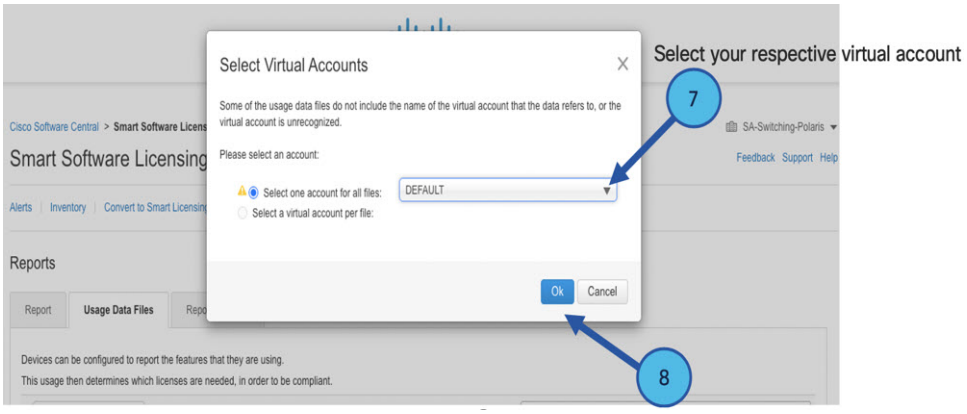
Step 6 Select the Virtual Account.

Figure 3: Select Account



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

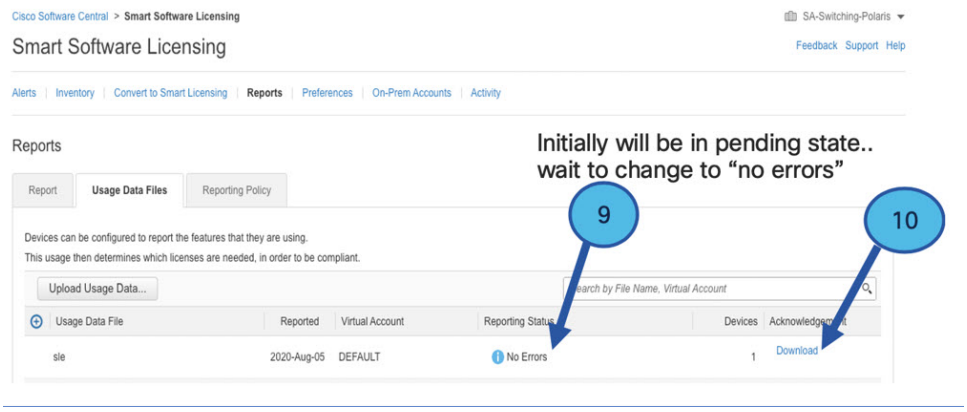
Figure 4: Select Your Account



Step 8 Click **Ok**.

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

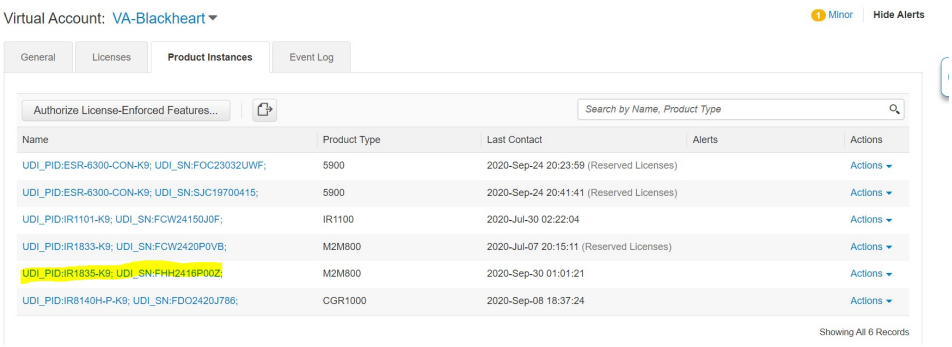
Figure 5: Reporting Status



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

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

Figure 6: Product Instances



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

Importing the ACK file from CSSM to your Device

Procedure

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

Example:

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

Step 2 Verify Product Instance has imported the data

Example:

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (IR8100_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
```

Step 3 Verify the license is in use.

Example:

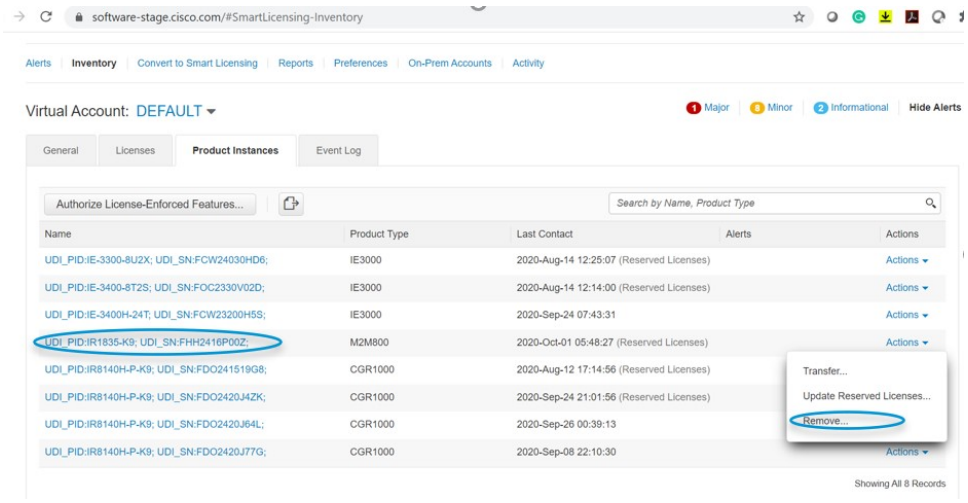
```
Router# show license summary
License Usage:
  License                                        Entitlement tag              Count    Status

  -----------------------------------------------------------------------------------------
  network-advantage_250M  (ir8100_P_250M_A)          1      IN USE

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

Removing the Device from CSSM

Procedure

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

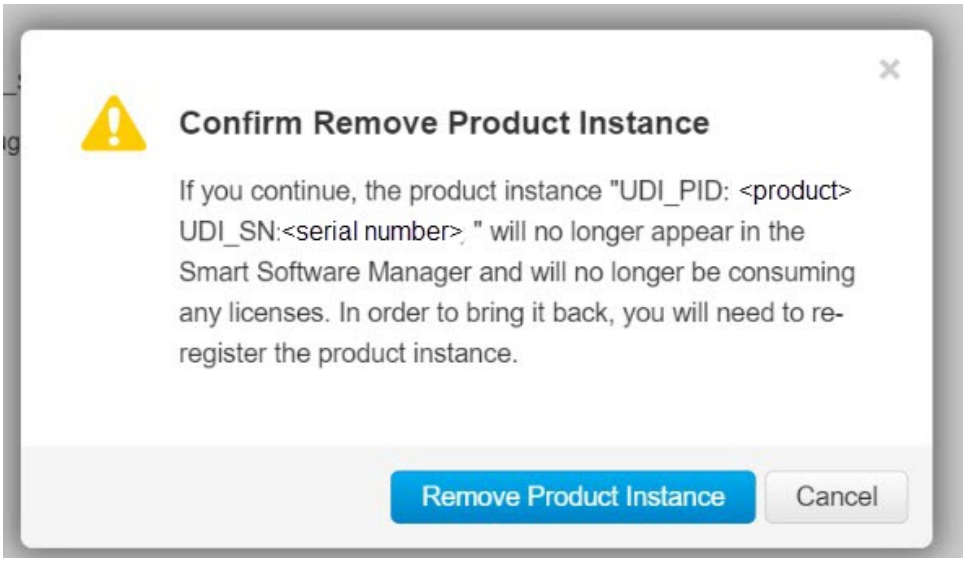
Figure 7: Product Instances



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

The Confirm Remove Product Instance window appears.

Figure 8: Confirm Remove Product Instance

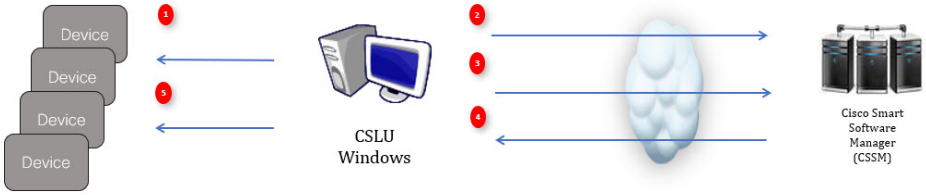


Step 3 Click **Remove Product Instance**.

License Installation Procedure - CSLU has No Access to CSSM

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

Refer to the following graphic for the flow of information:



Procedure

Step 1 In CSLU, identify the devices that require an AuthCode, and initiate the request. An AuthCode file is created.

Step 2 Export the AuthCode file to CSSM.

Step 3 Upload the AuthCode to CSSM SA/VA account.

Step 4 Export the AuthRequestAuthcode file to CSLU.

Step 5 Upload ACK file or AuthRequestAuthCode

Procedure when devices are connected to the CSLU

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

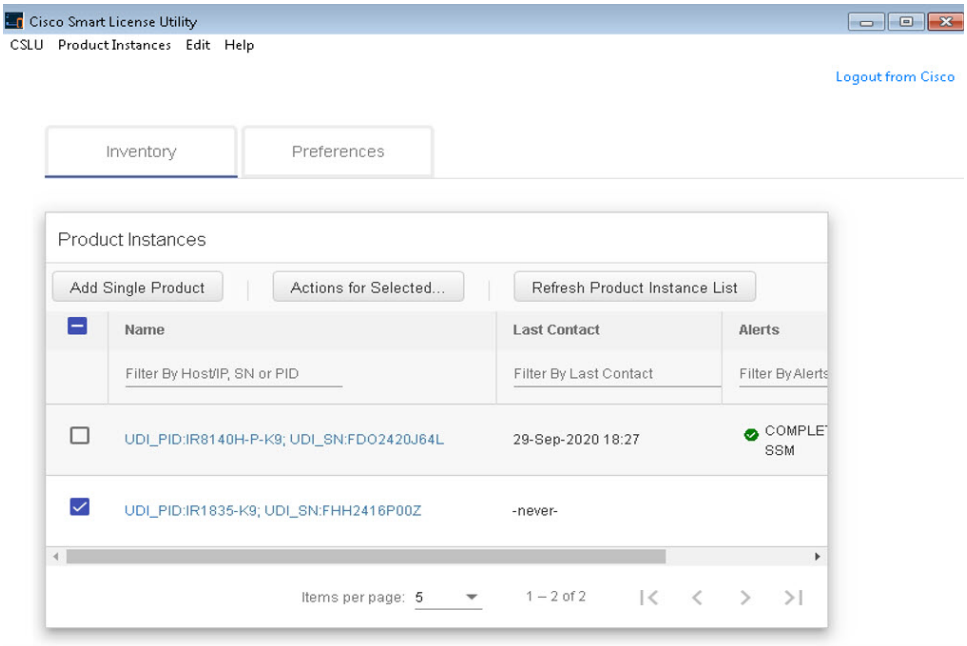
```
Router#show license summary
License Reservation is ENABLED
License Usage:
License Entitlement tag Count Status
-----------------------------------------------------------------------------
network-essentials_250M (IR8100_P_250M_E) 1 IN USE
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!
Router(config)#end
Router#sh license udi
UDI: PID:IR1835-K9,SN:FHH2416P00Z
```

Procedure

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

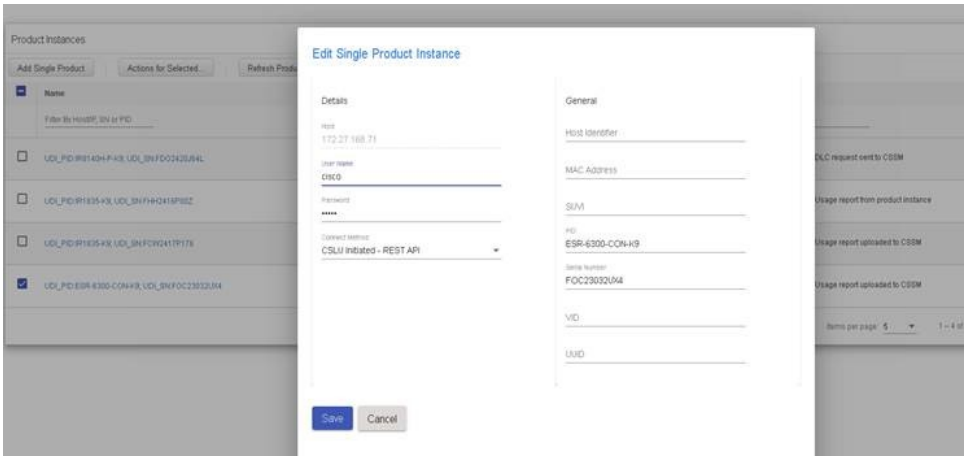
Step 2 Navigate to the **Product Instances** tab, then click on the UDI.

Figure 9: Select UDI



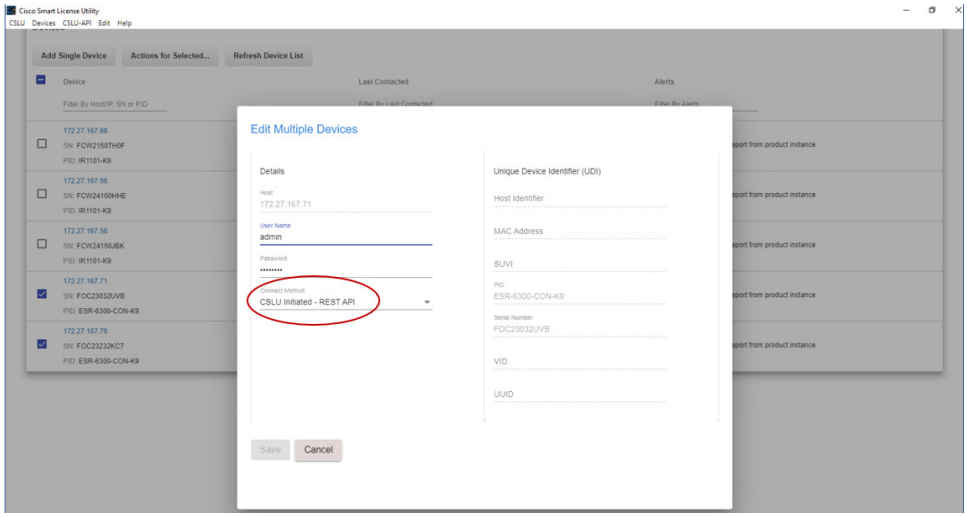
Step 3 The **Edit Single Product Instance** window appears.

Figure 10: Edit Single Product Instance



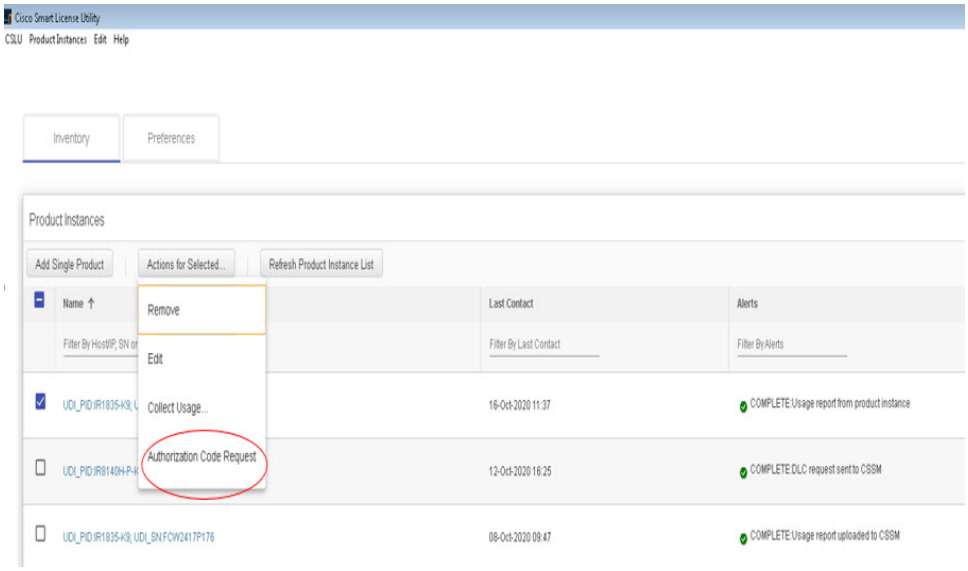
Step 4 The **Edit Multiple Devices** window appears. Supply your account password and click **Save**.

Figure 11: Edit Multiple Devices



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

Figure 12: Actions for Selected Devices



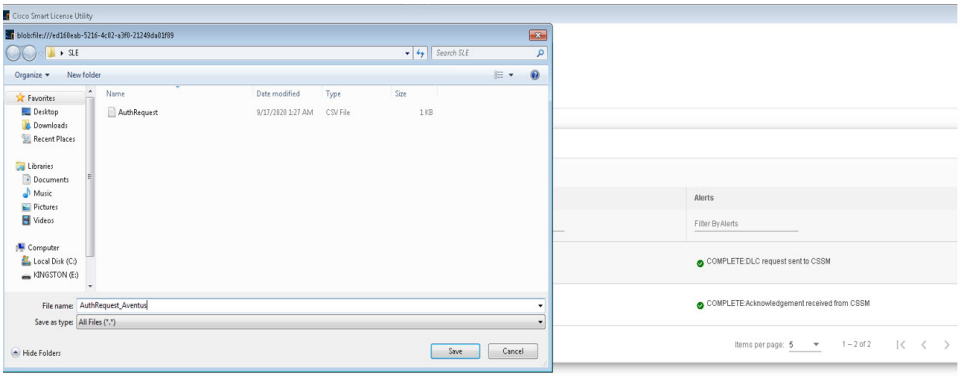
Step 6 Select **Authorization Code Request**.

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

Figure 13: Authorization Request Information

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

Figure 14: Authorization Request File



Exporting the AuthRequest File to CSSM

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

Launch CSSM.

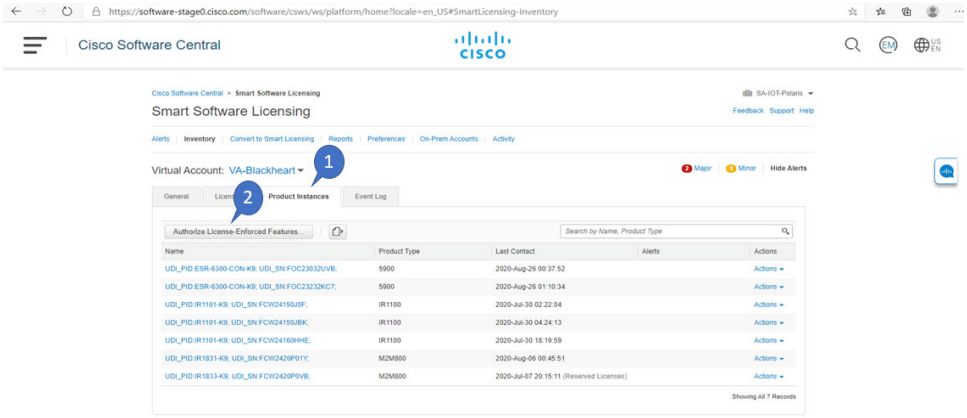
Click on the **Inventory** Tab, select your Virtual Account.

Procedure

Step 1 Click on the **Product Instances** Tab.

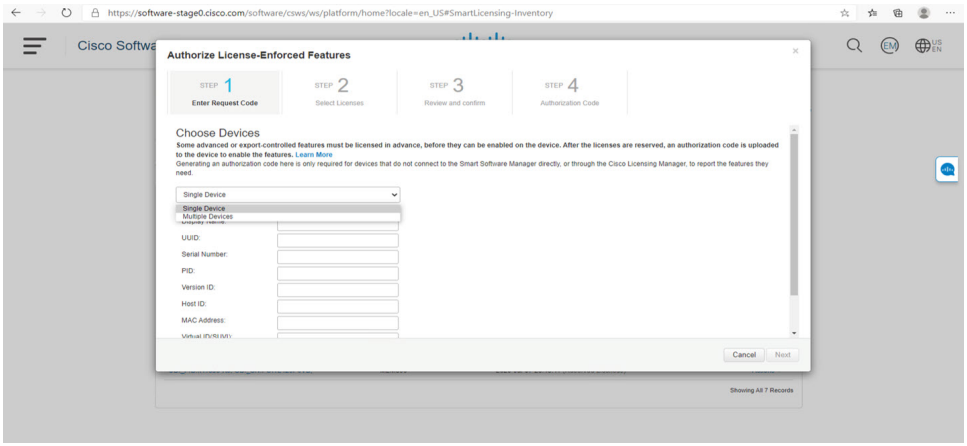
Step 2 Click on **Authorize License-Enforced Features**.

Figure 15: Authorize License-Enforced Features



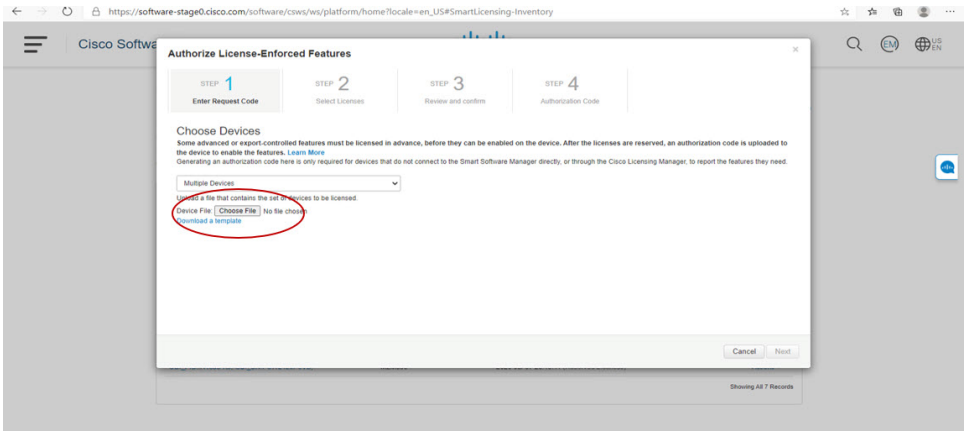
The **Authorize License-Enforced Features** window appears**.**

Figure 16: Authorize License-Enforced Features



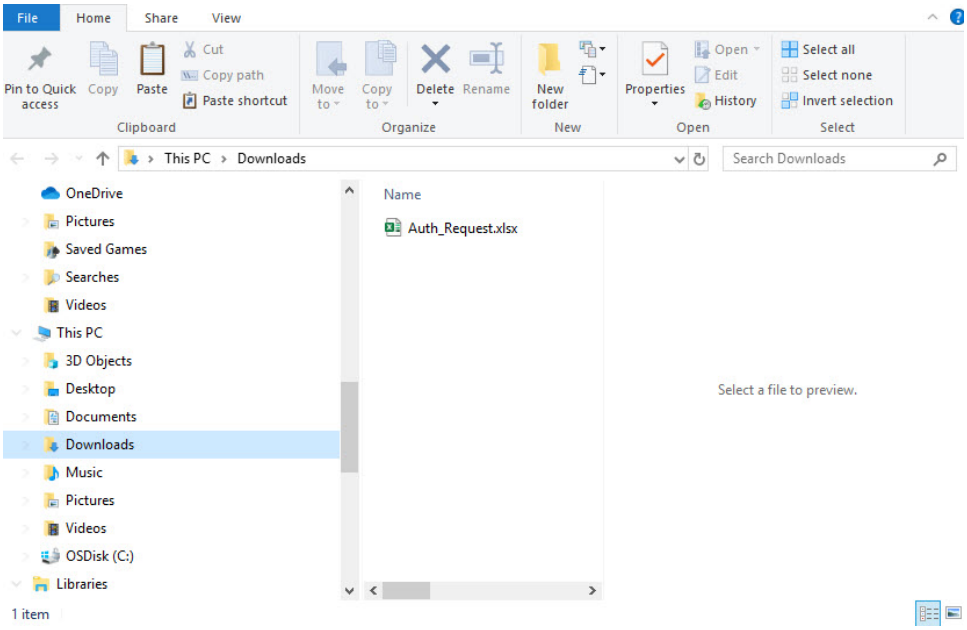
Step 3 Choose **Multiple** or **Single** devices from the pull-down.

Step 4 The window changes to an option to select a device file. Click on **Choose File**.



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

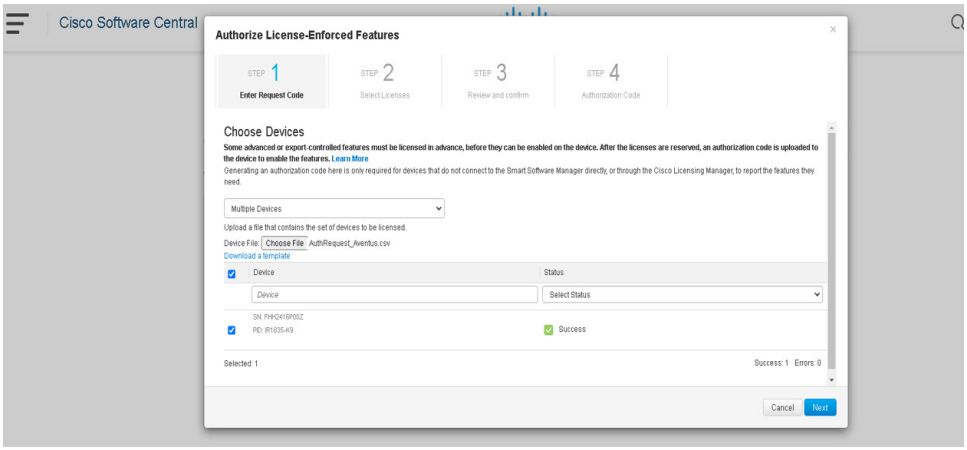
Figure 17: Open File Navigation Window



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

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

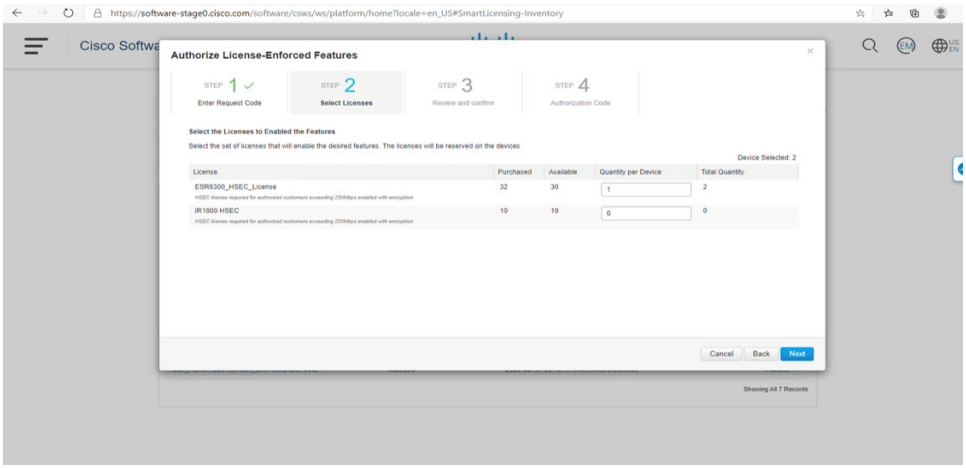
Figure 18: Present Devices



Step 8 When successful, click **Next**.

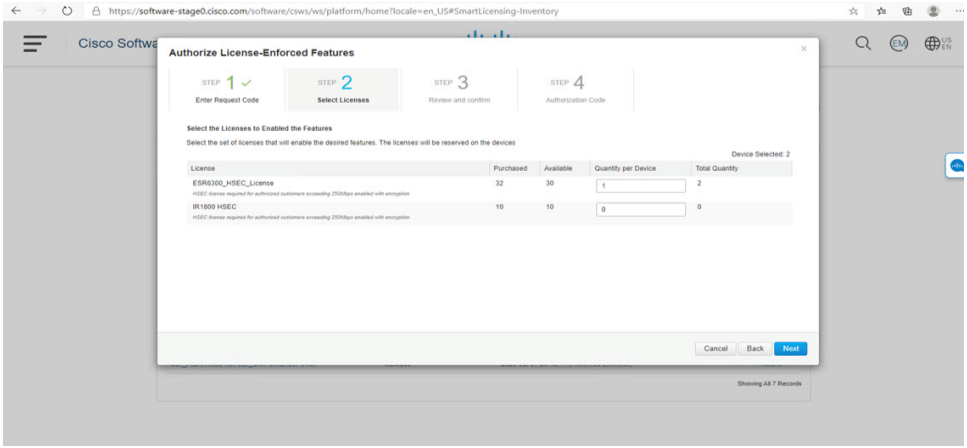
Step 9 The **Select Licenses** Tab opens.

Figure 19: Select Licenses



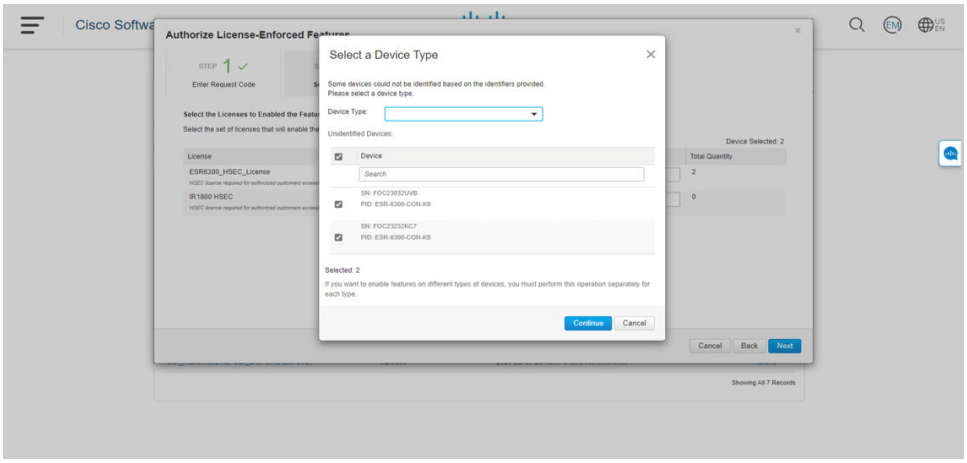
Step 10 Under **Quantity per Device**, enter the number you wish.

Figure 20: Enter Number



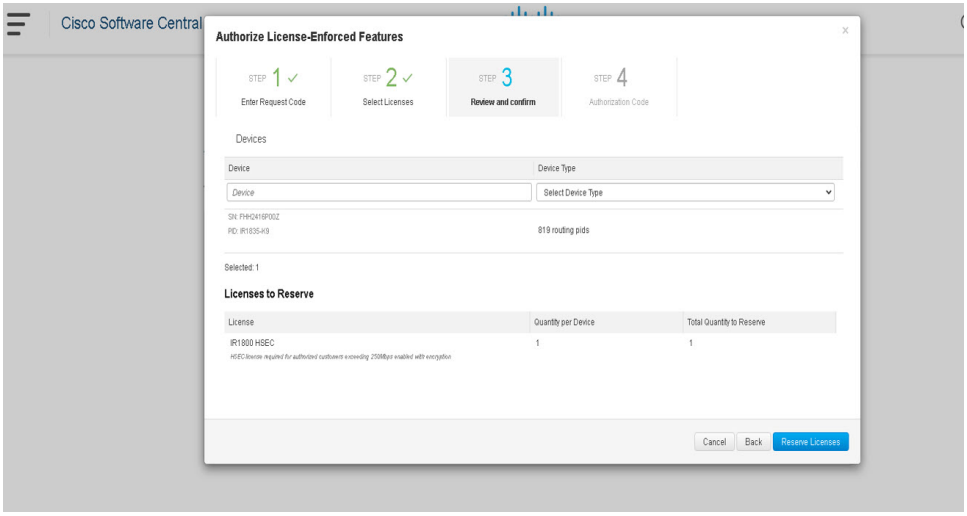
Step 11 If CSSM cannot identify your device from the identifying information, you can select it manually.

Figure 21: Select a Device Type



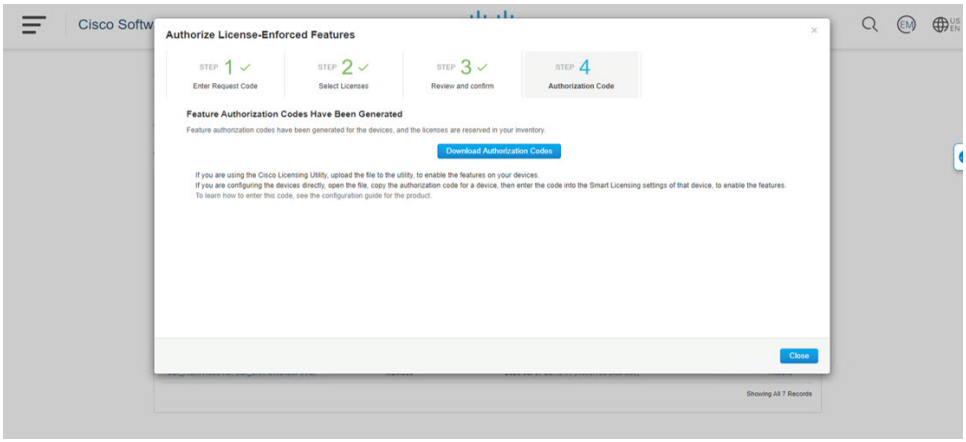
Step 12 Click **Continue**, and the window changes to **Review and Confirm**.

Figure 22: Review and Confirm



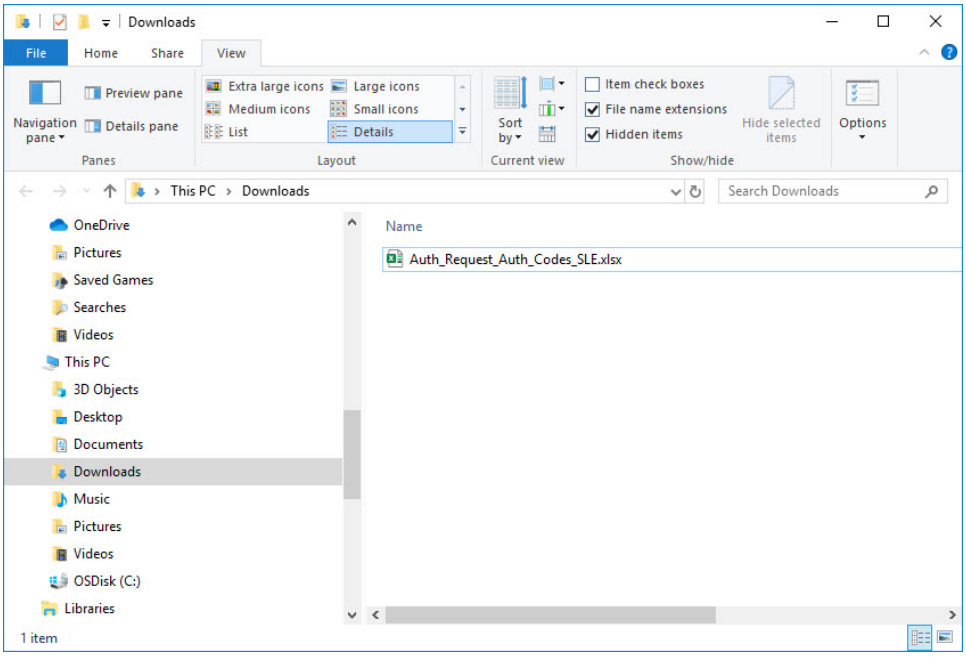
Step 13 Click on **Reserve Licenses**, and CSSM generates feature authorization codes.

Figure 23: Feature Authorization Codes



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

Figure 24: Save Authorization Code



Step 15 Click **Ok**.

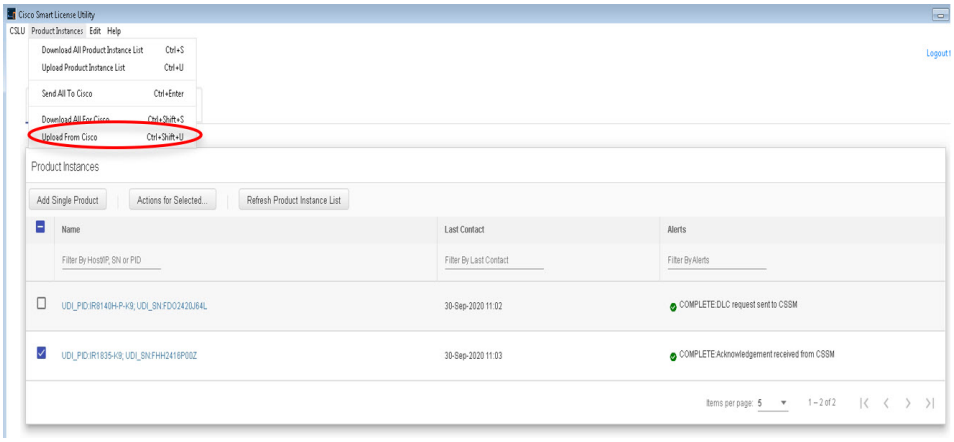
Uploading the Authorization Request Code file into CSLU

Procedure

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

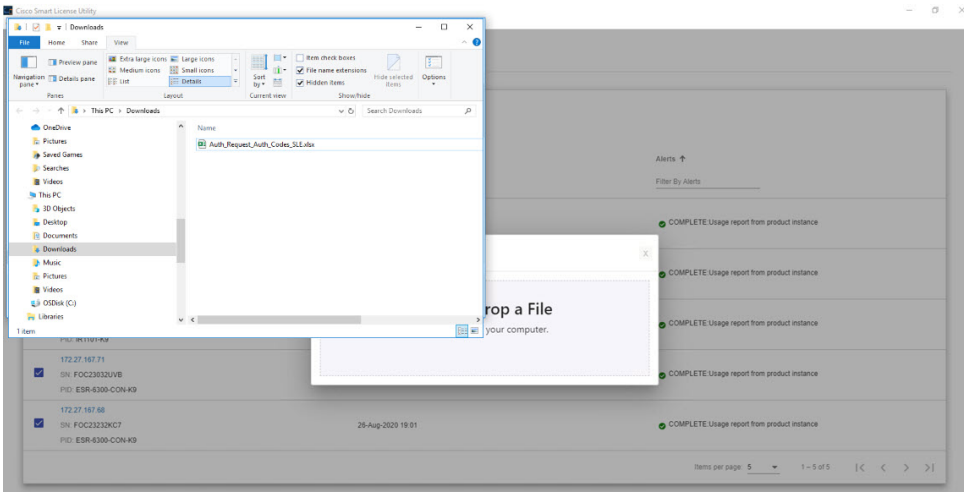
Step 2 Navigate to **Product Instances**, and then select **Upload From Cisco**.

Figure 25: Upload From Cisco



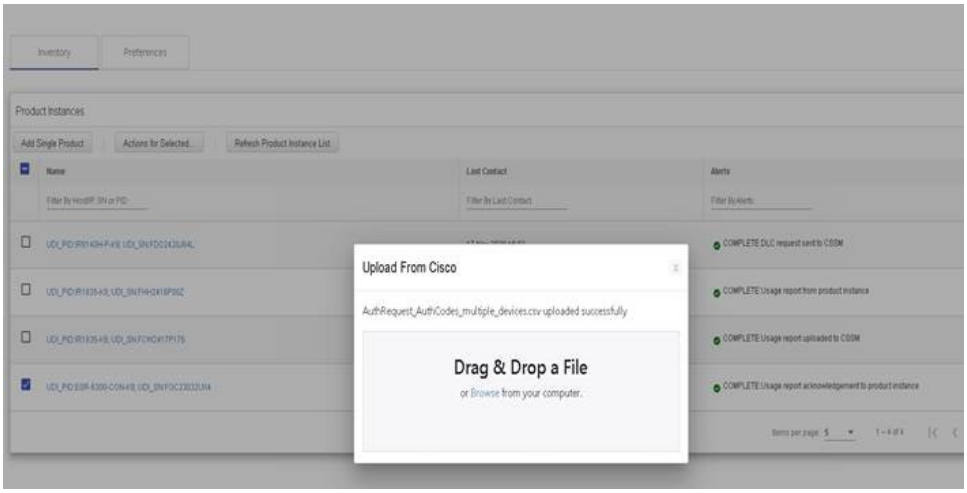
Step 3 There are two options to load your file. **Drag and Drop**, or **Browse** to where you saved your file. This example shows Browse.

Figure 26: Browse to File



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

Figure 27: Successful Upload

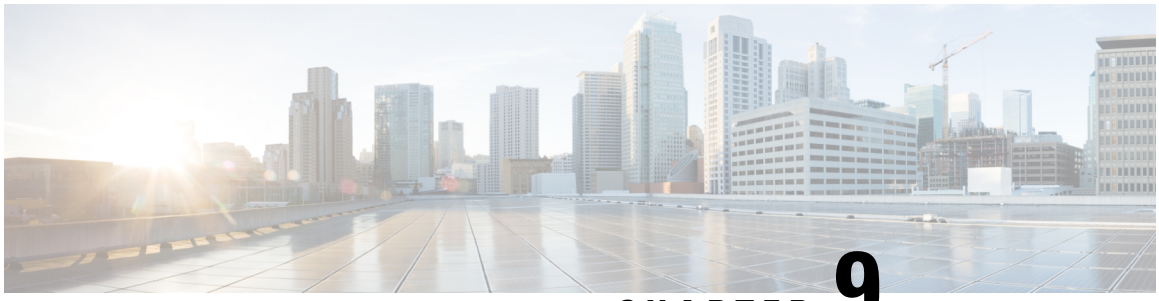


License Installation Process in the Router

Perform the following from the command line interface.

```
Router#show license summary
License Reservation is ENABLED
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  network-essentials_250M (IR8100_P_250M_E)                 1 IN USE
  hseck9                  (IR8100_HSEC)                     1 IN USE
Router#show license usage
License Authorization:
  Status: Not Applicable
network-essentials_250M (IR8100_P_250M_E):
  Description: network-essentials_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-essentials_250M
  Feature Description: network-essentials_250M
  Enforcement type: NOT ENFORCED

hseck9 (IR8100_HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
Router(config)#end
```

```
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#show license summary
License Reservation is ENABLED
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  network-essentials_250M (IR8100_P_250M_E)                 1 IN USE
  hseck9                  (IR8100_HSEC)                     1 IN USE
  network-essentials_2G   (IR8100_P_2G_E)                   1 IN USE
```



CHAPTER 9

Battery Backup Unit (BBU)

- Battery Backup Unit Overview, on page 89
- Configuring BBU Mode, on page 89
- Upgrade BBU, on page 93

Battery Backup Unit Overview

The integrated modular battery backup unit (BBU) is a smart charging and monitoring system. When the system AC power is turned off on the IR8100, the installed BBU supplies power to the router. The BBU also allows graceful shutdown of events on the router based on the configured voltage level thresholds. IR8100 supports up to three BBU units installed on the system.

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

Configuring BBU Mode

The BBU automatically begins to supply power to the router when it detects that power is not being received from the AC power supply. You may want to disable and enable the BBU for the following reasons:

- To inhibit the BBU discharge during storage, shipping or transportation in order to preserve battery life.
- To replace the battery in an installed and operating router.

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 still can be charged when disabled.

Enabling BBU

To enable the BBU in the router:

Procedure

Step 1 Enter the **request platform hardware battery enable** command:

Example:

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

Step 2 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 3 To check the BBU status, enter the **show platform hardware battery unit** command:

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
```

Disabling BBU

To disable the BBU in the router:

Procedure

Step 1 Enter the **request platform hardware battery disable** command:

Example:

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

Step 2 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 3 To check the BBU status, enter the **show platform hardware battery unit** command:

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

Example:

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

Step 2 Confirm the action when prompted:

Example:

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

Step 3 Verify the BBU status, with the **show platform hardware battery unit** command:

Example:

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

Step 4 Use the **request platform hardware battery reset disable** command to reconnect communications with the battery:

Example:

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

Step 5 Confirm the action when prompted:

Example:

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

Step 6 Verify the BBU status, with the **show platform hardware battery unit** command:

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
```

Transportation Mode

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 **request platform hardware battery transportation-mode enable** command to enable the transportation-mode:

Example:

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

Step 2 Confirm the action when prompted:

Example:

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

Step 3 Verify the BBU status, with the **show platform hardware battery unit** command:

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 4 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 5 Confirm the action when prompted:

Example:

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

Upgrade BBU

We recommend 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 Create a new directory **bbu_fw**. You must spell **bbu_fw** exactly.

Example:

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

Step 2 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.SPA
7228108800 bytes total (5388279808 bytes free)
```

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 3 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 4 Upgrade the firmware. Do not interrupt the process until it is complete.

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
```

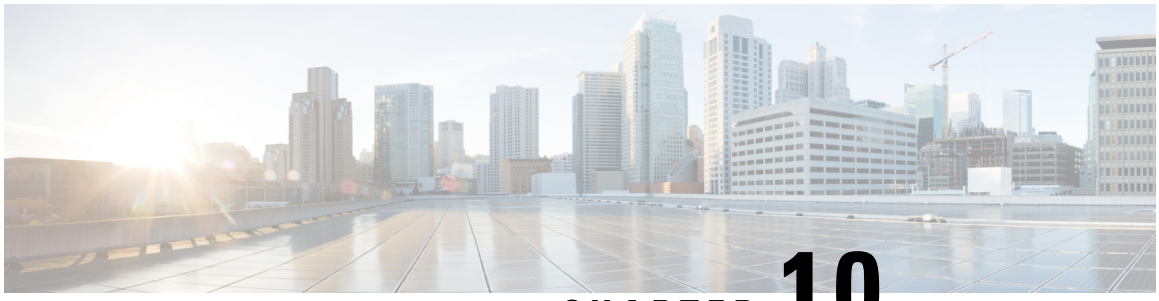
Example logs:

```
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
successfully
Oct  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
```

Step 5 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

- Tamper Detection, on page 97

Tamper Detection

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 IOT-FND, a corresponding event is also sent to IOT-FND.

The cover detection applies for the following 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 IOT-FND at a later time.

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

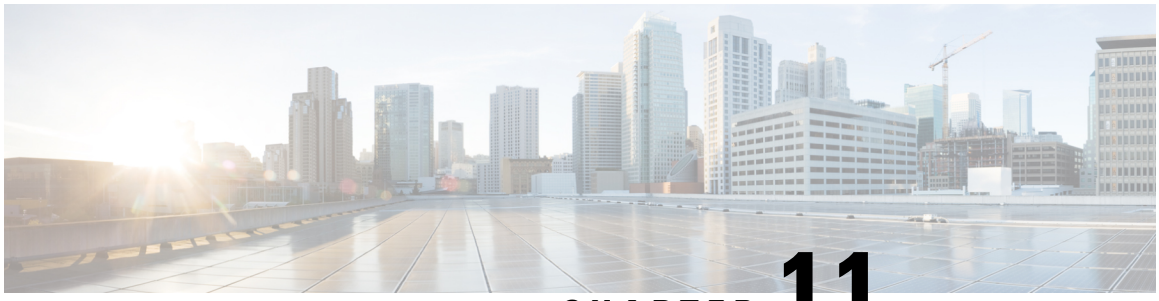
Note It is highly recommended to power down the module prior to physically remove it, using the following CLI command. For example, if the module is in slot 3:

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

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

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

Tamper Detection



CHAPTER 11

Power Over Ethernet (PoE)

- Power over Ethernet, on page 99
- Device Detection and Power Allocation, on page 99
- Command Line Interface, on page 99

Power over Ethernet

Power over Ethernet (PoE) is typically used to power up devices such as Access points, IP Cameras and IP Phones connected to the device's Ethernet ports. The total PoE available power is 15W to be shared by the Gi0/0/0 interface.

The power allocation is as follows:

- 1 x POE (AT Type1 or AF-Class 0/3) ports (15.4 W)

Device Detection and Power Allocation

The router will detect a Cisco Pre-standard or an IEEE-compliant PD when the PoE is enabled and the connected device is not being powered by an AC adapter.

After device detection, the router will determine the power requirements based on power classification class. Depending on the available power in the power budget, the router determines if a port can be powered. The router initially allocates this power when it detects and powers the device. Power negotiation using CDP/LLDP protocols happens thereafter. Supported protocols for power negotiation are CDP for Cisco PD, and LLDP for non-Cisco PDs. Maximum power budget for 1 WAN port at any time is 15.4 W. On reload the PoE ports are powered down until the unit reboots.

Command Line Interface

This section describes the CLI to use for configuring and displaying PoE.

To configure auto or off:

```
power inline auto | never
```

Configuration example:

```
Router#config terminal
Router#interface g0/0/0
Router(config-if)#power inline {auto|never}
```

To verify your configuration:

```
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
Router#
```

To show power on a particular interface:

```
Router#show power inline {interface-id}
```

Displays PoE status for a router for the specified interface.

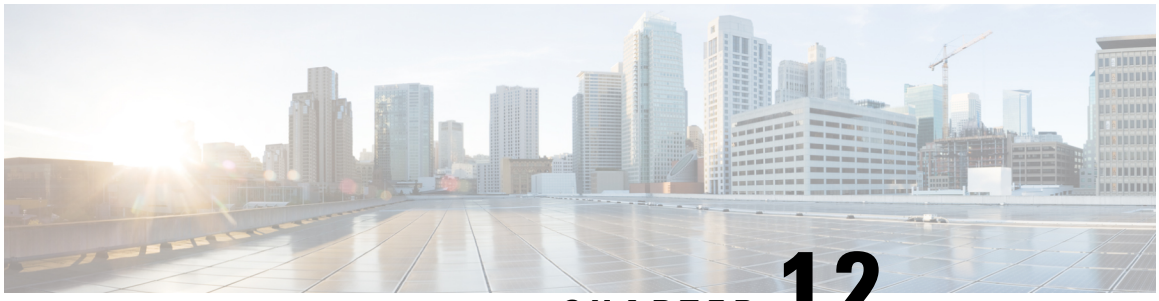
```
show power inline interface-id detail
```

To show power consumption:

```
Router#show power
Main PSU :
  Total Power 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
Router#
```

The list of commands for debugging PoE follows:

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

12V DC Output for 3rd Party Device

- Enabling 12V DC Output, on page 101

Enabling 12V DC Output

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%.

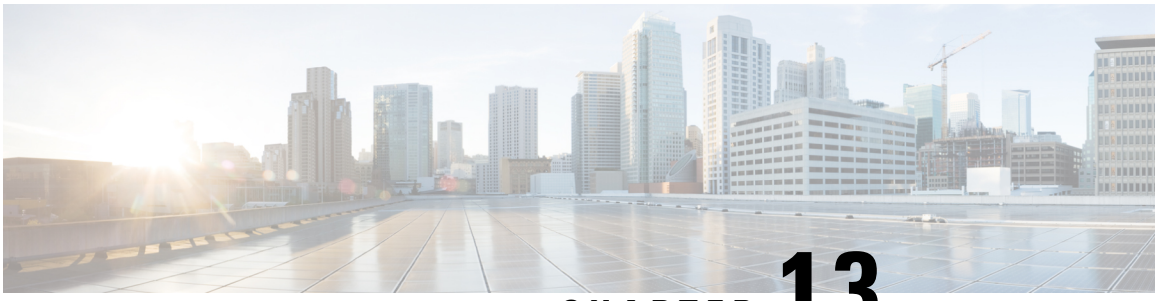
Note PoE and 12V configuration are mutually exclusive.

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
```



CHAPTER 13

NTP Timing Based on GPS Clock

- Configuring NTP using GPS Time, on page 103

Configuring 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 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Configure the NTP reference clock as GPS:

Example:

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

Step 3 To verify the configuration, use the **show** commands in the following example:

Example:

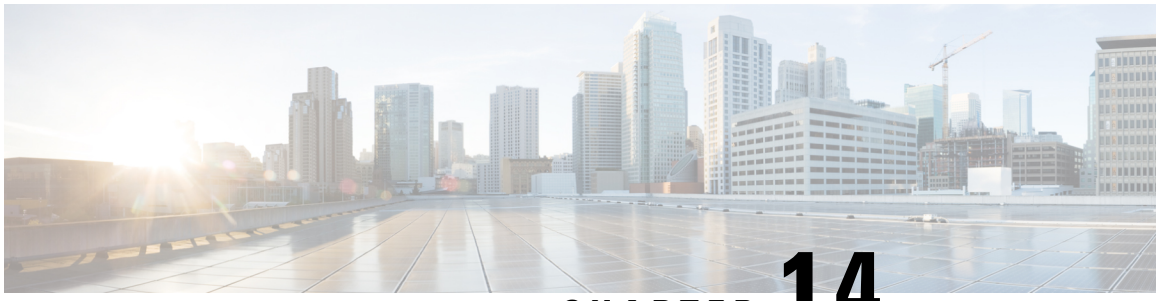
```
Router#
Sep 24 19:58:43.046 GMT: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Router#show ntp status
Clock is synchronized, stratum 1, reference is .GPS.
nominal freq is 250.0000 Hz, actual freq is 249.9970 Hz, precision is 2**10
ntp uptime is 94000 (1/100 of seconds), resolution is 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#
Router#show clock
20:00:43.660 GMT Thu Sep 24 2020
Router#
```

Step 4 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 14

vCPU and RAM Distribution

- Introduction, on page 105
- Distribution of vCPU and RAM Resources for Cisco IOx Applications, on page 105
- Higher CPU and RAM Allocation for IOx Applications , on page 106
- Configure Data Plane Heavy Template, on page 106
- Verify the Active vCPU and RAM Distribution, on page 107
- Configure Service Plane Heavy Template, on page 107
- Verify the Active vCPU and RAM Distribution, on page 108

Introduction

This chapter provides information on how to distribute Virtual Central Processing Unit (vCPU) cores and RAM resources for Cisco IOx applications on Cisco Catalyst IR8100 router.

Note vCPU is also known as physical processor.

Distribution of vCPU and RAM Resources for Cisco IOx Applications

Distributing the available resources efficiently allows you to run multiple IOx applications simultaneously.

Use these templates to distribute the vCPU and RAM resources:

- **Data Plane Heavy—**Refers to a router configuration where majority of system resources are dedicated to the data plane, which is responsible for processing and forwarding network packets.

  Data Plane Heavy template maximizes throughput and ensures high-speed packet transfer, which is essential for network traffic demands. This ensures more processing power and memory to handle the increased load on the data plane, enhancing router's ability to move large volumes of data efficiently.

Note The Data Plane Heavy is the default template for vCPU and RAM distribution in the IR8100 router.

- **Service Plane Heavy—**Refers to a router configuration where majority of system resources are allocated to the service plane, which is responsible for providing network services such as Quality of Service (QoS), security functions, and load balancing.

  Service Plane Heavy template allocates additional vCPU and RAM to IOx applications. However, it 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

From Cisco IOS XE Release 17.15.1, the IR8100 router with 8 GB RAM supports Data Plane Heavy and Service Plane Heavy distribution templates. You can allocate 3 GB RAM and two vCPU cores to IR8100 router for hosting Cisco IOx applications. We recommend the Service Plane Heavy template to allocate resources for hosting IOx applications.

Configure Data Plane Heavy Template

Procedure

Step 1 Enter the configuration command to enable the data plane heavy template:

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

Step 2 Enter the reload command to reboot the router and activate the data plane heavy template:

```
Router#reload
```

What to do next

Verify the active vCPU and RAM distribution.

Verify the Active vCPU and RAM Distribution

Use the **show** command to verify the vCPU cores allocation for IOx applications.

```
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
```

Use the **show** command to verify the RAM allocation for IOx applications.

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

Use the **show** command to verify the CPU units resource allocation for IOx applications.

```
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: 33%
  Available: 33%
  Quota: 1617(Units)
  Available: 1617(Units)
```

Configure Service Plane Heavy Template

Procedure

Step 1 Enter the configuration command to enable the service plane heavy template:

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

Step 2 Enter the reload command to reboot the router and activate the service plane heavy template:

```
Router#reload
```

What to do next

Verify the active vCPU and RAM distribution.

Verify the Active vCPU and RAM Distribution

Use the **show** command to verify the vCPU cores allocation for IOx applications.

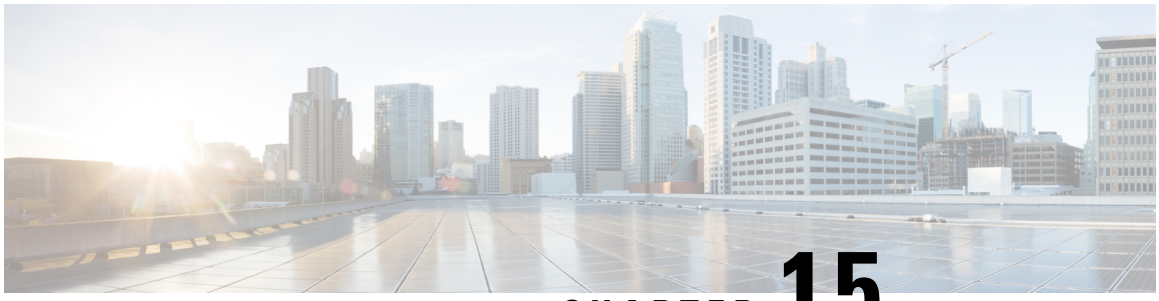
```
Router#show platform software cpu allocation
CPU Allocation Information:
  Control plane cpu alloc: 0-1
  Data plane cpu alloc: 3
  Service plane cpu alloc: 0-2
Template used: CLI-service_plane_heavy
```

Use the **show** command to verify the RAM allocation for IOx applications.

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

Use the **show** command to verify the CPU units resource allocation for IOx applications.

```
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 15

Cellular Pluggable Interface Module Configuration Guide

The Cisco 4G LTE-Advanced Configuration chapter has been replaced by a new standalone guide called Cellular Pluggable Interface Module Configuration Guide. This guide contains updated information on all aspects of using the Cisco Cellular PIM.

Important The Pluggable Module is not hot swappable. The router must be reloaded after a new module is installed.

- Support for the P-5GS6-GL Pluggable Module on the ESR6300, on page 109
- Galileo Support on the LTE Pluggable Modules, on page 109

Support for the P-5GS6-GL Pluggable Module on the ESR6300

Support for the P-5GS6-GL Pluggable Module works the same on the ESR6300 as it does on the other IoT Routers. For details, see 5G Sub-6 GHz Pluggable Interface Module and Cellular Pluggable Interface Module Configuration Guide.

Galileo Support on the LTE Pluggable Modules

With Cisco IOS XE 17.11.1a and earlier, the only GNSS constellation supported was GPS. This release introduces support for Galileo.

Note Only ONE constellation can be enabled at a time.

There are new CLI options available to support the new constellation:

Configuration Commands

```
config# controller cellular <slot/port>
(config-controller)# <no> lte gps constellation <gps | galileo | gnss >
```

Example:

```
(config-controller)#lte gps constellation ?
  galileo  select Galileo as active constellation
  gps      select GPS as active constellation
  gnss      select multiple GNSS as active constellation
```

Note The default setting is gps mode.

The new galileo and gnss options in the above CLI are used to configure Galileo and Multiple/Simultaneous GNSS (GPS + Galileo etc) respectively.

If you disable the GPS configuration, ensure there is no constellation configured, consistent with GPS mode configuration. For example:

```
config# controller Cellular 0/1/0
(config-controller)# no lte gps constellation gps
```

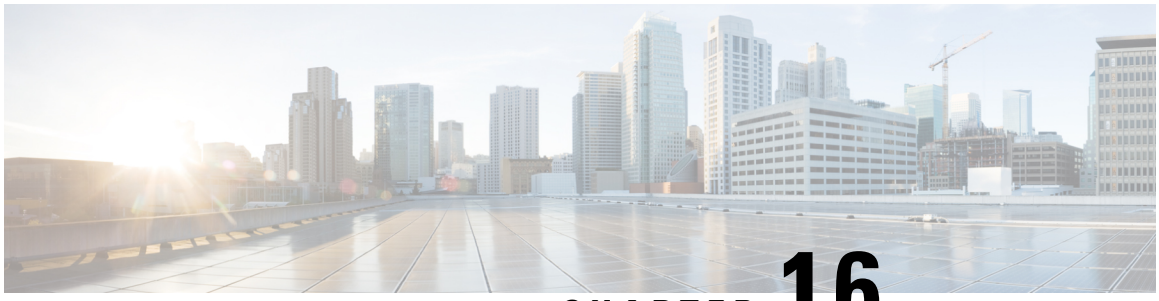
Show Commands

The following example shows the current GNSS constellation as Galileo:

```
#show cellular 0/1/0 gps detail
GPS Feature =  enabled
GPS Mode Configured =  standalone
Current Constellation Configured =  galileo | gps | gnss
GPS Port Selected =  Dedicated GPS port
GPS Status =  GPS acquiring
```

Any changes made to the configuration will require the router to be rebooted.

More information is available in the Cellular Pluggable Interface Module Configuration Guide.



CHAPTER 16

Configuring Cisco Resilient Mesh and the WPAN Module

- Resilient Mesh and WPAN Module Overview, on page 111
- Configuring the WPAN Interface, on page 112
- Configuring Group Multicast, on page 116
- Configuring RPL, on page 117
- Configuring the Power Outage Server, on page 119
- Configuring Cisco Resilient Mesh Security, on page 119
- Configuring the IPv6 Multicast Agent, on page 122
- Configuring DTLS Relay for EST, on page 125
- Configuring Wi-SUN Mode, on page 125
- Modulation and Data Rate (MDR), on page 127
- Limited Function Node (LFN), on page 130
- Direct Parenting of LFN Support in Wi-SUN Mesh Deployment, on page 132
- Verifying WPAN Configuration, on page 133
- Example IR8100 Basic WPAN Configuration, on page 134
- Example IR8100 Configuration for CG-Mesh, on page 145
- Example ASR Configuration for CG-Mesh, on page 149
- Checking and Upgrading the WPAN Firmware Version, on page 154

Resilient Mesh and WPAN Module Overview

This guide explains how to install the IEEE 802.15.4e/g Cisco Wireless Personal Area Network (WPAN) module and how to configure the Cisco Resilient Mesh. This guide addresses configuration for a Cisco IR8100 Series Router installed with Cisco IOS-XE software.

Note IoT FND provides the user interface for all Cisco Resilient Mesh configuration and management. Cisco Resilient Mesh has no CLI and no graphical user interface for configuration or management.

All configuration and management occur only by using IoT FND through the IR8140H Series WPAN module by using Cisco IOS-XE software commands.

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

On the IR8140H, the WPAN module serial PID is displayed in IOS-XE as IRMH-WPAN-NA, as shown in the following example:

```
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
```

Configuring the WPAN Interface

At the IR8140H, configure the WPAN Module interface as follows:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

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

WPAN slot is always 1 and port is 0/1.

Example:

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

Enabling dot1x, mesh-security and DHCPv6

You must enable the dot1x (802.1X), mesh-security, and DHCPv6 features to configure the WPAN interface. To enable these features, enter the following commands:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enable 802.1X authentication globally on the router:

Example:

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

Step 3 Enter interface configuration mode and specify the WPAN interface:

Example:

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

Step 4 Enable the WPAN interface to respond to messages meant for an IEEE 802.1x authenticator:

Example:

```
Router(config-if)# dot1x pae authenticator
Router(config-if)#authentication host-mode multi-auth
Router(config-if)#authentication port-control auto
```

Step 5 Enable IPv6 and specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface:

Example:

```
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 dhcp relay destination  <IPv6 address >
```

Configuring IEEE154 Settings

Follow these steps to configure WPAN radio-related settings:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter interface configuration mode and specify the WPAN interface:

Example:

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

Step 3 Configure the name of your IEEE 802.15.4 Personal Area Network Identifier (PAN ID):

Example:

```
Router(config-if)#ieee154 panid ?
  <0-65534>  Enter a value between 0 and 65534

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

Step 4 Configure the name of the Service Set Identifier (SSID).

The SSID identifies the owner of the Resilient Mesh Endpoint (RME). The SSID is set on a RME in manufacturing, and that same SSID must also be configured on the IR8100 WPAN interface.

Example:

```
Router(config-if)# ieee154 ssid ?
  WORD  ssid string (Max size 32)
Router(config-if)# ieee154 ssid myWPANssid
```

Step 5 Configure the notch.

A notch is a list of disabled channels from the 902-to-928 MHz range. If there is no notch at all, then all channels are enabled. if there is a notch [x, y], then channels between x and y are disabled.

Note A channel list is a list of enabled channels.

Notch configuration must comply with your regional regulations (for example, a notch configuration is not required for the U.S.). Notch configuration must match between the WPAN interface of the IR8100 and the RME.

Example:

```
Router(config-if)#ieee154 notch ?
  <0-128>  channel id
Router(config-if)#ieee154 notch 10-15
```

Note To verify the notch configuration, you can use the **show hardware channel-list** command, for example:

```
Router(config-if)# end
Router# show wpan 0/1/0 hardware channel-list
channel list: 0 1 2 3 4 5 6 7 8 9 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
```

Step 6 Specify the IEEE154 PHY mode (a value from 1-255) of the IRMH-WPAN module.

The IRMH-WPAN module operates within a RF900 wireless network to provide digital automation (DA) control over RMEs. The PHY mode setting selects the adaptive modulation, which enhances the backward compatibility with the classic Cisco Resilient Mesh network and improves the transmitting ability in the classic Cisco Resilient Mesh network. Adaptive modulation is supported in both Wi-SUN and Cisco mesh modes.

Supported PHY modes are:

- 1: Classic; Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=ON; Channel Spacing=200 kHz
- 17: Classic; Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz
- 2: Classic; Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz
- 18: Classic; Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
- 64: Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz

- 96: Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=ON; Channel Spacing=200 kHz
- 66: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
- 98: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz
- 128: Rate=100 kb/s; Modulation=OFDM; Option=1; MCS=0; Channel Spacing=1200 kHz
- 129: Rate=200 kb/s; Modulation=OFDM; Option=1; MCS=1; Channel Spacing=1200 kHz
- 130: Rate=400 kb/s; Modulation=OFDM; Option=1; MCS=2; Channel Spacing=1200 kHz
- 131: Rate=800 kb/s; Modulation=OFDM; Option=1; MCS=3; Channel Spacing=1200 kHz
- 132: Rate=1200 kb/s; Modulation=OFDM; Option=1; MCS=4; Channel Spacing=1200 kHz
- 133: Rate=1600 kb/s; Modulation=OFDM; Option=1; MCS=5; Channel Spacing=1200 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
- 146: Rate=200 kb/s; Modulation=OFDM; Option=2; MCS=2; 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
- 162: Rate=100 kb/s; Modulation=OFDM; Option=3; MCS=2; Channel Spacing=400 kHz
- 163: Rate=200 kb/s; Modulation=OFDM; Option=3; MCS=3; Channel Spacing=400 kHz
- 164: Rate=300 kb/s; Modulation=OFDM; Option=3; MCS=4; 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
- 192: Rate=6.25 kb/s; Modulation=OQPSK; Chip Rate=100 kchip/s; Rate Mode=0; Channel Spacing=200 kHz

Note Adaptive modulation only supports configuring the same Orthogonal Frequency-division Multiplexing (OFDM) option PHY mode or the same OFDM option plus FSK PHY mode.

Cisco Resilient Mesh Release 6.3 only supports PHY mode 64, 66, 161, 162, 163, 165, and 166 for IRMH-WPAN.

The following example shows configuring adaptive modulation in Wi-SUN mode, which sets the channel to 254 and notch to none:

Example:

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

Router(config-if)#
```

Note To verify PHY mode configuration, enter **show wpan 4/1 hardware config** in privileged EXEC mode.

Configuring Group Multicast

Follow these steps to configure group multicast on the router. Group multicast allows the router to forward multicast traffic to a specific group of devices. The devices in one group can cross multiple PANs.

Note This feature is not supported in Cisco Resilient Mesh Release 6.3.

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enable IPv6 multicast-routing:

Example:

```
Router(config)# ipv6 multicast-routing
```

Step 3 Enable MPL:

Example:

```
Router(config)#fan-mpl domain 0
```

Step 4 Check the mcast address reported by node:

- show wpan 0/1/0 rpl mcast-info domains
- show wpan 0/1/0 rpl mcast-info groups

Step 5 Enter interface configuration mode and add the multicast agent interface (uplink interface):

Example:

```
Router(config)#interface WPAN 0/1/0
Router(config-if)#mcast-agent interface gi0/0/0
```

Step 6 Enable LFN:

Example:

```
Router(config)#interface WPAN 0/1/0
Router(config-if)#lfn
```

Step 7 Add the multicast agent port:

Example:

```
Router(config-if)#mcast-agent port
```

Step 8 Add the multicast agent group:

Example:

```
Router(config-if)#mcast-agent group-join ?
  X:X:X:X::X multicast group address
```

Step 9 Check the multicast agent port, interface, and groups:

Example:

```
show wpan 0/1/0 mcast-agent ?
 group-join multicast group address
 interface mcast-interface
 ports Mcast optional ports
```

Configuring RPL

Resilient Mesh Endpoints (RMEs) perform routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL). For information about RPL, refer to "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

To determine the available RPL functions, query the **rpl** command:

```
Router(config)#int WPAN 0/1/0
Router(config-if)#rpl ?
  dag-lifetime       RPL DAG lifetime
  dag-lifetime-unit  RPL DAG lifetime unit in seconds
  dio-dbl            RPL DIO dbl value
  dio-min            RPL DIO min value
  option             RPL option configuration for wisun mode
  pon                RPL PON configuration
  route-poisoning    Route poisoning
  storing-mode       Storing mode
  version-incr-time  Version increment time in minutes
```

Parameter	Range	Description
dag-lifetime	Value between 1 and 255	Destination-Oriented Directed Acyclic Graph (DODAG) lifetime duration. Each node uses the lifetime duration parameter to drive its own operation (such as Destination Advertisement Object (DAO) transmission interval). Also, the router uses this lifetime value as the timeout duration for each RPL routing entry.
dag-lifetime-unit	Value between 60 and 3600	DAG lifetime unit in seconds.

Parameter	Range	Description
dio-dbl	Value between 0 and 9	DODAG Information Object (DIO) double parameter. DIO double is a doubling factor parameter used by the RPL protocol. **Caution** This command must only be used by an expert RPL protocol administrator.
dio-min	Value between 14 and 23	Minimum DIO value. **Caution** This command must only be used by an expert RPL protocol administrator.
pon	PON RPL instance.	Power Outage Notification (PON).
version-incr-time	Value between 10 and 255	Minimum time between RPL version increments.

Enabling the RPL PON Instance

The RPL Power Outage Notification (PON) instance is used in the power outage report. (See Configuring the Power Outage Server, on page 119.)

If you enable this option, the node uses the new PON instance in the outage report. If this option is disabled, the node uses the original RPL instance to report the outage event.

Note This option is supported only in WiSUN mode.

```
Router(config)#int WPAN 0/1/0
Router(config-if)#rpl pon ?
  dio-dbl   RPL PON DIO dbl value
  dio-min   RPL PON DIO min value
  instance  Enable RPL PON instance
Router(config-if)#rpl pon instance
```

Configuring Redistribution of RPL in Other Routing Protocols

On IR8100 Series routers, routes learned from RPL can be redirected to other routing protocols directly. The route type is RL instead of connected in the ipv6 routing table. The following commands show redistribution of RPL to the OSPF protocol:

```
Router(config)#ipv6 router ospf 100
Router(config-rtr)#redistribute rpl metric 3
```

Configuring 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.

To configure the power outage server, use the **outage server** command to specify an IPv6 address or IPv6 resolvable FQDN of a server. For example:

```
Router(config-if)# outage server 2001:c1::8a43:e1ff:fec3:2aa
```

or

```
Router(config-if)# outage server fnd.cisco.com
```

Configuring Cisco Resilient Mesh Security

RMEs use the IEEE 802.1X protocol, known as Extensible Authentication Protocol over LAN (EAPOL), for authentication.

Note Cisco Resilient Mesh does not support TLS 1.1. If the RADIUS server does not support TLS1.2, you need to disable TLS 1.1 on the RADIUS server for compatibility.

Configuring Mesh Key

Procedure

Step 1 Set the mesh key using the command **mesh-security set mesh-key interface wpan <slot>/<port> key <hex-string>**, where <hex-string> is an even number of hex digits, up to 32.

Example:

```
Router# mesh-security set mesh-key interface wpan 0/1/0 key 1234567891234567
```

Step 2 To configure mesh lfn key, use the **mesh-security set mesh-lfn-key**command.

Example:

```
Router# mesh-security set mesh-lfn-key interface wpan 0/1/0 key 12312311
```

Step 3 To configure the mesh key lifetime, use the **mesh-security mesh-key lifetime** command in interface configuration mode.

The **mesh-key lifetime** value should be less than 120 days (10368000 seconds).

Caution Use this command only if you are an expert mesh-security administrator.

Example:

```
Router(config)#int wpan 0/1/0
Router (config-if)# mesh-security mesh-key lifetime 60
```

Note Mesh-Security configuration and keys do not appear in **show running-config** or **show startup-config** command output.

Step 4 To configure lfn mesh-key lifetime, use the following commands:

Example:

```
mesh-security mesh-lfn-key revocation-lifetime-reduction 30
mesh-security mesh-lfn-key rollover-ratio 180
mesh-security mesh-lfn-key lifetime 7776000 ptk-lifetime 31104000 pmk-lifetime 46656000
```

Example Cisco Resilient Mesh Security Configuration

The following 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

Use the following commands to verify Cisco Resilient Mesh Security configuration:

- **show dot1x all details**

  Displays the configuration and clients of the Cisco Resilient Mesh 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).

```
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
```

- show mesh-security keys lfn

```
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
```

- **show mesh-security keys**

  Displays the mesh-security set-key configuration.

```
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
```

- **show mesh-security session all**

  Displays Cisco Resilient 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).

```
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..
```

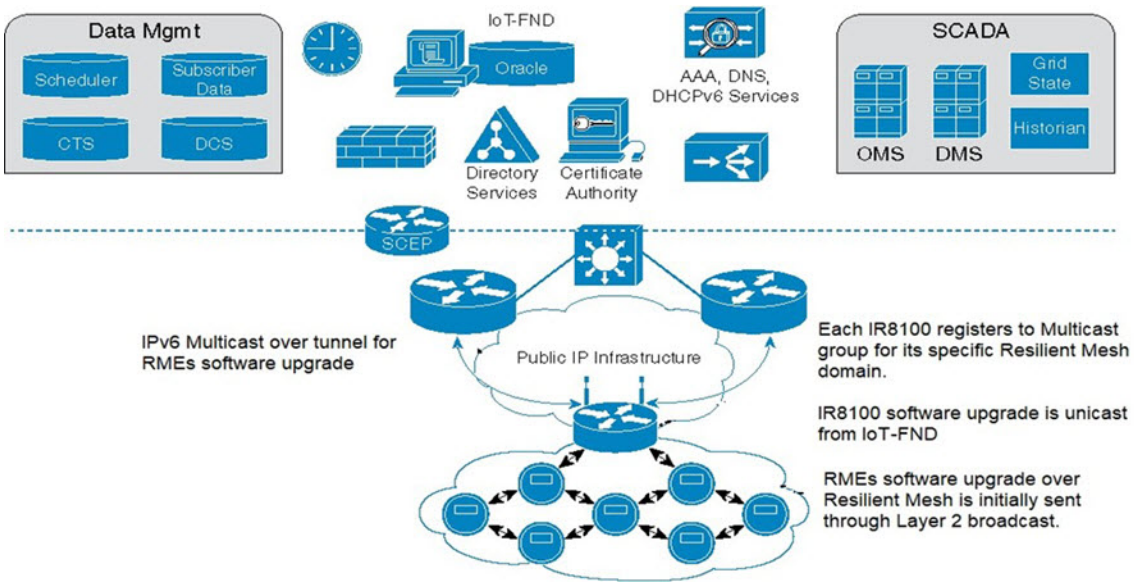
- **show mesh-security interface wpan <slot >/<port >**

Configuring the IPv6 Multicast Agent

You must configure an IPv6 multicast agent to enable 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.

IPv6-multicasting requires proper configuration on the head-end router (Cisco ASR 1000) as well as on IoT FND and the AMI head-end server.

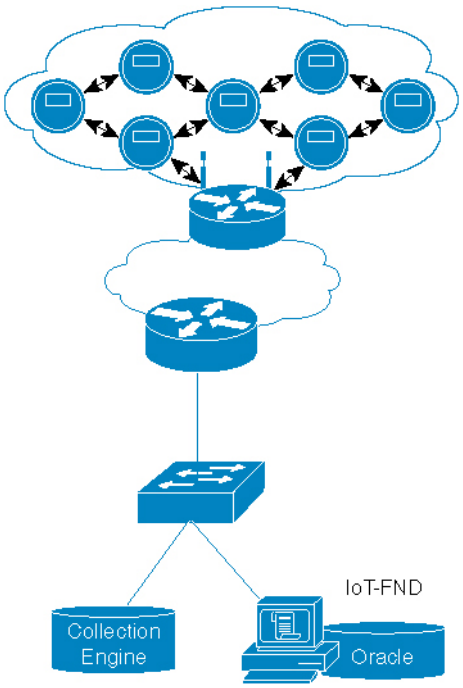
The following figure shows an IPv6 FAN with a multicast configuration.



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 following figure shows an overview of the Multicast operation in an 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.

Configuring IR8100 as PIM6 Router

The preferred method of forwarding multicast traffic to the IR8100 is to enable ipv6 multicast routing on the IR8100 and configure it as a PIM6 router. Because the unicast-prefix-based multicast address is still needed for WPAN, you must configure it under loopback0 on the IR8100, and configure the IR8100 to become a PIM-neighbor with the ASR head-end.

To configure this method, perform the following steps on the IR8100:

Procedure

Step 1 Enable IPv6 multicast-routing:

Example:

```
Router(config)# ipv6 multicast-routing
```

Step 2 Configure MLD under the loopback0:

Example:

```
Router(config-if)# interface loopback 0
Router(config-if)# ipv6 mld join-group ff38:40:2001:0db8:beef:cafe:0:1
```

Step 3 Configure the IPv6 PIM Rendezvous Point (RP):

Example:

```
Router(config)# ipv6 pim rp-address 2333::1
```

Example

ASR/CSR configuration 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
```

Configuring DTLS Relay for EST

The Cisco Resilient Mesh uses Enrollment over Secure Transport (EST) over CoAP/DTLS/UDP for certificate enrollment. During the initial bootstrapping process, nodes that have already joined the network (enrolled and authenticated) act as Datagram Transport Layer Security (DTLS) relays for nodes being bootstrapped.

Use the **dtls-relay** command in interface configuration mode to configure DTLS relay:

```
Router(config)#interface wpan 0/1/0
Router (config-if)#dtls-relay ?
X:X:X:X::X   IPv6 address (aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh, aaaa::bbb)
Router(config-if)#dtls-relay 2060:FACD::6 ?
lifetime     specify session lifetime
max-sessions specify maximum number of sessions
port         destination port
Router(config-if)#dtls-relay 2060:FACD::6 port 61629 max-sessions 10 lifetime 300
```

Use the **show wpan 0/1/0 config** command to verify the DTLS relay configuration.

Configuring Wi-SUN Mode

Wireless Smart Utility Network (Wi-SUN) mode is supported from Cisco Resilient Mesh Release 6.1.

Note

- Cisco Resilient Mesh Release 6.3 only supports Wi-SUN mode.
- Changing wisun-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 affect after 3 DIO messages are sent. Validate the connectivity to the IR8100 router.

To enable Wi-SUN mode, follow these steps:

Procedure

Step 1 Enter configuration mode:

Example:

```
Router#configure terminal
```

Step 2 Specify the WPAN interface and enter interface configuration mode:

Example:

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

Step 3 Enable wi-sun mode:

Example:

```
Router(config-if)#wisun-mode
```

Step 4 Set the beacon version increase interval to 0:

Example:

```
Router(config-if)#ieee154 beacon-ver-incr-time 0
```

Step 5 Set the phy mode to wisun supported phy mode:

Example:

```
Router(config-if)#ieee154 phy-mode 66
```

Step 6 (Optional) Change ucast dwell, bcast dwell, and bcast interval.

If not configured, all the parameters use the default values.

Example:

```
Router(config-if)#ieee154 wisun-dwell ucast-dwell-int <125> bcast-dwell-int <125> bcast-int
 <500>
```

Modulation and Data Rate (MDR)

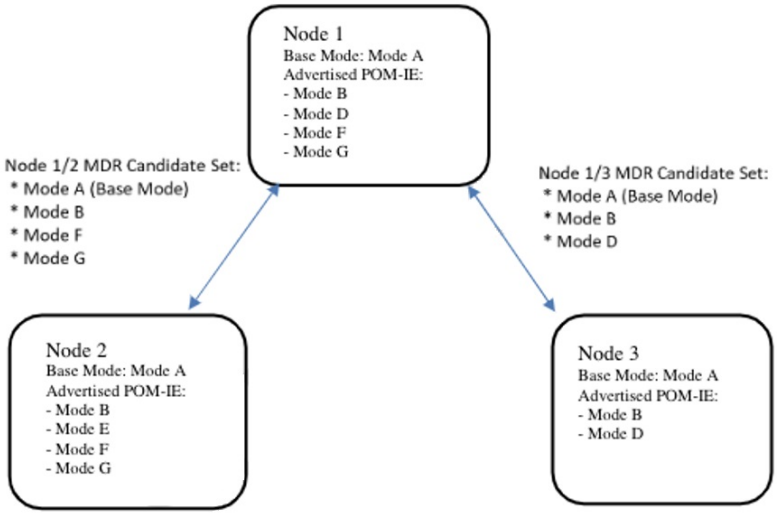
FAN networks typically consist of devices with different physical layer capabilities. The wireless links between different devices in the network may vary greatly due to distance, transmission power, noise, or other interference. Because of these differences, devices should be able to adapt the data 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.

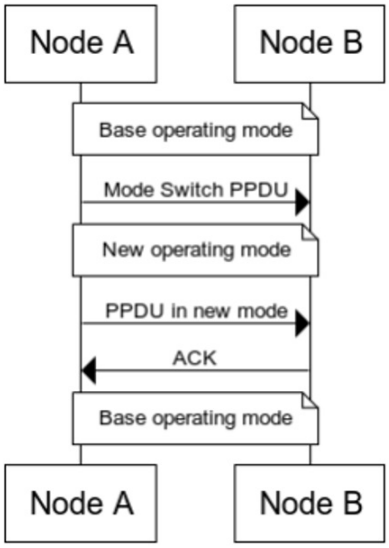
Supported platforms and software releases:

- Border Router: IR8140H, Cisco IOS XE Dulin 17.11.1
- Endpoint: IR510, IR530, WPAN (OFDM and FSK modules), Cisco Resilient Mesh Release 6.6

Selection of PHY Operating Mode and Switching

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

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.

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.

MDR Configuration

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

```
▼ phyModeList
  ▼ PhyModeInfo
      phyMode          0x40 (64)
      txPower          30 dBm
  ▼ PhyModeInfo
      phyMode          0x90 (144)
      txPower          28 dBm
  ▼ PhyModeInfo
      phyMode          0x93 (147)
      txPower          26 dBm
    bandID             4
    networkScale       small (1)
```

Verifying the Configuration

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 Node (LFN)

Limited Function Nodes (LFNs) are battery powered end devices. Battery lifetime is expected in the range of 15 to 20 years. LFNs are RPL leaf nodes in the Mesh network, therefore LFNs are relieved of RPL routing functionality. LFN cannot be the parent of other nodes in the Mesh network. Wi-SUN FAN 1.1v5 details the implementation of LFN node in a FAN Mesh network. LFN node has its own unicast interval, broadcast schedule, mesh keys in a FAN.

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

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.

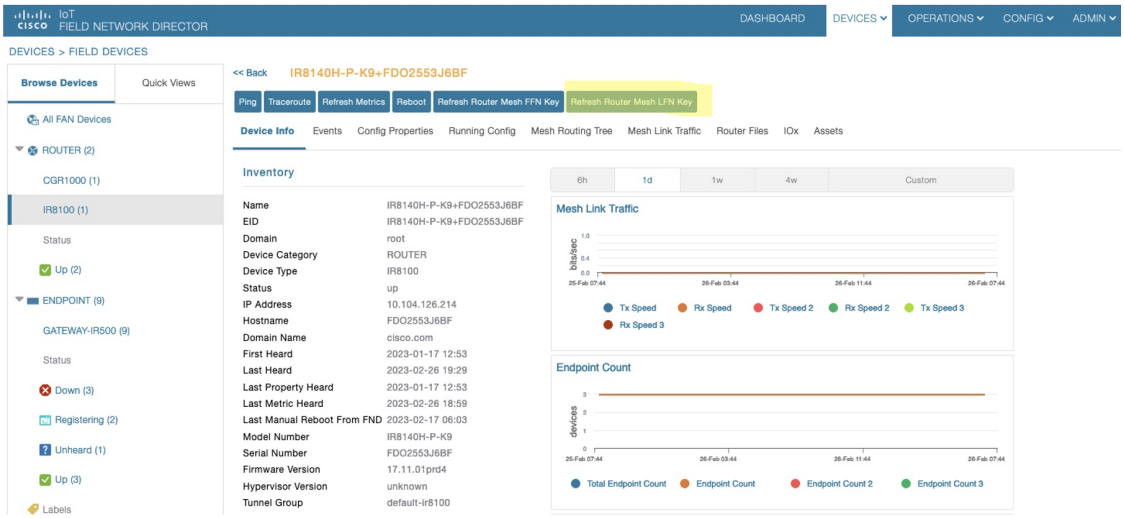
```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#mesh-security key-exchange-message-timeout 30
```

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



Verifying the Configuration

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

From Cisco IOS-XE Release 17.14.1, the IR8140 routers support direct parenting of Limited Function Nodes (LFNs) in Wi-SUN Mesh deployments. LFNs are the battery-powered low-energy endpoints typically used for utility metering of electricity, gas, and water. Several such LFN endpoints connect to a border router forming a sensor network to implement an Advanced Metering Infrastructure (AMI) deployment. LFN endpoints can connect to IR8140 as a child but cannot parent other devices in a Mesh network.

Previous releases supported IR8140 indirectly parenting LFNs through a partner Full Function Node (FFN) device. For more information, see Limited Function Node.

Use the following command to determine if the router has enabled LFN support:

```
IR8140#show wpan 0/2/0 hardware configuration
lfn support: Enabled
```

Use the following command 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
```

Verifying WPAN Configuration

Use WPAN show and debug commands to view WPAN configuration or troubleshoot operation.

To see all WPAN show commands, enter the following command:

```
Router# show wpan 0/1/0 ?
  config             Configuration information
  data-rate          Data rate during last 1 minute
  eap-table          Recent EAP node table
  hardware           Hardware information
  ieee154            IEEE 802.15.4 related information
  ieeep19012         IEEE P1901.2 related information
  link-neighbors     Layer 3 link neighbor information
  module-type        Module type (RF or PLC)
  oui-table          OUI mapping table for 8-to-6 MAC address translation
                     (EUI64 <-->IEEE MAC)
  outage-server      WPAN outage server
  outage-table       WPAN outage table
  packet-count       Packet counts
  restoration-table  WPAN restoration table
  rpl                RPL related information
  service-state      WPAN service state
  slave-mode         Slave mode
```

The following table describes some WPAN show commands and debug command.

Command	Description
show wpan config	Displays the WPAN basic configuration.
show wpan hardware	Displays WPAN hardware information. Enter **show wpan 0/1/0 hardware ?** to see a list of options. **Note** The output of the command **show wpan <slot >/1 hardware key** shows mesh-security keys (GTKs) that reside on the WPAN hardware. The **show wpan <slot>/1 hardware key** output should agree with the output of **show mesh-security-keys**. The **show wpan <slot>/1 hardware link-neighbor** command shows the list of recently heard IEEE 802.15.4 link neighbors. These link neighbors are RMEs within a 1-hop transmit range from the IR8100 and from which the IR8100 has recently heard IEEE 802.15.4 frames. The list shows only the most recently heard subset from all possible 1-hop neighbors.
show wpan packet-count	Displays incoming and outgoing packet counts for WPAN traffic.

Command	Description
show wpan link-neighbors	Shows the information about the WPAN link neighbors. These link neighbors are RMEs within a 1-hop transmit range from the IR8100 that sent at least one IPv6 or IEEE 802.1X packet to the CGR during the last hour. **Note** The minimum RSSI to join a mesh network is -95 dBm; a lower RSSIF/RRSIR value will not allow the node to establish connectivity.
show wpan outage-table	Shows recent power-outage notification (PON) events in the PAN during the past hour.
show wpan restoration-table	Shows recent power restoration notification (PRN) events in the PAN during the past hour.
show wpan rpl	Displays WPAN RPL information. Enter **show wpan 0/1/0 rpl ?** to see a list of options.
debug wpan all	Displays all WPAN debugging messages, including errors, fan-mpl, info, packets, and rpl.

Example IR8100 Basic WPAN Configuration

The following example is for a IR8100 with a basic WPAN configuration.

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.

```
IR8140H #sh run
Building configuration...

Current configuration : 24773 bytes
!
! Last configuration change at 21:43:01 PST Sun Dec 6 2020 by iox
! NVRAM config last updated at 21:16:59 PST Fri Dec 4 2020 by iox
!
version 17.5
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname IR8140H
!
boot-start-marker
```

```
boot system flash bootflash:ir8100-universalk9.BLD_POLARIS_DEV_LATEST_20201118_061101.SSA.bin
boot-end-marker
!
!
!
aaa new-model
!
!
aaa group server radius aaa-radius-group
 server name aaa-radius-server
!
aaa authentication login default local
aaa authentication dot1x default group aaa-radius-group
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
!
aaa session-id common
aaa password restriction
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
!
!
!
!
!
!
!
!
login on-success log
ipv6 unicast-routing
ipv6 dhcp database flash:/DHCP-DB write-delay 60
ipv6 dhcp pool MeterNetwork
 prefix-delegation pool MeterNetwork lifetime 1814400 1360800
 address prefix AAAA:BBBB:CCCC:3::/112 lifetime 1814400 1360800
 vendor-specific 26484
  suboption 1 address 3000::4
  suboption 2 address 3000::5
!
ipv6 multicast-routing
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
parameter-map type webauth global
 watch-list dynamic-expiry-timeout 0
!
```

```
multilink bundle-name authenticated
!
!
!
!
!
!
!
access-session mac-move deny
!
!
crypto pki trustpoint LDevID
 enrollment retry count 10
 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:FDO2420J79N,CN=IR8140H_FDO2420J79N
 revocation-check none
 rsakeypair LDevID 2048
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-138894244
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-138894244
 revocation-check none
 rsakeypair TP-self-signed-138894244
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_22_57_57_UTC_Thu_Dec_3_2020
 revocation-check none
!
crypto pki profile enrollment LDevID
 enrollment url  http://ca.iok.cisco.com/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 LDevID
 certificate 5B00005E81DF0B79B1968437E1000000005E81
  308205B3 3082049B A0030201 0202135B 00005E81 DF0B79B1 968437E1 00000000
  5E81300D 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 31323033 32323531
  30385A18 0F323036 30313132 33323235 3130385A 30483128 30260603 55040513
  1F504944 3A495238 31343048 2D502D4B 3920534E 3A46444F 32343230 4A37394E
  311C301A 06035504 030C1349 52383134 30485F46 444F3234 32304A37 394E3082
  0122300D 06092A86 4886F70D 01010105 00038201 0F003082 010A0282 010100B0
  1C3E3320 97FF0E0F 583A7D41 8E7EA4E0 94CC6797 7CC99CEC 1742BBEE BD810E10
  EEE9B8BD F7AE212D AE17D1BD 40269478 1DB95762 7A157557 F1CFE31D 68A6FABE
  26E80E3E F98004DD 8AEA6DC6 95510EC1 96178014 8EB23D2A E35EF02A 820DDCE9
  4316EEE4 86830E86 09D64A02 1DDD26B4 7664378E 90EC8435 FAD9DC8A 269DF984
  91AB0047 029051A2 11BEBB8C 947700DD 48C32030 6CF19F6E 6218AD1F D06F611A
  57DA077C 45E97DEF 2441EC3F 6CD72D08 B2B34653 1901A30B 869792A7 6356A900
```

```
  E8C76625 AFE8318F 7728C40B 05D12D3D 4B56B553 A5CA6241 4B042ED4 259088C1
  7C9E7CAD 7708C4B7 89CD5973 20E5B17C A81F01DA 89553289 FCD88605 2E805102
  03010001 A382027B 30820277 300B0603 551D0F04 04030204 F0301D06 03551D0E
  04160414 A0895FE6 72E3C526 DC18D1AE 64A2E846 91B942A0 301F0603 551D2304
  18301680 1422A59D B25D909E DA074C00 39B59575 B3F8898F 533081D5 0603551D
  1F0481CD 3081CA30 81C7A081 C4A081C1 8681BE6C 6461703A 2F2F2F43 4E3D7369
  742D6463 2D534954 2D44432D 43412C43 4E3D7369 742D6463 2C434E3D 4344502C
  434E3D50 75626C69 63253230 4B657925 32305365 72766963 65732C43 4E3D5365
  72766963 65732C43 4E3D436F 6E666967 75726174 696F6E2C 44433D73 69742D64
  632C4443 3D636973 636F2C44 433D636F 6D3F6365 72746966 69636174 65526576
  6F636174 696F6E4C 6973743F 62617365 3F6F626A 65637443 6C617373 3D63524C
  44697374 72696275 74696F6E 506F696E 743081CA 06082B06 01050507 01010481
  BD3081BA 3081B706 082B0601 05050730 028681AA 6C646170 3A2F2F2F 434E3D73
  69742D64 632D5349 542D4443 2D43412C 434E3D41 49412C43 4E3D5075 626C6963
  2532304B 65792532 30536572 76696365 732C434E 3D536572 76696365 732C434E
  3D436F6E 66696775 72617469 6F6E2C44 433D7369 742D6463 2C44433D 63697363
  6F2C4443 3D636F6D 3F634143 65727469 66696361 74653F62 6173653F 6F626A65
  6374436C 6173733D 63657274 69666963 6174696F 6E417574 686F7269 7479303B
  06092B06 01040182 37150704 2E302C06 242B0601 04018237 15088593 BB6B8585
  8C6C8289 810E86C7 AC03E7EF 037D84B1 A57EB4FB 34020164 02010730 1D060355
  1D250416 30140608 2B060105 05070301 06082B06 01050507 03023027 06092B06
  01040182 37150A04 1A301830 0A06082B 06010505 07030130 0A06082B 06010505
  07030230 0D06092A 864886F7 0D01010B 05000382 010100AA F097FF39 BF324E9B
  9D469801 1EBA004A 0308BB2A 737576A7 F32F9323 F963233D 9431E83A 66E77B74
  B4F5D25B 6D746729 E38EF0FA D50A77C4 C37E9FD6 B45DED13 8600F7EE 91AD2D90
  B1361A82 E5C59706 B36FC8BE A6AD4949 EB58817F 8AEE3E63 91E0D7BF 1248AE8D
  3EEB0D41 47458C36 4B172593 81561D71 E4204D86 8E2E264C FBB74463 1CA8315A
  C5F98B8E 6FE4C2D5 84A0F922 3A3E5FE8 74405FEB 3E53AF71 A45D81B6 92FC66C1
  7A907EBC F28A497B 64FA458D 90A16A32 5370169B AC92EE7C 26B1BF0A 254F05CC
  2977143A DAE495D4 A53EC612 224745D2 2E74D281 AF8911C2 FC865C4A F5ACA85D
  6C3D6292 AB40CAB9 C4E5E536 2A1D0FC1 D20D8DE0 DF0CE0
        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
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-138894244
 certificate self-signed 01
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31333838 39343234 34301E17 0D323031 32303332 32353735
  305A170D 33303132 30333232 35373530 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3133 38383934
  32343430 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 B6A01EE3 667B8D0E EF1BC93C 6F5925CA 9C4223CC 37FC5F61 53264E2D
  E5D89F9B A4B32F70 732C76F0 ECBABD98 B53EEBD3 6411EB5E F66F6C23 F6E20FE7
  2E2BA210 0E82D6D2 DC99670A 00A511D4 8006BD04 0ED4928C 0187028C 9513FA42
  61C41C4A D37D249E 7F331130 769CC58A C06AA7EB 48CCF781 C11549FF A2289F13
  CEBE4076 D58280A2 015689DA 4AC29732 5BB395B8 A3E94411 1EC943AC DA949659
  592FFEE6 1F40FE6C A9736E1A 1A4D7D4C 54B2DD87 AF20AAED 5D139637 F9816736
  2AC0E22A 86981E8C F56EBD49 0EA893E1 E3A14D59 4503EC8A B578A4F3 E8C6ADDA
  35B6324C 751F714A 874483DB 1974F177 753FC641 8CBB04FC 1C5BE284 1A637231
  B9E90233 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 23041830 1680146D 23D38934 824F75AC 853375D6 557CE3E4 5A252830
  1D060355 1D0E0416 04146D23 D3893482 4F75AC85 3375D655 7CE3E45A 2528300D
  06092A86 4886F70D 01010505 00038201 0100A685 7A44E9DD E4185176 742D91A8
  3FBC514C EA66F095 3D6202DB E730B178 99DB7C4E 9CA8F398 E9F9306A BCAFC0B1
  27458D65 72A202CE 55B42843 E71743EA 347EEBDD 10BDC71E 5840BEAC 627B25C1
  F7FDE729 7E1011F4 1A160803 CF1CED13 4AFB4402 CEAB7F5C A9E4C783 711062A3
  3F551D7F 58A847C9 C0C4D8BE 576DEFA1 A2383F74 BDF0ABEE 17FB784B 32DDFE16
  AEE23933 979A4C9E 2545114F 651206DD C668FA4C 2D54CCD7 87D22AE8 52D240F7
  8E5548B7 F411BE02 0DA89663 779794B0 90C4B69C 935E584B C9E945E7 40C17C69
  AC5E71AA 274C6363 7438F423 0C139869 68A399D6 97662323 E9543C9A A185B589
  F8977558 EEADBC59 F8C60924 E68E2BF7 3E69
       quit
crypto pki certificate chain fnd
 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 FDO2420J79N
license boot level network-advantage
archive
 path bootflash:/archive/fnd_
 maximum 8
memory free low-watermark processor 47508
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
 linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
dot1x system-auth-control
!
username iox privilege 15 secret 8
$8$MCZ4.RbP0h3mhk$oD4slpuk7rxM8A1Q4sVfct5i.90A91bSQ.Z0BOXJghk
username admin privilege 15 secret 8
$8$EPbjkRKro7I9G.$XEDUTW4a7kSfE4Eg57AdaC9UqHxks/.mFHAZ44nFsPw
username cg-nms-administrator privilege 15 secret 8
$8$EvudyM9Ko4qx5E$1jwTxrgxTgzkH2pkGPHa9vvP/jBMHffknWiBn2dBYWk
!
redundancy
```

```
 mode none

!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_IPv4_LAN
 route set access-list ipv6 FlexVPN_Client_IPv6_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
  peer 1 1001::3
  client connect Tunnel10
!
!
controller Cellular 0/2/0
!
!
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match result-type aaa-timeout
 match authorization-status authorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
!
```

```
!
policy-map type control subscriber POLICY_WP0/1/0
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
!
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 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 Loopback0
 ip address 10.10.10.34 255.255.255.255
 ipv6 address 2000::182B/128
!
interface Tunnel10
 description IPsec tunnel to CISCO-IOK-HER
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1362
 ipv6 tcp adjust-mss 1302
 ipv6 ospf 10 area 10
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre ipv6
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup0
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip address dhcp
```

```
 negotiation auto
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
 ipv6 nd ra suppress all
 ipv6 dhcp client request vendor
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface Cellular0/2/0
 ip address negotiated
 ipv6 enable
!
interface Cellular0/2/1
 no ip address
 shutdown
!
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
!
router ospfv3 10
 !
 address-family ipv6 unicast
 exit-address-family
!
iox
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-client-auth
ip http secure-trustpoint LDevID
ip http max-connections 10
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client connection forceclose
ip http client source-interface Loopback0
ip http client secure-trustpoint LDevID
ip forward-protocol nd
ip tftp source-interface GigabitEthernet0/0/1
ip ssh rsa keypair-name LDevID
ip ssh version 2
!
!
ip access-list standard FlexVPN_Client_IPv4_LAN
 10 permit 10.10.10.34
```

```
!
!
ip radius source-interface Loopback0
!
snmp-server group cgnms v3 priv
snmp-server community readonly RO
snmp-server community readwrite RW
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps wpan
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server enable traps c3g
snmp-server host 3000::4 version 3 priv cg-nms-administrator
!
!
!
!
radius server aaa-radius-server
 address ipv6 3000::6 auth-port 1812 acct-port 1813
 key Cisco12345!
!
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
 sequence 20 permit ipv6 host 2000::182B any
 sequence 30 permit ipv6 AAAA:BBBB:CCCC:2::/64 3000::/112
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 length 0
 transport preferred none
 stopbits 1
 speed 115200
line vty 0 4
 session-timeout 10
 exec-timeout 0 0
 length 0
 transport preferred none
 transport input all
line vty 5 15
 session-timeout 10
 exec-timeout 0 0
 privilege level 15
 length 0
 transport preferred none
 transport input all
!
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 ntp.iok.cisco.com
ntp server her.iok.cisco.com
!
wsma agent exec
 profile exec
!
wsma agent config
 profile config
!
!
!
!
wsma profile listener exec
 transport https path /wsma/exec
!
wsma profile listener config
 transport https path /wsma/config
!
cgna gzip
!
cgna heart-beat interval 1
cgna heart-beat active
!
cgna profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 2
 url https://tps.iok.cisco.com:9120/cgna/ios/tunnel
 gzip
!
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://fnd.iok.cisco.com:9121/cgna/ios/registration
 gzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 hardware version | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 rpl brief | format flash:/managed/odm/cg-nms.odm
```

```
 add-command show wpan 0/1/0 conf | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 packet-count | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/2/0 all | format flash:/managed/odm/cg-nms.odm
 interval 1
 url https://fnd.iok.cisco.com:9121/cgna/ios/metrics
 gzip
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 180
event manager directory user policy "tmpsys:/eem_policy"
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass
!
app-hosting appid sparrow_iperf_app_1
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.0.2 netmask 255.255.255.0
 app-default-gateway 192.168.0.1 guest-interface 0
gnxi
gnxi server
netconf-yang
end
```

Example IR8100 Configuration for CG-Mesh

The following example shows the configuration for an IR8100 in a Cisco Resilient Mesh network.

```
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
```

Example ASR Configuration for CG-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 4B8801480001000000FC
 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#
```

Checking and Upgrading the WPAN Firmware Version

This section describes how to check the WPAN hardware and firmware versions and perform firmware upgrades. For the IR8100, only IRMH WPAN is supported and the minimum version is 6.2.19.

Note WPAN firmware is not integrated in IR8100 firmware and must be upgraded separately.

To check the version of the WPAN hardware in slot 1, run the following command:

```
Router# sh wpan 0/1/0 hardware hwversion
hardware version: CGM-WPAN, 1.0, IRMH-WPAN/1.0/2.0
```

To check the installed firmware version of the WPAN, run the following command:

```
Router# sh wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```

The **show wpan <slot>/1 config** command also displays the WPAN firmware version:

```
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)
```

Upgrading WPAN Firmware

The appropriate WPAN firmware image must be copied and available on the IR8100 flash in the root directory.

To upgrade the WPAN firmware, follow these steps:

Procedure

Step 1 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 Power down the WPAN module:

Example:

```
Router# config t
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

Step 3 Wait for WPAN power-down messages, and then wait another 60-90 seconds. Then, power up the module:

Example:

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

Step 4 Wait for WPAN power-up messages, and then wait at least 500 seconds before proceeding with any task on a WPAN under reload. Then, check WPAN status and hardware version:

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
```

Upgrading WPAN Firmware (CG-Mesh to WiSUN)

Follow these steps to upgrade the WPAN firmware from 6.2 to 6.3, which upgrades the WPAN module from cgmesh mode to wisun mode.

Procedure

Step 1 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 6.3 firmware successfully (94 sec).
Please reload the WPAN module in slot 1!!
```

Step 2 Enter configuration mode:

Example:

```
Router#configure terminal
```

Step 3 Specify the WPAN interface and enter interface configuration mode:

Example:

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

Step 4 Enable wi-sun mode:

Example:

```
Router(config-if)#wisun-mode
```

Step 5 Set the beacon version increase interval to 0:

Example:

```
Router(config-if)#ieee154 beacon-ver-incr-time 0
```

Step 6 Set the phy mode to wisun supported phy mode:

Example:

```
Router(config-if)#ieee154 phy-mode 66
```

Step 7 Exit interface configuration mode and return to privileged EXEC mode:

Example:

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

Step 8 Power down the WPAN module:

Example:

```
Router# config t
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

Step 9 Wait for WPAN power-down messages, and then wait another 60-90 seconds. Then, power up the module:

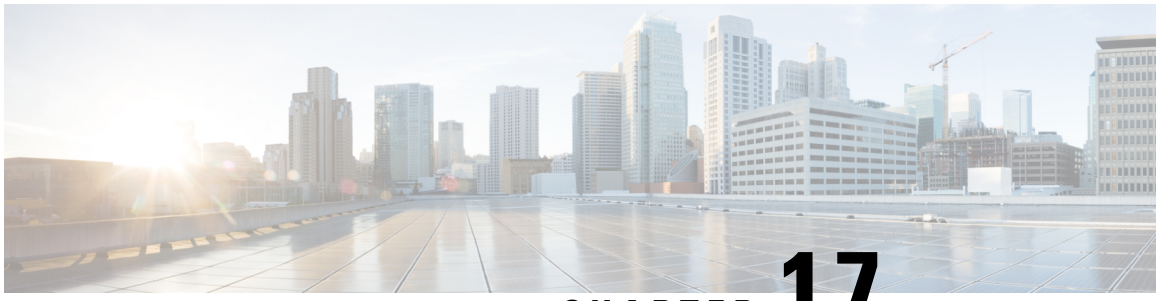
Example:

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

Step 10 Wait for WPAN power-up messages, and then wait at least 500 seconds before proceeding with any task on a WPAN under reload. Then, check WPAN status and hardware version:

Example:

```
Router# show ip interface brief | inc Wpan
  Wpan0/1/0                  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 17

System Messages

This chapter contains the following sections:

- System Messages, on page 157

System Messages

This chapter contains the following sections:

Information About Process Management

You can access system messages by logging in to the console through Telnet protocol and monitoring your system components remotely from any workstation that supports the Telnet protocol.

Starting and monitoring software is referred to as process management. The process management infrastructure for a router is platform independent, and error messages are consistent across platforms running on Cisco IOS XE. You do not have to be directly involved in process management, but we recommend that you read the system messages that refer to process failures and other issues.

How to Find Error Message Details

To show further details about a process management or a syslog error message, enter the error message into the Error Message Decoder tool at: https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi.

For example, enter the message `%PMAN-0-PROCESS_NOTIFICATION` into the tool to view an explanation of the error message and the recommended action to be taken.

The following are examples of the description and the recommended action displayed by the Error Message Decoder tool for some of the error messages.

Error Message: `%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]`

Explanation	Recommended Action

The process lifecycle notification component failed, preventing proper detection of a process start and stop. This problem is likely the result of a software defect in the software subpackage.	Note the time of the message and investigate the kernel error message logs to learn more about the problem and see if it is correctable. If the problem cannot be corrected or the logs are not helpful, copy the error message exactly as it appears on the console along with the output of the **show tech-support** command and provide the gathered information to a Cisco technical support representative.

Error Message: `%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

Explanation	Recommended Action
A process important to the functioning of the router has failed.	Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

Explanation	Recommended Action

A process that does not affect the forwarding of traffic has failed.	Note the time of the message and investigate the kernel error message logs to learn more about the problem. Although traffic will still be forwarded after receiving this message, certain functions on the router may be disabled because of this message and the error should be investigated. If the logs are not helpful or indicate a problem you cannot correct, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])`

Explanation	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. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.`

Explanation	Recommended Action
A process failure is being ignored due to the user-configured debug settings.	If this behavior is desired and the debug settings are set according to a user's preference, no action is needed. If the appearance of this message is viewed as a problem, change the debug settings. The router is not expected to behave normally with this debug setting. Functionalities such as SSO switchover, router reloads, FRU resets, and so on will be affected. This setting should only be used in a debug scenario. It is not normal to run the router with this setting.

Error Message: `%PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])`

Explanation	Recommended Action
The process was restarted too many times with repeated failures and has been placed in the hold-down state.	This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the **show logging** and **show tech-support** commands and your pertinent troubleshooting logs.

Error Message: `%PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]`

Explanation	Recommended Action
The route processor is being reloaded because there is no ready standby instance.	Ensure that the reload is not due to an error condition.

Error Message: `%PMAN-3-RELOAD_RP : Reloading: [chars]`

Explanation	Recommended Action

The RP is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-RELOAD_SYSTEM : Reloading: [chars]`

Explanation	Recommended Action
The system is being reloaded.	Ensure that the reload is not due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]`

Explanation	Recommended Action
The executable file used for the process is bad or has permission problem.	Ensure that the named executable is replaced with the correct executable.

Error Message: `%PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>`

Explanation	Recommended Action
The executable file used for the process is missing, or a dependent library is bad.	Ensure that the named executable is present and the dependent libraries are good.

Error Message: `%PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]`

Explanation	Recommended Action
The executable file used for the process is empty.	Ensure that the named executable is non-zero in size.

Error Message: `%PMAN-5-EXITACTION : Process manager is exiting: [chars]`

Explanation	Recommended Action
The process manager is exiting.	Ensure that the process manager is not exiting due to an error condition. If it is due to an error condition, collect information requested by the other log messages.

Error Message: `%PMAN-6-PROCSHUT : The process [chars] has shutdown`

Explanation	Recommended Action
The process has gracefully shut down.	No user action is necessary. This message is provided for informational purposes only.

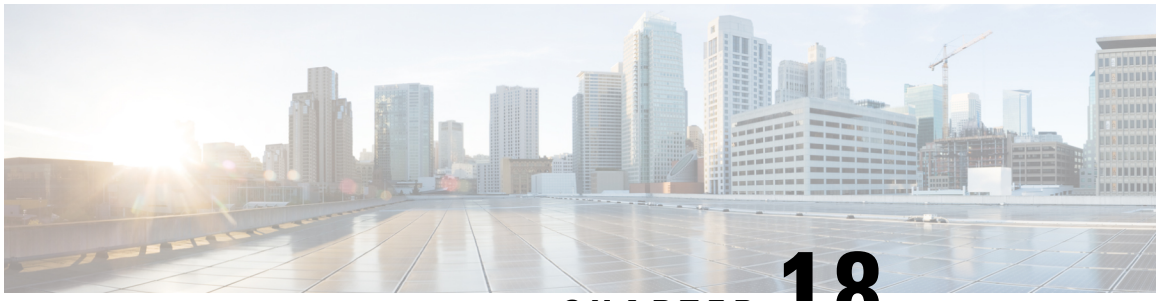
Error Message: `%PMAN-6-PROCSTART : The process [chars] has started`

Explanation	Recommended Action

The process has launched and is operating properly.	No user action is necessary. This message is provided for informational purposes only.

Error Message: `%PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless`

Explanation	Recommended Action
The process has requested a stateless restart.	No user action is necessary. This message is provided for informational purposes only.



CHAPTER 18

Environmental Monitoring

- Environmental Monitoring, on page 163

Environmental Monitoring

Environmental Monitoring

The router provides a robust environment-monitoring system with several sensors that monitor the system temperatures. The following are some of the key functions of the environmental monitoring system:

- Monitoring temperature of CPUs and Motherboard
- Recording abnormal events and generating notifications
- Monitoring Simple Network Management Protocol (SNMP) traps
- Generating and collecting Onboard Failure Logging (OBFL) data
- Sending call home event notifications
- Logging system error messages
- Displaying present settings and status

Environmental Monitoring and Reporting Functions

Monitoring and reporting functions allow you to maintain normal system operation by identifying and resolving adverse conditions prior to loss of operation.

- Environmental Monitoring Functions, on page 163
- Environmental Reporting Functions, on page 164

Environmental Monitoring Functions

Environmental monitoring functions use sensors to monitor the temperature of the cooling air as it moves through the chassis.

The router is expected to meet the following environmental operating conditions

- Non-operating Temperature: -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.

The following table displays the levels of status conditions used by the environmental monitoring system.

Table 8: Levels of Status Conditions Used by the Environmental Monitoring System

Status Level	Description
Normal	All monitored parameters are within normal tolerance.
Warning	The system has exceeded a specified threshold. The system continues to operate, but operator action is recommended to bring the system back to a normal state.
Critical	An out-of-tolerance temperature or voltage condition exists. Although the system continues to operate, it is approaching shutdown. Immediate operator action is required.

The environmental monitoring system sends system messages to the console, for example, when the conditions described here are met:

Temperature and Voltage Exceed Max/Min Thresholds

The following example shows the warning messages indicating the maximum and minimum thresholds of the temperature or voltage:

```
Warnings :
--------
For all the temperature sensors (name starting with “Temp:”) above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).

For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

Environmental Reporting Functions

You can retrieve and display environmental status reports using the following commands:

- **show diag all eeprom**

- **show environment**
- **show environment all**
- **show inventory**
- **show platform**
- **show platform diag**
- **show platform software status control-processor**
- **show diag slot R0 eeprom detail**
- **show version**
- **show power**

These commands show the current values of parameters such as temperature and voltage.

The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are shown below:

show diag all eeprom: Example

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

Product Identifier (PID) : 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#
```

show environment: Example

```
Router# show environment
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0

Slot Sensor Current State Reading Threshold(Minor,Major,Critical,Shutdown)
---------- ------------- --------------- ------------ ------------------------------------
R0 Temp: LM75BXXX Normal 39 Celsius (80 ,85 ,90 ,na )(Celsius)

Router#
```

show environment all: Example

```
Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: LM75BXXX R0 Normal 48 Celsius
```

show inventory: Example

```
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:
```

show platform: Example

```
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#
```

show platform diag: Example

```
Router# show platform diagChassis 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#
```

show platform software status control-processor: Example

```
Router# show platform software status control-processorRP0: 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#
```

show diag slot R0 eeprom detail: Example

```
Router# show diag slot R0 eeprom detailSlot 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#
```

show version: 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


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#
```

show power: Example

```
Router# show powerMain 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

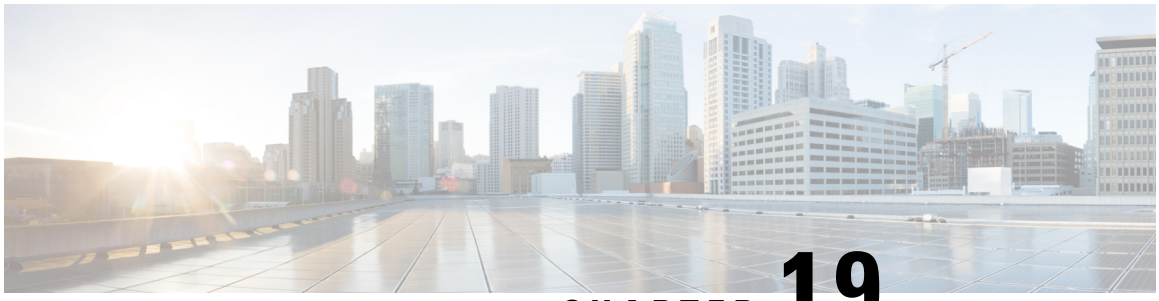
The following sections provide references related to the power efficiency management feature.

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

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. 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. 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 19

IOx Application Hosting

This section contains the following topics:

- Application Hosting, on page 175

Application Hosting

A hosted application is a software as a service solution, and it can be run remotely using commands. Application hosting gives administrators a platform for leveraging their own tools and utilities.

This module describes the Application Hosting feature and how to enable it.

Information About Application Hosting

Need for Application Hosting

The move to virtual environments has given rise to the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes. This ranges from automation, configuration management monitoring, and integration with existing tool chains.

Cisco devices support third-party off-the-shelf applications built using Linux tool chains. Users can run custom applications cross-compiled with the software development kit that Cisco provides.

IOx Overview

IOx is a Cisco-developed end-to-end application framework that provides application hosting capabilities for different application types on Cisco network platforms.

IOx architecture for the IR8100 is different compared to other Cisco platforms that use the hypervisor approach. In other platforms, IOx runs as a virtual machine. IOx runs as a process on the IR8100.

Cisco Application Hosting Overview

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.

Application hosting provides the following services:

- Launches designated applications in containers.

- Checks available resources (memory, CPU, and storage), and allocates and manages them.
- Provides support for console logging.
- Provides access to services via REST APIs.
- Provides a CLI endpoint.
- Provides an application hosting infrastructure referred to as Cisco Application Framework (CAF).
- Helps in the setup of platform-specific networking (packet-path) via VirtualPortGroup and management interfaces.

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. IOXMAN is based on the lifecycle of the guest application to enable and disable the tracing service, to send logging data to IOS syslog, to save tracing data to IOx tracelog, and to maintain IOx tracelog for each guest application.

Application Hosting on the IR8100 Industrial Integrated Services Router

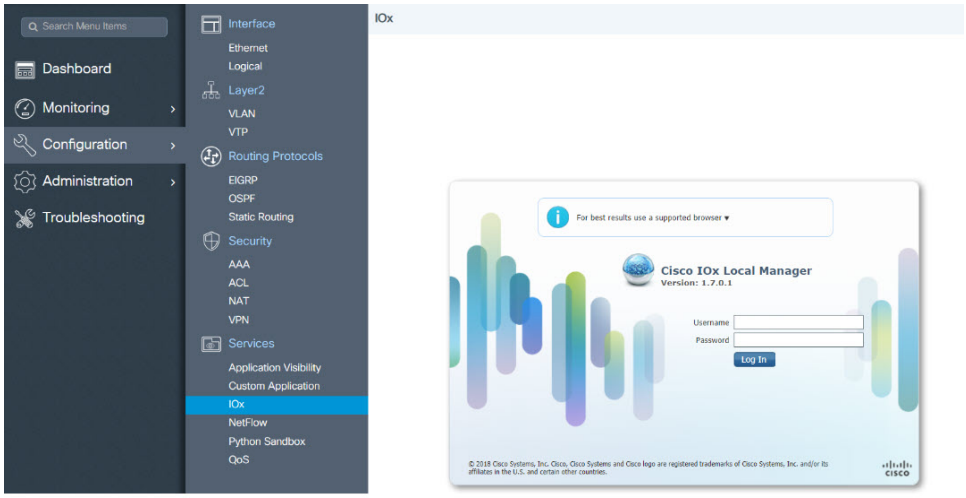
This section describes the application hosting characteristics specific to the IR8100.

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.

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 28: 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

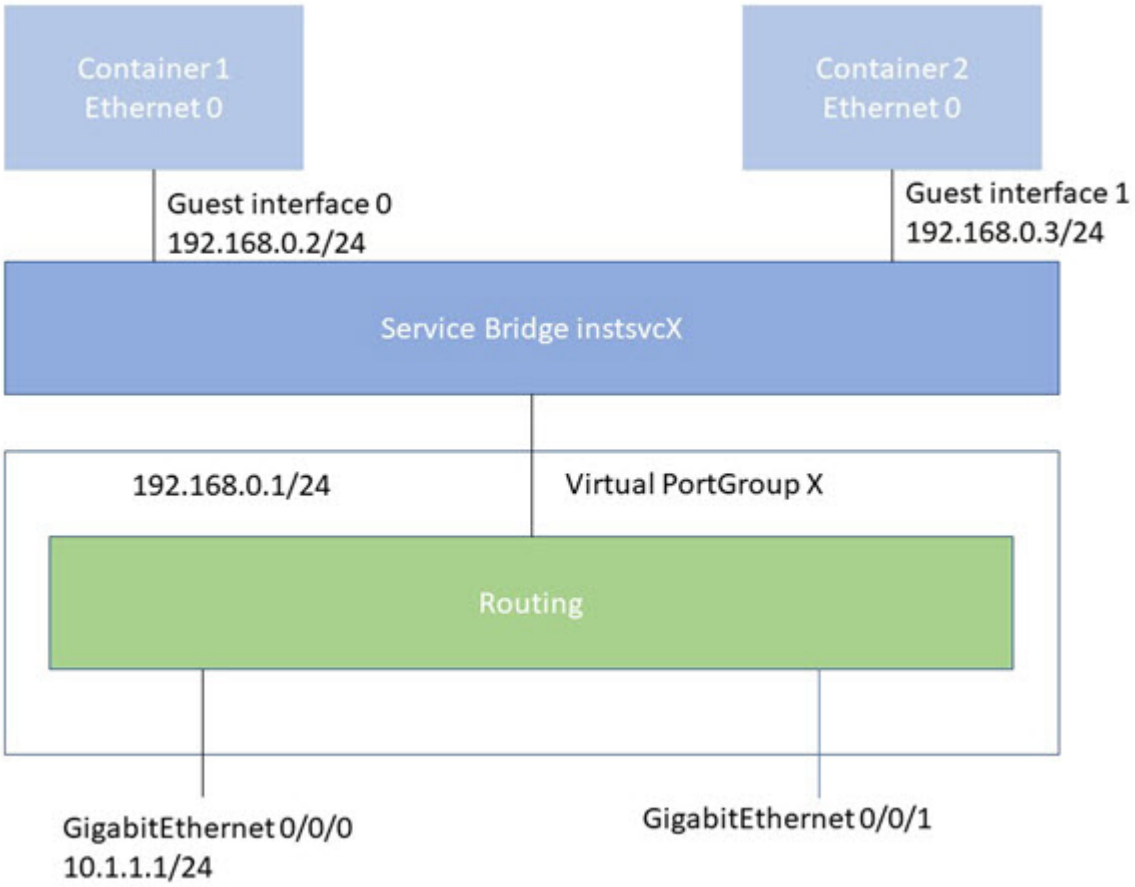
The VirtualPortGroup is a software construct on Cisco IOS that maps to a Linux bridge IP address. As such, the VirtualPortGroup represents the switch virtual interface (SVI) of the Linux container. Each bridge can contain multiple interfaces; each mapping to a different container. Each container can 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 following graphic helps to understand the relationship between the VirtualPortGroup and other interfaces, as it is different than the IR8x9 routers.

Figure 29: Virtual Port Group Mapping



vNIC

For the container life cycle management, the Layer 3 routing model that supports one container per internal logical interface is used. This means that a virtual Ethernet pair is created for each application; and one interface of this pair, called vNIC is part of the application container. The other interface, called vpgX is part of the host system.

NIC is the standard Ethernet interface inside the container that connects to the platform dataplane for the sending and receiving of packets. IOx is responsible for the gateway (VirtualPortGroup interface), IP address, and unique MAC address assignment for each vNIC in the container.

The vNIC inside the container/application are considered as standard Ethernet interfaces.

How to Configure Application Hosting

Enabling IOx

Perform this task to enable access to the IOx Local Manager. 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.

Note In the steps that follow, IP HTTP commands do not enable IOX, but allow the user to access the WebUI to connect the IOX Local Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **iox**
4. **ip http server**
5. **ip http secure-server**
6. **username** *name* **privilege** *level* **password** {**0** | **7** | *user-password* }*encrypted-password*
7. **end**

DETAILED STEPS

Steps	Command	Purpose
1.	**enable** Example: `Device>enable`	Enables privileged EXEC mode. Enter your password if prompted.
2.	**configure terminal** Example: `Device#configure terminal`	Enters global configuration mode.
3.	**iox** Example: `Device(config)#iox`	Enables IOx
4.	**ip http server** Example: `Device(config)#ip http server`	Enables the HTTP server on your IP or IPv6 system.
5.	**ip http secure-server** Example: `Device(config)#ip http secure-server`	Enables a secure HTTP (HTTPS) server.

Steps	Command	Purpose
6.	**username** *name* **privilege** *level* **password** {**0** | **7** | *user-password* }*encrypted-password* Example: `Device(config)#username cisco privilege 15 password 0 cisco`	Establishes a username-based authentication system and privilege level for the user. The username privilege level must be configured as 15.
7.	**end** Example: `Device(config-if)#end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. VirutalPortGroups 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **interface** *type number*
5. **no switchport**
6. **ip address** *ip-address mask*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **end**

DETAILED STEPS

Step	Command
1.	**enable** Example: `Device>enable`
2.	**configure terminal** Example: `Device#configure terminal`
3.	**ip routing** Example: `Device(config)#ip routing`
4.	**interface type number** Example: `Device(config)#interface gigabitethernet 0/0/0`
5.	**no switchport** Example: `Device(config-if)#no switchport`
6.	**ip address ip-address mask** Example: `Device(config-if)#ip address 10.1.1.1 255.255.255.0`
7.	**exit** Example: `Device(config-if)#exit`
8.	**interface type number** Example: `Device(config)#interface virtualportgroup 0`

Step	Command
9.	**ip address ip-address mask** Example: `Device(config-if)#ip address 192.168.0.1 255.255.255.0`
10.	**end** Example: `Device(config-if)#end`
11.	**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Example: `Device#configure terminal`
12.	**app-hosting appid app1** Example: `Device(config)#app-hosting appid app1`
13.	**app-vnic gateway0 virtualportgroup 0 guest-interface 0** Example: `Device(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0`
14.	**guest-ipaddress 192.168.0.2 netmask 255.255.255.0** Example: `Device(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.2 netmask 255.255.255.0`
15.	**app-default-gateway 192.168.0.1 guest-interface 0** Example: `Device(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0`
16.	**end** Example: `Device#end`

Installing and Uninstalling Apps

SUMMARY STEPS

1. **enable**
2. **app-hosting install appid** *application-name* **package** *package-path*
3. **app-hosting activate appid** *application-name*
4. **app-hosting start appid** *application-name*
5. **app-hosting stop appid** *application-name*
6. **app-hosting deactivate appid** *application-name*
7. **app-hosting uninstall appid** *application-name*

DETAILED STEPS

Step	Command
1.	**enable** Example: `Device>enable`
2.	**app-hosting install appid** *application-name* **package** *package-path* Example: `Device#app-hosting install appid lxc_app package flash:my_iox_app.tar`
3.	**app-hosting activate appid** *application-name* Example: `Device#app-hosting activate appid app1`

Step	Command
4.	**app-hosting start appid** *application-name* Example: `Device#app-hosting start appid app1`
5.	**app-hosting stop appid** *application-name* Example: `Device#app-hosting stop appid app1`
6.	**app-hosting deactivate appid** *application-name* Example: `Device#app-hosting deactivate appid app1`
7.	**app-hosting uninstall appid** *application-name* Example: `Device#app-hosting uninstall appid app1`

Overriding the App Resource Configuration

Resource changes will take effect only after the app-hosting activate command is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **app-hosting appid** *name*
4. **app-resource profile** *name*
5. **cpu** *unit*
6. **memory** *memory*
7. **vcpu** *number*
8. **end**

DETAILED STEPS

Step	Command
1.	**enable** Example: `Device>enable`
2.	**configure terminal** Example: `Device#configure terminal`
3.	**app-hosting appid** *name* Example: `Device(config)#app-hosting appid app1`
4.	**app-resource profile** *name* Example: `Device(config-app-hosting)#app-resource profile custom`
5.	**cpu** *unit* Example: `Device(config-app-resource-profile-custom)# cpu 800`
6.	**memory** *memory* Example: `Device(config-app-resource-profile-custom)# memory 512`
7.	**vcpu** *number* Example: `Device(config-app-resource-profile-custom)# vcpu 2`

Step	Command
8.	**end** Example: `Device(config-app-resource-profile-custom)# end`

Verifying the Application Hosting Configuration

SUMMARY STEPS

1. **enable**
2. **show iox-service**
3. **show app-hosting detail**
4. **show app-hosting list**

DETAILED STEPS

1. **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device>enable
```

2. show iox-service

Displays the status of all IOx services

Example:

```
Device# 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
Device#
```

3. show app-hosting detail

Displays detailed information about the application.

Example:

```
Device#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
```

4. show app-hosting list

Displays the list of applications and their status.

Example:

```
Device#show app-hosting list
App id                           State
---------------------------------------------------------
app1                             RUNNING
```

Configuration Examples for Application Hosting

See the following examples:

Example: Enabling IOx

```
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
```

Example: Configuring a VirtualPortGroup to a Layer 3 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
```

Example: Installing and Uninstalling Apps

```
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
```

Example: Overriding the App Resource Configuration

```
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 enables users to deploy the docker applications on the IR1800. The application lifecycle process is similar to the procedure in the Installing and Uninstalling Apps section. For docker applications, entry point configuration is required as part of the application configuration. Please refer to the following example for the entry point configuration.

```
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 following 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#
```

Signed Application Support

Cisco Signed applications are now supported on the IR1800. In order to install a signed application, signed verification has to be enabled on the device. Signed verification can be enabled by following the following instructions.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#app-hosting signed-verification
Router(config)#
Router(config)#exit
```

After enabling the signed verification, follow the instructions in the Installing and Uninstalling Apps section under IOx Application Hosting in order to install the application.

Cisco Cyber Vision and Edge Intelligence

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

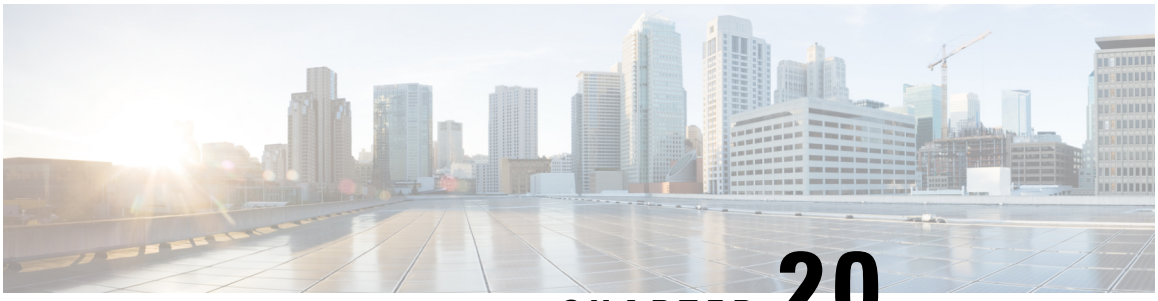
Deployment of Cyber Vision Center (CVC) on IOS-XE platform and Release Notes for Cisco Cyber Vision Release 3.1.1.

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/.



CHAPTER 20

Cisco SD-WAN Support

This chapter contains the following:

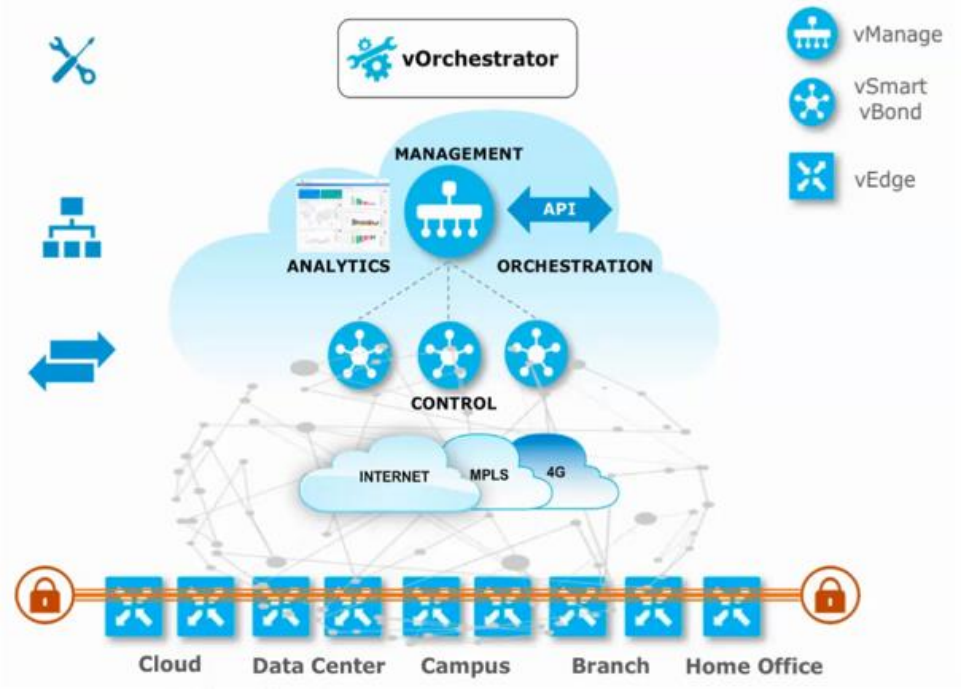
- Cisco SD-WAN Overview, on page 191
- Related Documentation, on page 192

Cisco SD-WAN Overview

Cisco SDWAN adopts a cloud based solution, it consists of vOrchestrator, vManage, vSmart and vEdge.

- vOrchestrator is responsible for launching all controllers VMs in the cloud.
- vManage is the management plane for the overall SDWAN solution. It uses netconf/YANG to talk to vEdge devices.
- vSmart is the control plane for the overall SDWAN solution. It talks to the vEdge device, acts as the route reflector, key reflector, and policy engine.
- vEdge is the data plane of the overall SDWAN solution. The IR8100 platform talks to vSmart, vManage, as part of the SDWAN network.

The follow diagram shows the high level architecture of SDWAN:



Related Documentation

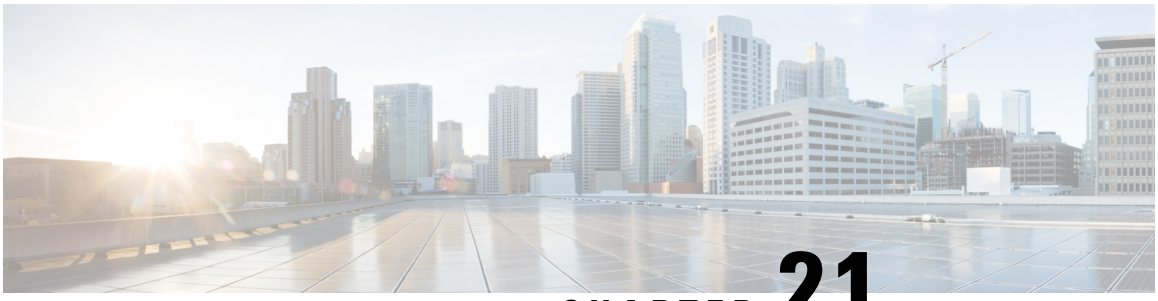
Cisco SDWAN documentation is available from the following sources:

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 21

ROM Monitor Overview

• ROM Monitor Overview and Basic Procedures, on page 193

ROM Monitor Overview and Basic Procedures

This chapter provides an overview of ROM Monitor concepts and operations.

This chapter includes the following main topics:

ROM Monitor Overview

The *ROM Monitor* is a bootstrap program that initializes the hardware and boots the Cisco IOS XE software when you power on or reload a router. When you connect a terminal to the router that is in ROM Monitor mode, the ROM Monitor (rommon 1>) prompt is displayed.

During normal operation, users do not use ROM Monitor mode. ROM Monitor mode is used only in special circumstances, such as reinstalling the entire software set, resetting the router password, or specifying a configuration file to use at startup.

The *ROM Monitor software* is known by many names. It is sometimes called *ROMMON* because of the CLI prompt in ROM Monitor mode. The ROM Monitor software is also called the *boot software* , *boot image* , or *boot helper* . Although it is distributed with routers that use the Cisco IOS XE software, ROM Monitor is a separate program from the Cisco IOS XE software. During normal startup, the ROM Monitor initializes the router, and then control passes to the Cisco IOS XE software. After the Cisco IOS XE software takes over, the ROM Monitor is no longer in use.

Environmental Variables and the Configuration Register

Two primary connections exist between ROM Monitor and the Cisco IOS XE software: the ROM Monitor environment variables and the configuration register.

The ROM Monitor environment variables define the location of the Cisco IOS XE software and describe how to load it. After the ROM Monitor has initialized the router, it uses the environment variables to locate and load the Cisco IOS XE software.

The *configuration register* is a software setting that controls how a router starts up. One of the primary uses of the configuration register is to control whether the router starts in ROM Monitor mode or Administration EXEC mode. The configuration register is set in either ROM Monitor mode or Administration EXEC mode as needed. Typically, you set the configuration register using the Cisco IOS XE software prompt when you

need to use ROM Monitor mode. When the maintenance in ROM Monitor mode is complete, you change the configuration register so the router reboots with the Cisco IOS XE software.

Accessing ROM Monitor Mode with a Terminal Connection

When the router is in ROM Monitor mode, you can access the ROM Monitor software only from a terminal connected directly to the console port of the card. Because the Cisco IOS XE software (EXEC mode) is not operating, nonmanagement interfaces are not accessible. Basically, all Cisco IOS XE software resources are unavailable. The hardware is available, but no configuration exists to make use of the hardware.

Network Management Access and ROM Monitor Mode

It is important to remember that ROM Monitor mode is a router mode, not a mode within the Cisco IOS XE software. It is best to remember that ROM Monitor software and the Cisco IOS XE software are two separate programs that run on the same router. At any given time, the router runs only one of these programs, .

One area that can be confusing when using ROM Monitor and the Cisco IOS XE software is the area that defines the IP configuration for the Management Ethernet interface. Most users are comfortable with configuring the Management Ethernet interface in the Cisco IOS XE software. When the router is in ROM Monitor mode, however, the router does not run the Cisco IOS XE software, so that Management Ethernet interface configuration is not available.

When you want to access other devices, such as a TFTP server, while in ROM Monitor mode on the router, you must configure the ROM Monitor variables with IP access information.

Note TFTP access variables are currently not supported on the IR1800 platform.

Access ROM Monitor Mode

The following sections describe how to enter the ROMMON mode, and contains the following sections:

Checking the Current ROMMON Version

To display the version of ROMmon running on a router, use the **show rom-monitor** command . To show all variables that are set in ROMmon, use show romvar.

```
Router#show rom-monitor r0
System Bootstrap, Version 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


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

Router# reload
```

If your configuration register was set to hex value 0x0 or 0x1820, reload operation will bring you to the ROMmon mode command prompt (rommon 1>). Invoking the set command at the prompt (rommon 1> set) will display the same information as "show romvar" above in IOS/XE exec mode.

```
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 9: 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
```

Changing the ROM Monitor Prompt

You can change the prompt in ROM Monitor mode by using the **PS1=** command as shown in the following example:

```
rommon 8 > PS1="IR1800 rommon ! > "
IR1800 rommon 9 >
```

Changing the prompt is useful if you are working with multiple routers in ROM Monitor at the same time. This example specifies that the prompt should be “IR1800 rommon ”, followed by the line number, and then followed by “ > “ by the line number.

Displaying the Configuration Register Setting

To display the current configuration register setting, enter the **confreg** command without parameters as follows:

```
rommon > confreg
   Configuration Summary
   (Virtual Configuration Register: )
enabled are:
[ 0 ] break/abort has effect
[ 1 ] console baud: 9600
 boot:...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:
```

The configuration register setting is labeled *Virtual Configuration Register* . Enter the **no** command to avoid changing the configuration register setting.

Environment Variable Settings

The ROM Monitor environment variables define the attributes of the ROM Monitor. Environmental variables are entered like commands and are always followed by the equal sign (=). Environment variable settings are entered in capital letters, followed by a definition. For example:

```
IP_ADDRESS=10.0.0.2
```

Under normal operating conditions, you do not need to modify these variables. They are cleared or set only when you need to make changes to the way ROM Monitor operates.

This section includes the following topics:

Frequently Used Environmental Variables

The following table shows the main ROM Monitor environmental variables. For instructions on how to use these variables, see the relevant instructions in this document. The 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 10: Frequently Used ROM Monitor Environmental Variables

Environmental variable	Description
BOOT=path/file	Identifies the boot software for a node. This variable is usually set automatically when the router boots.

Displaying Environment Variable Settings

To display the current environment variable settings, enter the **set** command :

```
rommon 1 > showmon
System Bootstrap, Version 1.4(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.
```

Entering Environment Variable Settings

Environment variable settings are entered in capital letters, followed by a definition. The following example shows the environmental variables that can be configured in ROMmon mode.:

```
rommon 1 > confreg 0x0
rommon 1> BOOT_WDOG = DISABLE
rommon 1> BOOT = IR8100-K9_image_name
```

Saving Environment Variable Settings

To save the current environment variable settings, enter the **sync** command:

```
rommon > sync
```

Note Environmental values that are not saved with the **sync** command are discarded whenever the system is reset or booted.

Exiting ROM Monitor Mode

To exit ROM Monitor mode, you must change the configuration register and reset the router.

Procedure

	Command or Action	Purpose
Step 1	**confreg** **Example:** `rommon 1> confreg`	Initiates the configuration register configuration prompts.
Step 2	Respond to each prompt as instructed.	See the example that follows this procedure for more information.
Step 3	**reset** **Example:** `rommon 2> reset`	Resets and initializes the router.

Configuration Example

```
rommon 3 > confreg
           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:
 enable  "use net in IP bcast address"? y/n  [n]:
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 disable "break/abort has effect"? y/n  [n]:
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:
change the boot characteristics? y/n  [n]:
           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:
```

Upgrading the ROMmon for a Router

ROMmon upgrade on the IR1800-K9 router is automatically done when the image is booted. The latest version of the ROMmon is bundled with the IOSXE image. An algorithm detects if the current running version is older than the bundled version, if so, it is automatically upgraded. If the current running version is equal to the bundled version no upgrade is executed. For every successful upgrade, the router is automatically rebooted in order for the new version to get loaded and executed.:

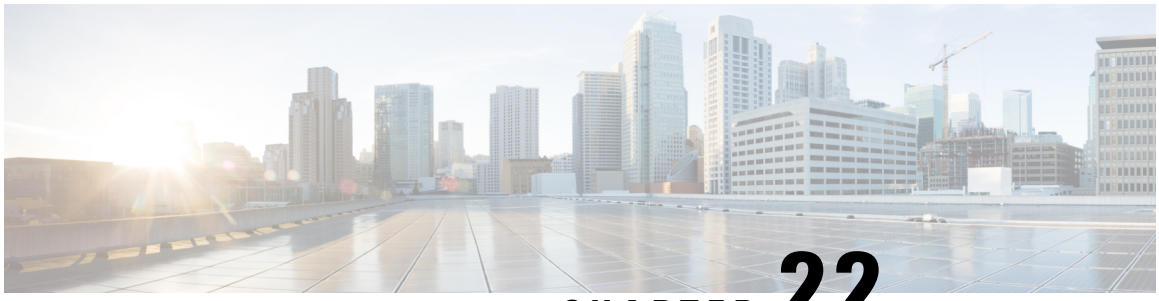
Procedure

Step 1 (Optional) Run the **show rom-monitor** *slot* command on the router to see the current release numbers of ROMmon on the hardware. See the Checking the Current ROMMON Version, on page 194 for information about interpreting the output of the command that you run.

Step 2 If autoboot has not been enabled by using the **config-register 0x2102** command, run the **boot** *filesystem:/file-location* command at the ROMmon prompt to boot the Cisco IOS XE image, where *filesystem:/file-location* is the path to the consolidated package file. The ROMmon upgrade is not permanent for any piece of hardware until the Cisco IOS XE image is booted.

Step 3 Run the **enable** command at the user prompt to enter the privileged EXEC mode after the boot is complete.

Step 4 Run the **show rom-monitor** *slot* command to verify whether the ROMmon has been upgraded.



CHAPTER 22

WAN Monitoring

This chapter contains the following topics:

- Information About WANMon, on page 201
- Prerequisites , on page 202
- Guidelines and Limitations, on page 202
- Configuring WANMon, on page 202
- Verifying WANMon Configuration, on page 204
- Configuration Examples, on page 205

Information About WANMon

WANMon is a flexible solution to address the WAN link recovery requirements for the following products 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.

You enable WANMon to monitor your WAN links and initiate link recovery actions on receipt of link failure triggers.

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

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

- 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.

Configuring WANMon

You can enable WANMon on the router and assign WAMMon 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. WANMon is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	**event manager policy** *tm_wanmon.tcl* **authorization bypass**	Enables the WANMon link recovery module. Use **authorization bypass** to avoid authorization for CLIs invoked by this policy.
Step 2	**event manager environment wanmon_if_list** <*instance*> {*interface name* {**ipsla** <*instance*>}}	Configures WANMon for the interfaces in your WAN, and indicates that this is an interface configuration command. **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 specifing an instance. **Note** WANMon only looks at the status of the SLA ID. Even though *icmp-echo* is most common, if needed any other type of SLA probe (for example, *udp-echo*) can be used instead.
Step 3	**event manager environment wanmon_if_listx** {*interface name* {**recovery** *Level0* {*Level1* } *Level2*}}	(Optional) Overrides the built-in thresholds.
Step 4	**publish-event sub-system 798 type 2000 arg1** <*interface name*> **arg2** <*level* >	(Optional) Configures custom recovery actions using link resetter applets. <*interface* > 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	**{stub** <*track-stub-id* > **}**	(Optional) Allows an event manager environment policy to set the track object value. WANMon can set a track-stub-object value to reflect the link state so that an external applet can track the stub object.

	Command or Action	Purpose
Step 6	**event manager environment wanmon_if_listx** {<*interface name* > {**checkip** <*instance* >}}	(Optional) Disables IP address checking.

What to do next

EXAMPLES

```
event manager policy tm_wanmon.tcl authorization bypass
```

The following examples are Event Manager commands to configure cellular and Ethernet interfaces:

```
event manager environment wanmon_if_list1 {cellular0/4/0 {ipsla 1}}
event manager environment wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}
```

This example sets custom recovery thresholds:

```
event manager environment wanmon_if_list {cellular0/4/0 {recovery 20 {90 75} 600}
```

where:

- The Level 0 threshold is set to 20 minutes after the link failure trigger. Level 0 recovery actions are performed for the cellular interface. Repeats indefinitely, no more than every 10 minutes (default).
- Level 1 threshold is set to 90 minutes. Level 1 recovery actions are performed for the cellular interface. Repeats no more frequently than every 75 minutes.
- The Level 2 threshold is set to 600 minutes (10 hours).

The following sets the track-stub-object value to 21:

```
conf t
track 21 stub-object
event manager environment wanmon_if_list {cellular0/4/0 {ipsla 1} {stub 21}
```

Verifying WANMon Configuration

Use the following steps to verify your WANMon configuraion.

Procedure

	Command or Action	Purpose
Step 1	**show event manager policy registered**	Displays the WAN monitoring policy.
Step 2	**show event manager environment**	Displays the interface environment variables set during interface configuration.

What to do next

EXAMPLE

```
show event manager policy registered
1    script    system  multiple   Off   Thu Jan 16 18:44:29 2014  tm_wanmon.tcl
show event manager environment
1 wanmon_if_list   {cell0/4/0 {ipsla 1}}
```

Configuration Examples

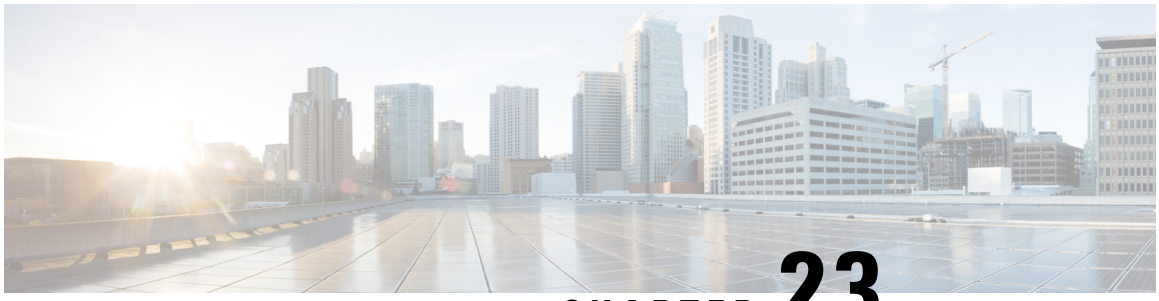
The following examples are provided:

WANMon Cellular Interface Configuration Example

```
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

```
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 23

Yang Data Models

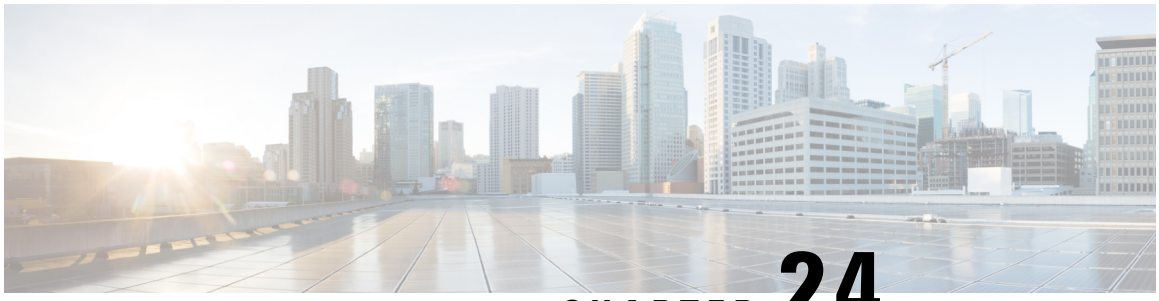
This chapter contains the following:

- Support for YANG Data Models, on page 207

Support for YANG Data Models

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 24

Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

- Process Health Monitoring, on page 209

Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

Monitoring Control Plane Resources

The following sections explain the details of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

- Avoiding Problems Through Regular Monitoring, on page 209
- Cisco IOS Process Resources, on page 209
- Overall Control Plane Resources, on page 216

Avoiding Problems Through Regular Monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. It also establishes a baseline for a normal system load. You can use this information as a basis for comparison, when you upgrade hardware or software to see if the upgrade has affected resource usage.

Cisco IOS Process Resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the **show memory** command and the **show process cpu** command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do

not include information for resources on the entire platform. When the **show memory** command is used in a system with 4 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

```
Router# show memory
Tracekey : 1#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
7F5F3731B0 0000000296 7F5F371138 7F5F373330 001  -------- -------- *Init*
:555F22A000+86B9178
7F5F373330 0000000568 7F5F3731B0 7F5F3735C0 001  -------- -------- *Init*
:555F22A000+86BEE5C
7F5F3735C0 0000032776 7F5F373330 7F5F37B620 001  -------- -------- Managed Chunk Q
:555F22A000+86AAC38
7F5F37B620 0000000056 7F5F3735C0 7F5F37B6B0 001  -------- -------- *Init*
:555F22A000+5EA29DC
7F5F37B6B0 0000032776 7F5F37B620 7F5F383710 001  -------- -------- Queue Pair - Q
:555F22A000+86D3A28
7F5F383710 0000012808 7F5F37B6B0 7F5F386970 001  -------- -------- *Init*
:555F22A000+11EFF930
7F5F386970 0000032776 7F5F383710 7F5F38E9D0 001  -------- -------- List Elements
:555F22A000+86798AC
7F5F38E9D0 0000032776 7F5F386970 7F5F396A30 001  -------- -------- List Headers
:555F22A000+86798EC
7F5F396A30 0000032776 7F5F38E9D0 7F5F39EA90 001  -------- -------- IOSXE Process S
:555F22A000+984FEE0
7F5F39EA90 0000032776 7F5F396A30 7F5F3A6AF0 001  -------- -------- IOSXE Queue Pro
:555F22A000+984FF24
7F5F3A6AF0 0000065544 7F5F39EA90 7F5F3B6B50 001  -------- -------- IOSXE Queue Bal
:555F22A000+984FF68
7F5F3B6B50 0000000328 7F5F3A6AF0 7F5F3B6CF0 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F3B6CF0 0000000328 7F5F3B6B50 7F5F3B6E90 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F3B6E90 0000000192 7F5F3B6CF0 7F5F3B6FA8 001  -------- -------- SDB String
:555F22A000+8629F60
7F5F3B6FA8 0000036872 7F5F3B6E90 7F5F3C0008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F3C0008 0000010008 7F5F3B6FA8 7F5F3C2778 001  -------- -------- Platform VM Pag
:555F22A000+986FC68
7F5F3C2778 0000002008 7F5F3C0008 7F5F3C2FA8 001  -------- -------- *Init*
iosd_crb_crankshaft_unix:7F83050000+6D850
7F5F3C2FA8 0000200712 7F5F3C2778 7F5F3F4008 001  -------- -------- Interrupt Stack
:555F22A000+98482F4
7F5F3F4008 0000000328 7F5F3C2FA8 7F5F3F41A8 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F3F41A8 0000002008 7F5F3F4008 7F5F3F49D8 001  -------- -------- Watcher Message
:555F22A000+86DE21C
7F5F3F49D8 0000000360 7F5F3F41A8 7F5F3F4B98 001  -------- -------- Process Events
:555F22A000+86D94A4
```

```
7F5F3F4B98 0000000328 7F5F3F49D8 7F5F3F4D38 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F3F4D38 0000000184 7F5F3F4B98 7F5F3F4E48 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F3F4E48 0000000264 7F5F3F4D38 7F5F3F4FA8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F3F4FA8 0000036872 7F5F3F4E48 7F5F3FE008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F3FE008 0000000328 7F5F3F4FA8 7F5F3FE1A8 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F3FE1A8 0000001504 7F5F3FE008 7F5F3FE7E0 001  -------- -------- Reg Function Se
:555F22A000+868AE50
7F5F3FE7E0 0000001504 7F5F3FE1A8 7F5F3FEE18 001  -------- -------- Reg Function Se
:555F22A000+868AEE0
7F5F3FEE18 0000000064 7F5F3FE7E0 7F5F3FEEB0 001  -------- -------- Parser Linkage
:555F22A000+5D98838
7F5F3FEEB0 0000000160 7F5F3FEE18 7F5F3FEFA8 001  -------- -------- *Init*
:555F22A000+530A17C
7F5F3FEFA8 0000036872 7F5F3FEEB0 7F5F408008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F408008 0000000328 7F5F3FEFA8 7F5F4081A8 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F4081A8 0000000760 7F5F408008 7F5F4084F8 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4084F8 0000000576 7F5F4081A8 7F5F408790 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F408790 0000000400 7F5F4084F8 7F5F408978 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F408978 0000000488 7F5F408790 7F5F408BB8 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F408BB8 0000000920 7F5F408978 7F5F408FA8 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F408FA8 0000200712 7F5F408BB8 7F5F43A008 001  -------- -------- Interrupt Stack
:555F22A000+98482F4
7F5F43A008 0000000968 7F5F408FA8 7F5F43A428 001  -------- -------- *Init*
iosd_crb_crankshaft_unix:7F83050000+378C0
7F5F43A428 0000000280 7F5F43A008 7F5F43A598 001  -------- -------- *Init*
:555F22A000+A3CE294
7F5F43A598 0000000896 7F5F43A428 7F5F43A970 001  -------- -------- Watched Message
:555F22A000+86DE1E8
7F5F43A970 0000001320 7F5F43A598 7F5F43AEF0 001  -------- -------- Process
:555F22A000+86E50BC
7F5F43AEF0 0000000096 7F5F43A970 7F5F43AFA8 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F43AFA8 0000036872 7F5F43AEF0 7F5F444008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F444008 0000003008 7F5F43AFA8 7F5F444C20 001  -------- -------- Watched Semapho
:555F22A000+86DE180
7F5F444C20 0000000360 7F5F444008 7F5F444DE0 001  -------- -------- Process Events
:555F22A000+86D94A4
7F5F444DE0 0000000368 7F5F444C20 7F5F444FA8 001  -------- -------- *Init*
:555F22A000+11EF88AC
7F5F444FA8 0000200712 7F5F444DE0 7F5F476008 001  -------- -------- Interrupt Stack
:555F22A000+98482F4
7F5F476008 0000002336 7F5F444FA8 7F5F476980 001  -------- -------- Process Array
:555F22A000+86E4F94
7F5F476980 0000000184 7F5F476008 7F5F476A90 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F476A90 0000000184 7F5F476980 7F5F476BA0 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F476BA0 0000000184 7F5F476A90 7F5F476CB0 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F476CB0 0000000184 7F5F476BA0 7F5F476DC0 001  -------- -------- *Init*
:555F22A000+86C945C
```

```
7F5F476DC0 0000000184 7F5F476CB0 7F5F476ED0 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F476ED0 0000000128 7F5F476DC0 7F5F476FA8 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F476FA8 0000036872 7F5F476ED0 7F5F480008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F480008 0000001320 7F5F476FA8 7F5F480588 001  -------- -------- Process
:555F22A000+86E50BC
7F5F480588 0000000184 7F5F480008 7F5F480698 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F480698 0000000184 7F5F480588 7F5F4807A8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F4807A8 0000000184 7F5F480698 7F5F4808B8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F4808B8 0000000184 7F5F4807A8 7F5F4809C8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F4809C8 0000000184 7F5F4808B8 7F5F480AD8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F480AD8 0000000184 7F5F4809C8 7F5F480BE8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F480BE8 0000000184 7F5F480AD8 7F5F480CF8 001  -------- -------- *Init*
:555F22A000+86C945C
7F5F480CF8 0000000096 7F5F480BE8 7F5F480DB0 001  -------- -------- *Init*
:555F22A000+86C940C
7F5F480DB0 0000000096 7F5F480CF8 7F5F480E68 001  -------- -------- Init
:555F22A000+862A110
7F5F480E68 0000000232 7F5F480DB0 7F5F480FA8 001  -------- -------- *Init*
:555F22A000+60E2660
7F5F480FA8 0000200712 7F5F480E68 7F5F4B2008 001  -------- -------- Interrupt Stack
:555F22A000+98482F4
7F5F4B2008 0000003008 7F5F480FA8 7F5F4B2C20 001  -------- -------- Reg Function Li
:555F22A000+868AE80
7F5F4B2C20 0000000064 7F5F4B2008 7F5F4B2CB8 001  -------- -------- Parser Linkage
:555F22A000+5D98838
7F5F4B2CB8 0000000064 7F5F4B2C20 7F5F4B2D50 001  -------- -------- Parser Linkage
:555F22A000+5D98A78
7F5F4B2D50 0000000080 7F5F4B2CB8 7F5F4B2DF8 001  -------- -------- Init
:555F22A000+5E87AC0
7F5F4B2DF8 0000000200 7F5F4B2D50 7F5F4B2F18 001  -------- -------- Init
:555F22A000+5E87AC0
7F5F4B2F18 0000000056 7F5F4B2DF8 7F5F4B2FA8 001  -------- -------- Init
:555F22A000+54DD60C
7F5F4B2FA8 0000036872 7F5F4B2F18 7F5F4BC008 001  -------- -------- *Init*
:555F22A000+98482F4
7F5F4BC008 0000001504 7F5F4B2FA8 7F5F4BC640 001  -------- -------- Reg Function Ca
:555F22A000+868AF10
7F5F4BC640 0000000224 7F5F4BC008 7F5F4BC778 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4BC778 0000000224 7F5F4BC640 7F5F4BC8B0 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4BC8B0 0000000328 7F5F4BC778 7F5F4BCA50 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4BCA50 0000000328 7F5F4BC8B0 7F5F4BCBF0 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4BCBF0 0000000328 7F5F4BCA50 7F5F4BCD90 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F4BCD90 0000000216 7F5F4BCBF0 7F5F4BCEC0 001  -------- -------- Init
:555F22A000+5E87AC0
7F5F4BCEC0 0000000144 7F5F4BCD90 7F5F4BCFA8 001  -------- -------- Init
:555F22A000+530F7A4
7F5F4BCFA8 0000200712 7F5F4BCEC0 7F5F4EE008 001  -------- -------- Interrupt Stack
:555F22A000+98482F4
7F5F4EE008 0000006888 7F5F4BCFA8 7F5F4EFB48 001  -------- -------- TTY data
:555F22A000+85C9E44
```

```
7F5F4EFB48 0000004104 7F5F4EE008 7F5F4F0BA8 001  -------- -------- TTY Input Buf
:555F22A000+85CBD60
7F5F4F0BA8 0000004104 7F5F4EFB48 7F5F4F1C08 001  -------- -------- TTY Output Buf
:555F22A000+85CBDB0
7F5F4F1C08 0000024584 7F5F4F0BA8 7F5F4F7C68 001  -------- -------- proc_hist_lmt_v
:555F22A000+BA3B718
7F5F4F7C68 0000008200 7F5F4F1C08 7F5F4F9CC8 001  -------- -------- proc_hist_lmt_v
:555F22A000+BA3B74C
7F5F4F9CC8 0000008200 7F5F4F7C68 7F5F4FBD28 001  -------- -------- proc_hist_lmt_v
:555F22A000+BA3B784
7F5F4FBD28 0000005008 7F5F4F9CC8 7F5F4FD110 001  -------- -------- messages
:555F22A000+86DE040
7F5F4FD110 0000005008 7F5F4FBD28 7F5F4FE4F8 001  -------- -------- Watched message
:555F22A000+86DE078
7F5F4FE4F8 0000020008 7F5F4FD110 7F5F503378 001  -------- -------- Watched Queue
:555F22A000+86DE0AC
7F5F503378 0000065544 7F5F4FE4F8 7F5F5133D8 001  -------- -------- Watched Queue I
:555F22A000+86DE0E4
7F5F5133D8 0000020008 7F5F503378 7F5F518258 001  -------- -------- Watched Boolean
:555F22A000+86DE118
7F5F518258 0000020008 7F5F5133D8 7F5F51D0D8 001  -------- -------- Watched Bitfiel
:555F22A000+86DE14C
7F5F51D0D8 0000010008 7F5F518258 7F5F51F848 001  -------- -------- Watcher Info
:555F22A000+86DE1B4
7F5F51F848 0000010008 7F5F51D0D8 7F5F521FB8 001  -------- -------- Read/Write Lock
:555F22A000+86DE250
7F5F521FB8 0000001232 7F5F51F848 7F5F5224E0 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F5224E0 0000000064 7F5F521FB8 7F5F522578 001  -------- -------- Init
:555F22A000+8D8F3A0
7F5F522578 0000002008 7F5F5224E0 7F5F522DA8 001  -------- -------- Injected msg CB
:555F22A000+ACBBF08
7F5F522DA8 0000000064 7F5F522578 7F5F522E40 001  -------- -------- SDB String
:555F22A000+8629F60
7F5F522E40 0000000056 7F5F522DA8 7F5F522ED0 001  -------- -------- *Init*
:555F22A000+5EA29DC
7F5F522ED0 0000000128 7F5F522E40 7F5F522FA8 001  -------- -------- XOS_MEM_XDT
:555F22A000+894FE1C
7F5F522FA8 0000028104 7F5F522ED0 7F5F529DC8 001  -------- -------- Process Stack
:555F22A000+98482F4
7F5F529DC8 0000000096 7F5F522FA8 7F5F529E80 001  -------- -------- Init
:555F22A000+862A110
7F5F529E80 0000000208 7F5F529DC8 7F5F529FA8 001  -------- -------- *Init*
:555F22A000+86C8D58
7F5F529FA8 0000016104 7F5F529E80 7F5F52DEE8 001  -------- -------- Process Stack
:555F22A000+98482F4
7F5F52DEE8 0000032776 7F5F529FA8 7F5F535F48 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F535F48 0000032776 7F5F52DEE8 7F5F53DFA8 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F53DFA8 0000032776 7F5F535F48 7F5F546008 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F546008 0000032776 7F5F53DFA8 7F5F54E068 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F54E068 0000032776 7F5F546008 7F5F5560C8 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F5560C8 0000032776 7F5F54E068 7F5F55E128 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F55E128 0000032776 7F5F5560C8 7F5F566188 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F566188 0000032776 7F5F55E128 7F5F56E1E8 001  -------- -------- List Elements
:555F22A000+8679DCC
7F5F56E1E8 0000005008 7F5F566188 7F5F56F5D0 001  -------- -------- Reg Function 12
:555F22A000+868AE1C
```

```
7F5F56F5D0 0000020008 7F5F56E1E8 7F5F574450 001  -------- -------- Subsys Malloc I
:555F22A000+86875C8
7F5F574450 0000001176 7F5F56F5D0 7F5F574940 001  -------- -------- SPA variable ms
:555F22A000+B9B3700
7F5F574940 0000000920 7F5F574450 7F5F574D30 001  -------- -------- SAMsgThread
:555F22A000+54E49DC
7F5F574D30 0000000064 7F5F574940 7F5F574DC8 001  -------- -------- Parser Linkage
:555F22A000+5D98A78
7F5F574DC8 0000000064 7F5F574D30 7F5F574E60 001  -------- -------- Parser Linkage
:555F22A000+5D98838
7F5F574E60 0000000064 7F5F574DC8 7F5F574EF8 001  -------- -------- Parser Linkage
:555F22A000+5D98A78
7F5F574EF8 0000000088 7F5F574E60 7F5F574FA8 001  -------- -------- Init
:555F22A000+54DD60C
7F5F574FA8 0000000968 7F5F574EF8 7F5F5753C8 001  -------- -------- Crypto CA
:555F22A000+8DC26C0
7F5F5753C8 0000000216 7F5F574FA8 7F5F5754F8 001  -------- -------- Crypto CA
:555F22A000+8DC2588
7F5F5754F8 0000002648 7F5F5753C8 7F5F575FA8 000  7F609C3C28 7F69C82D38 (coalesced)
:555F22A000+52BC2B8
7F5F575FA8 0000028104 7F5F5754F8 7F5F57CDC8 001  -------- -------- Process Stack
:555F22A000+98482F4
7F5F57CDC8 0000013112 7F5F575FA8 7F5F580158 001  -------- -------- SAMsgThread
:555F22A000+5360944
7F5F580158 0000004728 7F5F57CDC8 7F5F581428 001  -------- -------- *Packet Data*
:555F22A000+AF448CC
7F5F581428 0000000968 7F5F580158 7F5F581848 001  -------- -------- Exec
:555F22A000+5D9C004
7F5F581848 0000000600 7F5F581428 7F5F581AF8 001  -------- -------- Ether OAM subbl
:555F22A000+962A100
7F5F581AF8 0000000056 7F5F581848 7F5F581B88 000  7F69F8B620 7F6A906D40 (fragment)
:555F22A000+962A100
7F5F581B88 0000005008 7F5F581AF8 7F5F582F70 001  -------- -------- Reg Function iL
:555F22A000+868AEB0
7F5F582F70 0000065544 7F5F581B88 7F5F592FD0 001  -------- -------- Registry Call S
:555F22A000+8690EFC
7F5F592FD0 0000002584 7F5F582F70 7F5F593A40 001  -------- -------- *Init*
:555F22A000+868BC18
7F5F593A40 0000002080 7F5F592FD0 7F5F5942B8 001  -------- -------- *Init*
:555F22A000+ACB41D8
7F5F5942B8 0000002600 7F5F593A40 7F5F594D38 001  -------- -------- *Init*
:555F22A000+ACB41D8
7F5F594D38 0000020008 7F5F5942B8 7F5F599BB8 001  -------- -------- Peer uid cb chu
:555F22A000+ACBBE98
```

The **show process cpu** command displays Cisco IOS CPU utilization average:

```
Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   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
   5           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6          28          13       2153  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
   8           0           1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
   9       40648        7844       5182  0.00%  0.06%  0.05%   0 Check heaps
  10          16         845         18  0.00%  0.00%  0.00%   0 Pool Manager
  11           0           1          0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
```

```
  12           0           2           0  0.00%  0.00%  0.00%   0 Timers
  13           0         176           0  0.00%  0.00%  0.00%   0 WATCH_AFS
  14           0           1           0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
  15           0           1           0  0.00%  0.00%  0.00%   0 ARP Input
  16           4       52892           0  0.00%  0.00%  0.00%   0 ARP Background
  17           0           2           0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  18           0           1           0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  19           0           1           0  0.00%  0.00%  0.00%   0 CEF MIB API
  20           0           1           0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  21           0           1           0  0.00%  0.00%  0.00%   0 Policy Manager
  22           0           2           0  0.00%  0.00%  0.00%   0 DDR Timers
  23          16          10        1600  0.00%  0.00%  0.00%   0 Entity MIB API
  24         120          27        4444  0.00%  0.00%  0.00%   0 PrstVbl
  25           0           2           0  0.00%  0.00%  0.00%   0 Serial Backgroun
  26           0           1           0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
  27           0           2           0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
  28           0           2           0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
  29           4       25354           0  0.00%  0.00%  0.00%   0 IOSXE heartbeat
  30           0          86           0  0.00%  0.00%  0.00%   0 Btrace time base
  31           0          10           0  0.00%  0.00%  0.00%   0 DB Lock Manager
  32           4       50697           0  0.00%  0.00%  0.00%   0 GraphIt
  33           0           1           0  0.00%  0.00%  0.00%   0 DB Notification
  34           0           1           0  0.00%  0.00%  0.00%   0 IPC Apps Task
  35           0           1           0  0.00%  0.00%  0.00%   0 ifIndex Receive
  36           0       10142           0  0.00%  0.00%  0.00%   0 IPC Event Notifi
  37           0       49518           0  0.00%  0.00%  0.00%   0 IPC Mcast Pendin
  38           0           1           0  0.00%  0.00%  0.00%   0 Platform appsess
  39           0         846           0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  40           0       10142           0  0.00%  0.00%  0.00%   0 IPC Service NonC
  41           0           1           0  0.00%  0.00%  0.00%   0 IPC Zone Manager
  42           8       49518           0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  43           0       49518           0  0.00%  0.00%  0.00%   0 IPC Deferred Por
  44           0           1           0  0.00%  0.00%  0.00%   0 IPC Process leve
  45           0           1           0  0.00%  0.00%  0.00%   0 IPC Seat Manager
```

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
18412   18398      1%      1%      1%  S           135696  fman_fp_image
30574       2      0%      0%      0%  S                0  kworker/0:3
24231   16366      0%      0%      0%  S             2460  pman
24025   23998      0%      0%      0%  S             3392  nginx
24024   23998      0%      0%      0%  S             4300  nginx
23998   23990      0%      0%      0%  S             7944  nginx
23990    4251      0%      0%      0%  S             2460  pman
23605   23599      0%      0%      0%  S             7988  ngiolite
23599   16366      0%      0%      0%  S             2464  pman
23330   23309      0%      0%      0%  S            39600  iomd
23309   16366      0%      0%      0%  S             2460  pman
21981   15002      0%      0%      0%  S              416  sleep
21935   21906      0%      0%      0%  S            38680  iomd
21906   16366      0%      0%      0%  S             2460  pman
21830   13884      0%      0%      0%  S              416  sleep
21694       2      0%      0%      0%  S                0  kworker/0:0
21042       2      0%      0%      0%  S                0  kworker/u8:4
21041       2      0%      0%      0%  S                0  kworker/u8:3
```

```
21040       2      0%      0%      0%  S              0  kworker/u8:0
20737       2      0%      0%      0%  S              0  kworker/1:3
20731       2      0%      0%      0%  S              0  SarIosdMond
20574   20548      0%      0%      0%  S          12004  btman
20548   16921      0%      0%      0%  S           2432  pman
20180   20146      0%      0%      0%  S          17428  cman_fp
20146   16921      0%      0%      0%  S           2432  pman
20135   20105      0%      0%      0%  S          12228  btman
20105   16366      0%      0%      0%  S           2432  pman
20093       2      0%      0%      0%  S              0  kworker/0:1
19819   19796      0%      0%      0%  S         107992  cpp_cp_svr
19796   16921      0%      0%      0%  S           2436  pman
19549   19528      0%      0%      0%  S          18948  cmcc
19541   19512      0%      0%      0%  S          35124  cpp_driver
19528   16366      0%      0%      0%  S           2432  pman
19512   16921      0%      0%      0%  S           2432  pman
19280   19243      0%      0%      0%  S          38708  cpp_ha_top_leve
19243   16921      0%      0%      0%  S           2436  pman
18966   18959      0%      0%      0%  S          49916  cpp_sp_svr
18959   16921      0%      0%      0%  S           2436  pman
18877   18862      0%      0%      0%  S           5780  pttcd
18862    4251      0%      0%      0%  S           2432  pman
18856       2      0%      0%      0%  S              0  kworker/1:1
18711   18691      0%      0%      0%  S          10352  hman
18691   16366      0%      0%      0%  S           2432  pman
18679   16921      0%      0%      0%  S           2436  pman
18517   18495      0%      0%      0%  S          60720  pubd
18495    4251      0%      0%      0%  S           2432  pman
18398   16921      0%      0%      0%  S           2432  pman
18211       2      0%      0%      0%  S              0  kworker/0:2
18140   18120      0%      0%      0%  S          10352  hman
18120   16921      0%      0%      0%  S           2436  pman
17448   16921      0%      0%      0%  S            428  inotifywait
17253       2      0%      0%      0%  S              0  kworker/1:0
17204       1      0%      0%      0%  S           2064  rotee
16921       1      0%      0%      0%  S           5512  pvp.sh
16744   16366      0%      0%      0%  S            428  inotifywait
16582       1      0%      0%      0%  S           2060  rotee
16366       1      0%      0%      0%  S           5512  pvp.sh
15627       2      0%      0%      0%  S              0  bioset
15626       2      0%      0%      0%  S              0  dmcrypt_write
15625       2      0%      0%      0%  S              0  kcryptd
15624       2      0%      0%      0%  S              0  kcryptd_io
15623       2      0%      0%      0%  S              0  bioset
15621       2      0%      0%      0%  S              0  kdmflush
15618       2      0%      0%      0%  S              0  loop1
15563       2      0%      0%      0%  S              0  ext4-rsv-conver
15562       2      0%      0%      0%  S              0  jbd2/mmcblk0p1-
15023       2      0%      0%      0%  S              0  kworker/u8:1
15002   14992      0%      0%      0%  S           1440  sort_files_by_i
14992    4251      0%      0%      0%  S           2416  pman
13884   13874      0%      0%      0%  S           2816  flash_check.sh
```

Overall Control Plane Resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the **show platform software status control-processor brief** command (summary view) or the **show platform software status control-processor command** (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational, but that the operating level should be reviewed. Critical implies that the router is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, and so on.

The following sections describe the fields in the **show platform software status control-processor** command output.

Load Average

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

Memory Utilization

Memory utilization is represented by the following fields:

- Total—Total system memory
- Used—Consumed memory
- Free—Available memory
- Committed—Virtual memory committed to processes

CPU Utilization

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts
- SIRQ—System Interrupts
- IOwait—Percentage of time CPU was waiting for I/O

Example: show platform software status control-processor Command

The following are some examples of using the **show platform software status control-processor** command:

```
Router# show platform software status control-processor
RP0: online, statistics updated 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: 62.51
  IRQ: 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

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use **show** commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Oct  6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded

[free space is 1429020 kB] - Please clean up files on bootflash.
```

Approaches for Monitoring Hardware Alarms

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

Enabling the logging alarm Command

The **logging alarm** command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

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

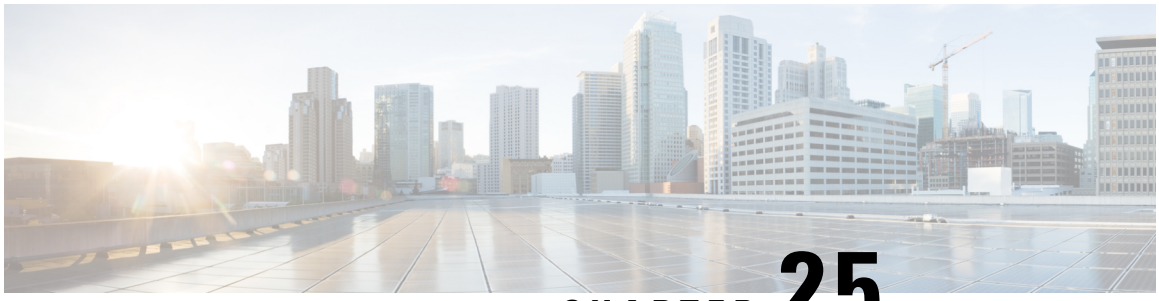
The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC4133 (required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB

- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)



CHAPTER 25

Troubleshooting

- Troubleshooting, on page 221
- Understanding Diagnostic Mode, on page 221
- Before Contacting Cisco or Your Reseller, on page 222
- show interfaces Troubleshooting Command, on page 222
- Software Upgrade Methods, on page 222
- Change the Configuration Register, on page 223
- Recovering a Lost Password, on page 226

Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a PC to the router via the console port. With a connected PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface by using Telnet. The Telnet option assumes that the interface is up and running.

Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into the diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.

- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

show interfaces Troubleshooting Command

Use the **show interfaces** command to display the status of all physical ports and logical interfaces on the router. describes messages in the command output.

The IR1800 supports the following 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

Several methods are available for upgrading software on the Cisco IR1840H Routers, including:

- Copy the new software image to flash memory over the WAN interface when the existing Cisco IOS software image is in use.
- Copy the new software image over the console port while in ROM monitor mode.

- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To boot the image from the TFTP server, the TFTP server must be on the same network as the router.

Change the Configuration Register

To change a configuration register, follow these steps:

Procedure

Step 1 Connect a PC to the CONSOLE port on the router.

Step 2 At the privileged EXEC prompt (*router_name* #), enter the **show version** command to display the existing configuration register value (shown in bold at the bottom of this output example):

Example:

```
Router# show version
Cisco IOS XE Software, Version 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)

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



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 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#
```

Step 3 Record the setting of the configuration register.

Step 4 To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register** <*value*>command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

Configuring the Configuration Register for Autoboot

Note Altering the configuration register is only for advanced troubleshooting and should only be done with guidance from Cisco support.

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the **config-reg** 0x0 command.
- From the ROMMON prompt, use the **confreg** 0x0 command.

Note Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

Reset the Router

To reset the router, follow these steps:

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.

Example:

```
rommon 1>
```

Step 2 Enter **confreg 0x2142** to ignore the running config.

Example:

```
rommon 2> confreg 0x2142
```

Step 3 (Optional) 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 the controller mode and needs to change it to autonomous mode.

Step 4 Sync the configuration changes with the **sync** command.

Example:

```
rommon 4>sync
```

Step 5 Reset the router to apply confreg. The router will reload with the reset.

Example:

```
rommon 5>reset
resetting...
```

Step 6 Verify that the correct confreg 0x2142 was applied, and enter**n** when asked if you want to change the configuration.

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 Boot the image with the confreg 0x2142.

Example:

```
rommon 2> boot
bootflash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210207_015223_V17_5_0_161.SSA.bin
```

Recovering a Lost Password

To recover a lost password, follow these steps. Refer to Reset the Router, on page 225 for details.

1. Reset the router.
2. Change the confreg to 0x2142.
3. Boot the router with confreg 0x2142 from Rommon.
4. If you used the reset button, add the license:

```
Router#config term
Router#license smart reservation
```

Note Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

Procedure

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

Example:

```
Router# configure terminal
```

Step 2 Enter the **configure register** command and the original configuration register value that you recorded.

Example:

```
Router(config)# config-reg
value
```

Step 3 Enter **exit** to exit configuration mode:

Example:

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

Note To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

Step 4 Reboot the router, and enter the recovered password.

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**transport-map type console** *transport-map-name* **Example:** `Router(config)# transport-map type console consolehandler`	Creates and names a transport map for handling console connections, and enters transport map configuration mode.
Step 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] **Example:** `Router(config-tmap)# connection wait none`	Specifies how a console connection will be handled using this transport map. • **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. **Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**. • **none**—The console connection immediately enters diagnostic mode.

	Command or Action	Purpose

Step 5	(Optional) **banner** [**diagnostic** | **wait**] *banner-message*
	Example:
	`Router(config-tmap)# banner diagnostic X`
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.
		• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
		Note Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.
		• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.
		• *banner-message*—Banner message, which begins and ends with the same delimiting character.

Step 6	**exit** **Example:** `Router(config-tmap)# exit`	Exits transport map configuration mode to re-enter global configuration mode.
Step 7	**transport type console** *console-line-number* **input** *transport-map-name* **Example:** `Router(config)# transport type console 0 input consolehandler`	Applies the settings defined in the transport map to the console interface. The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command.

Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

show transport-map [**all** | **name** *transport-map-name* | **type** [**console**]]

This command can be used either in user EXEC mode or privileged EXEC mode.

Example

The following example shows transport maps that are configured on the router: console port (`consolehandler`):

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type console
Transport Map:
Name: consolehandler


REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides

the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

Using the factory reset Commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.

Caution Use of the factory reset command should not be done lightly. All customer configurations will be ddeleted 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.

```
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
```

Boot Sequence after Factory Reset

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.